Heliyon 10 (2024) e29044

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Review article

Unraveling the role of cloud computing in health care system and biomedical sciences

Sonali Sachdeva [a], Saurabh Bhatia [b,c,**], Ahmed Al Harrasi [b], Yasir Abbas Shah [b], Khalid Anwer [d], Anil K. Philip [e], Syed Faisal Abbas Shah [f], Ajmal Khan [b], Sobia Ahsan Halim [b,*]

[a] IBM India Pvt. Ltd, India, 122002
[b] Natural & Medical Sciences Research Center, University of Nizwa, P.O. Box 33, 616 Birkat Al Mauz, Nizwa, Oman
[c] School of Health Science, University of Petroleum and Energy Studies, Prem Nagar, Dehradun, Uttarakhand, 248007, India
[d] Department of Pharmaceutics, College of Pharmacy, Prince Sattam Bin Abdulaziz University, Al-Kharj, 11942, Saudi Arabia
[e] School of Pharmacy, University of Nizwa, Birkat Al Mouz, Nizwa, 616, Oman
[f] Faculty of Computer Science & Information Technology, Virtual University of Pakistan, Lahore, 54000, Pakistan

ARTICLE INFO

Keywords:
Cloud computing
Health care
Genomics
Proteomics
Metabolomics
Radiology

ABSTRACT

Cloud computing has emerged as a transformative force in healthcare and biomedical sciences, offering scalable, on-demand resources for managing vast amounts of data. This review explores the integration of cloud computing within these fields, highlighting its pivotal role in enhancing data management, security, and accessibility. We examine the application of cloud computing in various healthcare domains, including electronic medical records, telemedicine, and personalized patient care, as well as its impact on bioinformatics research, particularly in genomics, proteomics, and metabolomics. The review also addresses the challenges and ethical considerations associated with cloud-based healthcare solutions, such as data privacy and cybersecurity. By providing a comprehensive overview, we aim to assist readers in understanding the significance of cloud computing in modern medical applications and its potential to revolutionize both patient care and biomedical research.

1. Introduction

The idea of cloud computing was presented in almost the middle of the nineteenth century by J C R Licklider [1], but instead of calling the term "Cloud" he termed this metaphor as "interconnected grid of computers" which is now represented as "Cloud" a symbol for the internet. An American computer scientist, John McCarthy, has explored concepts of artificial intelligence-based computing for public use [1]. The area of cyber security research started from the Phreaker movement. The Phreaker movement is a movement started by professionals involved in learning, understanding, controlling, and operating telephone communication systems. These skilled professionals have a good understanding of how to reverse engineer hardware and analogue communication protocols. They work regularly to study exactly how the telephone network and its operation work and operate. The main objective behind this knowledge is to learn and develop procedures for operating and manipulating the systems to get free services, for example,

* Corresponding author.
** Corresponding author. Natural & Medical Sciences Research Center, University of Nizwa, P.O. Box 33, 616 Birkat Al Mauz, Nizwa, Oman.
E-mail addresses: saurabhatia@unizwa.edu.om (S. Bhatia), sobia_halim@unizwa.edu.om (S. Ahsan Halim).

https://doi.org/10.1016/j.heliyon.2024.e29044
Received 10 December 2023; Received in revised form 24 March 2024; Accepted 28 March 2024
Available online 2 April 2024

long-distance calls. The phreaking movement was considered a major ethical issue in cyber security research; however, reviewing and testing telephonic network systems was not considered illegal. However, while reviewing and testing telephonic network systems mainly to enable free phone calls, sometimes the legal lines were crossed, which brings major concern regarding ethical issues and the safety of the network system. Previous reports also suggested that John McCarthy worked on artificial intelligence, in which he considered the idea of using computing for community use [1]. Owing to advancements in hardware, software, simple accessibility of telephony, as well as more bandwidth Internet, the impetus for cloud computing developed in the late nineteenth century. Via computer networks along with cloud computing, offers highly scalable and distributed computing solutions that considerably alleviate challenges associated with a deficiency of computing power in different areas [2]. Cloud computing is the next revolution in the IT industry and has been developing as a crucial area studied among IT researchers since 2007. Cloud computing was first proposed in China (2008) and later became more prevalent. China's Twelfth Five-Year Plan found that cloud computing has a significant contribution and position in the IT industry [3]. During this period, foremost IT companies like Amazon, IBM, Google, and Microsoft have started investing significant funds to expand as well as improve their cloud computing facilities. Cloud computing has notably gone through significant growth with the support of national policies, industrial developments, and scientific progress. Recently, several scientific reports based on cloud computing have been evidenced. Cloud computing or cloud security has diverse applications in different sectors, such as cloud health care, education, cloud life, and many more. One of the most emerging applications of cloud security is in healthcare. The ScienceDirect database search showed 3258 results after using the keywords 'cyber security, healthcare' on 02/07/21 at 11:30 a.m. (India), which signifies the importance of cyber security in the healthcare industry. Following similar results, using the same keywords showed that the number of research articles has increased from 02 (in 1971) up to 680 (in 2021). Using the potential of cloud security, massive healthcare data can be stored, secured, managed, arranged, and accessed securely in the cloud [4]. Cloud computing, as well as the Internet of Things, when utilized effectively to store, manage, access, secure, and organize medical and health data, is called 'cloud health care'. Cloud health care is defined as health care facilities that develop the delivery of diagnosis and treatment more effectively using tools including cloud computing and IoT [5].

Recently, various physicians and healthcare practitioners around the world have explored cloud healthcare in developing a strong, consistent, and economical cloud program-based design to deal with a greater number of simultaneous requirements from global healthcare facilities [6]. Due to the service-orientated, widespread, and on-demand nature of cloud computing, these concurrent requests from different resources can be dealt with in the best manner. Based on cloud security and wireless sensor networks system, Wang et al. [7] considered and evaluated a mobile health information system by implementing the grey hypothesis and the Markov model to calculate the progress of the bodies at the same time. Another team of researchers demonstrated the application of cloud computing in the health care system by using smart devices, as well as its applications as terminals to allow health professionals and relatives of patients to easily access medical data [8]. Recent reports also showed that big data analytics in the form of a cryptosystem allow healthcare workers to enable improvement in healthcare, mainly to detect any medical conditions by using any clinical images of the patients. In addition, in the COVID-19 pandemic, Big Data analytics could access image-based data (radiological and microscopical) of the lungs and other vital organs as well as case studies/diagnosis reports. The cryptosystem was found to be very secure against cyberattacks and other interferences and has a very strong key sensitivity [9]. A recent study demonstrated the positive effect of an Internet and mobile phone–targeted intervention on physical activity in patients with cardiovascular complications [10].

Recently, a deep neural network and the rapid public support of medical clothing have been efficiently transformed. Deep neural network driven IoT authorized new advancements for medical professionals and added new prospects to medical data analysis in the healthcare industry. A recent study showed that AI-driven IoT eHealth architecture based on the Grey Filter Bayesian Convolution Neural Network accurately assesses medical data analysis for heart signals by effectively distinguishing between healthy and unhealthy heart signals [11].

A recent interview with Steve Mansfield-Devine also concluded that healthcare organizations are getting more advanced and better at dealing with leaks and ransoms, which are considered key threats to healthcare organizations [12].

To study the lack of health insurance among adults who participated in the National Health and Nutrition Examination Survey, Cheung [13] analyzed the data using mobile medical testing centers. Zhongxing Telecommunication Equipment Corporation launched the Healthy Cloud Healthcare program, mainly to employ medical devices (without wire) to save human health data in real-time as we store the records in the cloud-based system. This cloud-based service can efficiently maintain medical e-mail data for individuals. Using mobile wireless devices, users can access these data at anytime from anywhere. By doing this, they can not only know their health conditions but also maintain appropriate communications with their physicians through the platform.

Each advancement has its two sides, positive as well as negative. Due to the increasing number of diseases or complications that result in more casualties or patients leading to the development of big data in the form of e-prescription services, digital imaging, e-health records, and enterprise resource planning systems are among the digital services, efficient cyber tool is required to store data with high security. Cyber security plays an important role in not only securing data from malware, vulnerabilities, or cyber-attacks but also identifying and mitigating risks. Based on the nature of vulnerabilities and risks associated with these vulnerabilities cybersecurity periodically asks the organization to update the program. Program updates could be minor or major depending upon the nature of vulnerabilities. Cybersecurity also deals with a situation when malware illicitly infects clouds after bypassing all the cybersecurity tools and controls or hacking the system for monetary benefits or for causing destruction. Thus, cybersecurity plays an important role in the healthcare sector. Integrations between the IT and these digital health care services are required to store and manage the data and provide access points to end users securely. Just like other sectors, the healthcare sector has also witnessed considerable advances from digital transformation, and with the effect of the growing Internet of Things. Patient data is generally more accessed by healthcare industries. Nevertheless, the more complications associated with IT networks that control healthcare organizations, and the total volume of data create more challenges associated with safeguarding network and data security [14].

In healthcare, one of the areas where cyber security is more applicable is DNA science, proteomics, and genomics. Due to the digital advancements in DNA and protein science, most of the researchers developed programs, software tools, and applications for protein-based quantitative structure–activity relationship, gene/DNA sequencing, gene/DNA synthesizing, gene/DNA analyzing, and accessing DNA and genomic data, storing protein or genetically based information in shared datastores. The advanced methods and techniques available in bioinformatics-based cloud computing allow scientists to study protein (receptor) and drug interactions, access and store genomic information from organisms, and create organisms with unique characteristics. These tools are mainly developed to store molecular (protein/nucleic acid/gene) information and to ensure their security via tools available in cyber security and generate secure access points for the end consumer. The main objective of cloud computing and security in DNA science is to study and detect susceptibilities in gene-based DNA databases and bioinformatics software applications, which can result in data breaches or cyber-attacks that influence the privacy, nature, and accessibility of such sensitive information [15].

The programming of robotics or sensors used in surgery or hospital infrastructure is highly sensitive and must be properly secured and updated to prevent any malware attacks. Cybersecurity plays an important role in securing the programming of these healthcare-based robotics, especially those that are in close contact with patients. Robotics associated with surgery offer a perfect ecosystem for surgical telemonitoring and telesurgery providing endoscopic optics and computerized device movement. The idea of surgical tele-mentoring allows the use of IT skills to offer real-time advice and practical support for surgical practices from a specialist physician at a different place. Another application of cyber computing is to store the data or applications or programs or tools associated with robotics used in surgery or radio imaging securely in cloud and to control this information and share it in secured networks for the end users. Recent studies have shown that tele-mentoring, as well as telesurgery in somewhat invasive surgery, is becoming more useful and economic in accelerating the training of modern surgical abilities globally and accessibility of surgical assistance in underserved locations [16].

The advent of cloud computing has ushered in a transformative era in various sectors, including healthcare and biomedical sciences. Cloud computing's potential to store, manage, and analyze vast amounts of data has opened new frontiers in these fields, promising to revolutionize the way health services are delivered and biomedical research is conducted. Despite its rapid adoption, there remains a paucity of comprehensive research that delineates the full spectrum of cloud computing's implications within these critical sectors. This gap in the literature signals a need for a thorough investigation into the multifaceted role of cloud computing in healthcare and biomedical sciences.

The significance of this research lies in its potential to inform healthcare providers, policymakers, and researchers about the benefits and challenges associated with the integration of cloud computing technologies. By providing a nuanced understanding of cloud computing applications—from electronic medical records and telemedicine to bioinformatics and genomic data analysis—this study aims to contribute to the optimization of health services and the advancement of scientific discovery.

2. Cloud tools used in biomedical sciences

Cloud computing plays an important role in biomedical science via offering users pay-*as*-you-go access to services for resolving widespread biomedical based complications troubles. Additional this cloud-based service presents secure on-demand storage as well as the evaluation and distinguished from conventional high-performance computing via their quick accessibility as well as scalability of facilities (Fig. 1) [17].

By using modern computation methods and tools, recently scientist have done much progress in molecular science such as have decoding of human genome, exploring new genes, created organisms with unique capabilities, identification of novel proteins and discovery of new drugs along with their automated manufacturing. With the advancement in cloud computing and cloud security it's

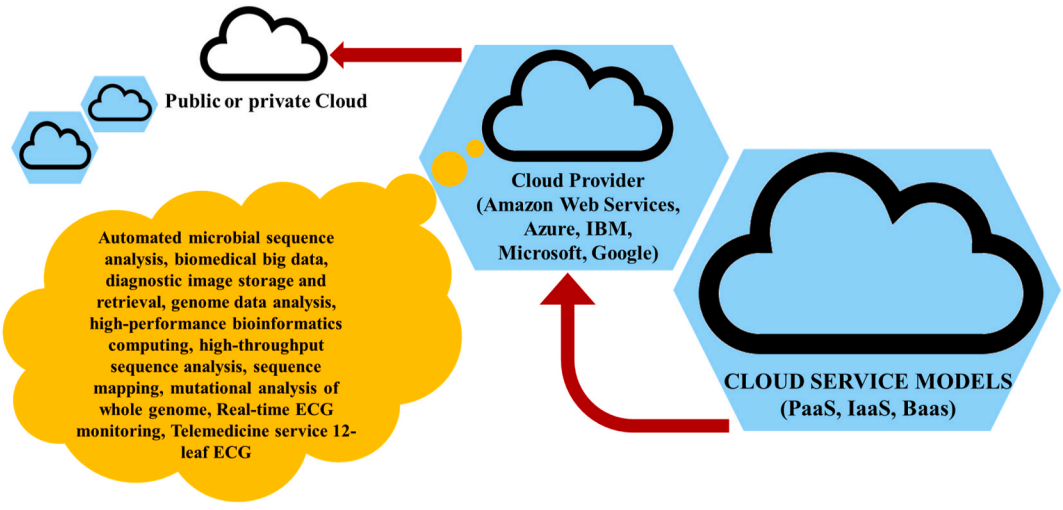

Fig. 1. Cloud services in Biomedical sciences.

now feasible to store this big confidential and sensitive nucleic acid and protein-based data safely in cloud space and access it whenever it's required from any location. Due to more commercialization and extensive research in this area there is always a risk of bio-cyber security threats. These threats can not only affect the leak the information but also corrupt the nature of proteomic or genomic-DNA data. Thus, with the aid of cyber security various programs or updates or software applications can be made for such data to secure as well as safely access this information. Recently various strategies have been developed to identify common threats or risks associated with genomic-DNA databases and bioinformatics applications which can lead to data breach or cyber-attacks influencing the privacy, integrity, and accessibility of such sensitive information. In biomedical sciences certain algorithm as well as program for equating main biological sequence information, including the amino-acid sequences of proteins or the nucleotides of DNA and/or RNA sequences have been developed in form of tools like BLAST (Basic Local Alignment Search Tool). BLAST is considered as one of the most important tools used in bioinformatic. Similarly, other programs such as FAST (for protein sequences), EMBOSS (European molecular biology open software suite), Staden packages (for sequence analysis), THREADER or PHD (for structure prediction), RasMol and WHATIF (for molecular imaging/modelling programs) and Clustalw (sequence alignment tool for DNA and protein sequences) are extensively used in bioinformatics [18]. Protein specific tools such as COPIA (COnsensus Pattern Identification and Analysis) is meant for structure related investigation for determining conserved regions called as motifs among various protein sequences and PROSPECT (PROtein Structure Prediction and Evaluation Computer ToolKit) is a tool used for protein-structure estimation specially to create a protein's 3-D model. These programs contain sensitive information which must be protected from cyber-attacks by using different cyber security tools.

Just like nucleic acid or protein based highly sensitive and confidential information, pathogenic microorganisms-based data especially genetic sequencing is also considered as highly sensitive and confidential data which is always vulnerable to cyber-attacks. The recent research, "Cyberbiosecurity: Remote DNA Injection Threat in Synthetic Biology," published in the academic journal Nature Biotechnology, demonstrated that attack records that how malware used to infiltrate a biologist's computer could breach many secure programs, replace unique nucleotide sequence in DNA. It was found that there is always a possibility of replacement of DNA sequence at the time when DNA orders are made to synthetic gene providers, as screening protocol might not work to detect the potentially harmful DNA. Software or the programs or applications developed to design and manage synthetic DNA projects may also be vulnerable to cyber-attacks that can be used to inject random DNA sequences into original genetic order, enabling "end-to-end cyberbiological attack" [19].

Real-time monitoring for the cyber threats especially for sensitive data like Viral Ebola and influenza genome data and cyber security of whole genomic information of microbial pathogenic strains causing outbreak such as food-borne disease-causing microorganisms related outbreaks and hospital outbreaks are studied recently. Handling of genomic data of microbial pathogens causing infection to plants resulting in epidemics for example the wheat blast outbreak as well as other data of pathogenic microorganisms that can cause public health and biosecurity must be monitored to prevent any leak and vulnerability. By breaching rules or programs set by the cyber security, these vulnerabilities cannot only leak the data but also it can change the nature of information by hacking, corrupting, deleting, or modifying data stored in server. In context to public health and biosecurity, cybersecurity has been considered as one of the major tools in dealing with the risks of new vulnerabilities associated with crucial and sensitive data. Relying more on public health and biological databases escalates risks for cyber-attacks by breaching biosecurity and conceding their integrity to either manipulate/corrupt/delete the data. It's also a fact that increase in reliability on genome databases escalates the risks of data breach or cyber-attacks which can affect community health and biosecurity systems by conceding nature, integrity, and privacy of the data.

Increase in utilization of genomic database raises the risks for public health as well as biosecurity as this can increase the chances of cyberthreats manipulating or hacking the information stored in secure domain. Health care professionals, physicians and end consumers are gradually more accepting IT networks and its devices in form of broadband access, mobile applications, cloud computing e-health services, and other health related portable wearable devices successfully eliminating the traditional boundaries around sensitive information. Using cyber security rule book and tools it's important to protect this information till the info goes to its expected end point including a patient, apps, electronic health records, general population, research databases, sensors, and websites. Protecting biological as well as health care related information in a cloud using digital ecosystem of tools can face formidable challenges in protecting the privacy and security of information. Thus, possible solutions to strengthen cyber biosecurity is required to offer maximum protection to data against both existing and future vulnerabilities.

3. Cybersecurity data science in protecting digital scientific data

Cybersecurity Data Science is considered as an emerging science to prevent, detect, and remediate expanding and evolving cybersecurity threats. Accessibility, security, and risks associated with highly sensitive and scientific digital platforms such as websites, scientific journals, digital scientific press, scientific databases, etc. can be efficiently monitored by cybersecurity tools. Closed and open access journals that need big data space with highly confidential and sensitive information of manuscript data (published as well as unpublished) flowing through internal system and accessed by multiple users in form of editors, authors and reviewers by web login can be secured by cyber security tools. Some journals have many issues in a year and need backup support for previous published reports. Such journals need more data space with high security. These days journals are also encouraging authors to submit supplementary material as well as videos or clippings of their research which again require more web space. E-journal scientific databases like Scopus, Directory of Open Access Journals, Web of Science, ScienceDirect, Wiley online library, JSTOR, SpringerLink, Taylor & Francis, PubMed, and Nature which are used to authenticate the systematic importance of the manuscripts can be more secured by using cyber security tools. Some of free libraries like Sci-Hub [one of the most criticized libraries in the world which was founded by Alexandra Elbakyan [20] to facilitate the free access to closed access manuscripts to avoid the high payment of articles behind

paywalls] has been recently criticized to pause serious data security concerns. Some of the science data based oldest repositories of research articles, books that use interface of website to provide the free access to the users are also vulnerable to possible cyber-attacks.

4. Role of cloud biosecurity in protecting genomic data

Cloud biosecurity is one of the most evolving interdisciplinary sciences which involves cybersecurity, cyber-physical security, and biosecurity. Earlier it was known for understanding the susceptibilities from undesirable resources, interferences, malicious and unsafe events. These activities can take place in or at the interfaces of medical sciences, supply chain, cyber, cyber-physical, and infrastructure systems. Cloud biosecurity in health care systems can develop and establish events to avert, protect against, alleviate, study, and feature those vulnerabilities pertaining to security. Genomic information is used in an ecosystem system where this information can be easily and efficiently produced and consumed. Genetic sequencing information are submitted by the labs to big databases including GenBank at the National Center for Biotechnology Information (NCBI) [21], DNA Data Bank of Japan (DDBJ) [22], the Gene Expression Omnibus (GEO) [23], the Short Read Archive (SRA) [24], the European Bioinformatics Institute EMBL database [25] and the microarray database Array Express [26]. Genetic sequencing-based information in these databases is stored, maintained, distributed, and organized by different tools. Usually, users access this information also via web portals formed by the databases, or via data integration genomic based web platforms or simply genome browser act as a centralized resource for the manipulation, analysis and visualization of that data such as Ensembl (genome browser) [27], University of California at Santa Cruz, (genome browser) [28], Galaxy (bioinformatics-based web-based portal) [29] and other model organism databases [30] (Fig. 2). Genomics professionals download this information from computer clusters and delete it when it's not required in future.

The number of digital platforms based on genome sequencing has been drastically increased with the advent of genome sequencing technology. Nevertheless, earlier the doubling time for DNA sequencing was time consuming in comparison to development in computer and storage capacity. After the arrival of next-generation sequencing (NGS) technologies various challenges have been overcome. Now archival databases and the value-added genome providers should not bother about less disk storage space as now their capacity can be easily upgraded. Thus, with the advent of cloud computing technologies, bioinformatics professionals must not bother about the shortage of disk storage space, necessarily potent networks, or computer clusters. Nevertheless, with the more advancements in next generation sequencing technologies and development of large amounts of data various considerable challenges developed such as.

- ➢ Issues associated with complexity and data management.
- ➢ Challenges associated with the increase in number of users to access the information in public cloud repositories resulting in significant traffic.
- ➢ Challenges associated with the increase in number of laboratories for the submissions of genetic data, resulting in increased significant crowdsourcing.
- ➢ Challenges linked with regulatory considerations for laboratories and their compliance in the regulatory environment for biological information.
- ➢ Cost and security concerns

One of the major challenges in genomic and data science is the development of gigantic supercomputer-based infrastructure with modern programs to achieve complete assessments of genomic information for biomedical as well as clinical studies. Recently various

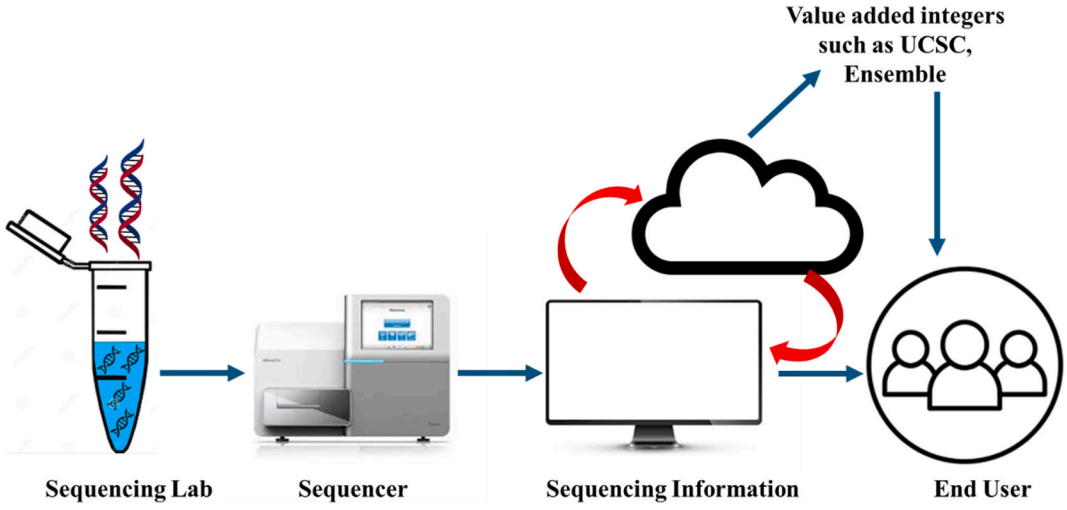

Fig. 2. Traditional approach of transmitting and interpreting genetic information by sequencing laboratories using internet to sequencing archival data base.

scientists are using cloud computing to put together data from systems biology, data mining in biomedicine and genomics. Additionally, cloud computing is also used to report data to solve biomedical challenges. Security risks associated with storing health information mainly genetic information in the cloud can cause considerable threats not only to end users but also to a healthcare-based organization as well as its patients if this information is not secured properly. Privacy and security both are interrelated terminologies, however readers must be familiar with differences as there might be slight differences in their meanings in different countries. Security or data protection in the US is defined as the protection of data from illegal access, unapproved activities, and susceptible damages while data privacy is primarily function as per administrative policies. Cloud computing offers several advantages including cost effectiveness and more productivity, however at the same time it also raises certain ethical as well as legal concerns related with data management, data protection, privacy and relocation, and liability. While storing genome-based data on any servers of big cloud service providers companies legally, above mentioned points must be considered. Meticulous genomic cloud computing is required to control as well as consistently monitor the security standards as well as the timely assessment of the data to secure and protect it. With current standards, genomic cloud computing can be used a climbable facility to store genetic sequence information and process it virtually usually via networked, significant data centers and access it remotely via different users and interface available over the Internet [31]. Instead of purchasing additional servers for the local research site, genomic cloud computing enables professionals to access tools, including application development interfaces to launch servers (Fig. 3). Different cloud computing services have evolved for genomic professionals such as DNAnexus [32] Galaxy [33], Bionimbus [34] and which enables professionals to execute genomic assessments utilizing only a web browser. These services can be used on certain clouds given by cloud service providers. With the advent in next generation sequencing, large sequencing-based information is increasing exponentially and considerable doubling in raw sequencing data in public archives has been also reported. To control and secure this massive data, genomic based researchers can use large-scale computational assets in form of cloud computing whereby clients can lease CPUs and storage from big data centers, where elasticity, reproducibility and privacy features of the data can be controlled [35].

Earlier, bioinformatics-based professionals download or upload genetic as well as healthcare-based information to local on-site storage such as computers for managing, evaluation and getting results followed by uploading data to repositories for publication. In comparison to the old bioinformatics workflow, the latest cloud computing decreases the requirement for professionals to transfer the information to their private computers. Rather than this, it is described by a one-stop plan where the computer is carried to the data (Fig. 3). Considering infrastructure as a service cloud computing, professionals can integrate and install their applications or programs into a cloud to run these applications and transfer the accumulated findings in a very secure manner (Fig. 3). However, the old bioinformatics workflow process, which was normally sluggish, is superfluous and requires high IT capital investment. Genomic cloud computing offers various merits over the traditional genetic data-based workflow process (Fig. 3). Most important merits include cost-effectiveness which enable admittance to reserve owing to its 'elasticity' i.e. an on-request facility in which one compensates (buying) for what one requires. This can avoid the requirement of buying several IT resources in-house to 'rent' such reserves from third parties when required.

For genomic professionals, this allows compensation for computing time and transfer. Additionally, to improve the internet connectivity as well as translational bandwidth, decreasing core bandwidth expenditure, large computer software programs purchase data transit in bulk. Subsequently, cloud computing also offers more data protection, since large-scale cloud platforms usually have the

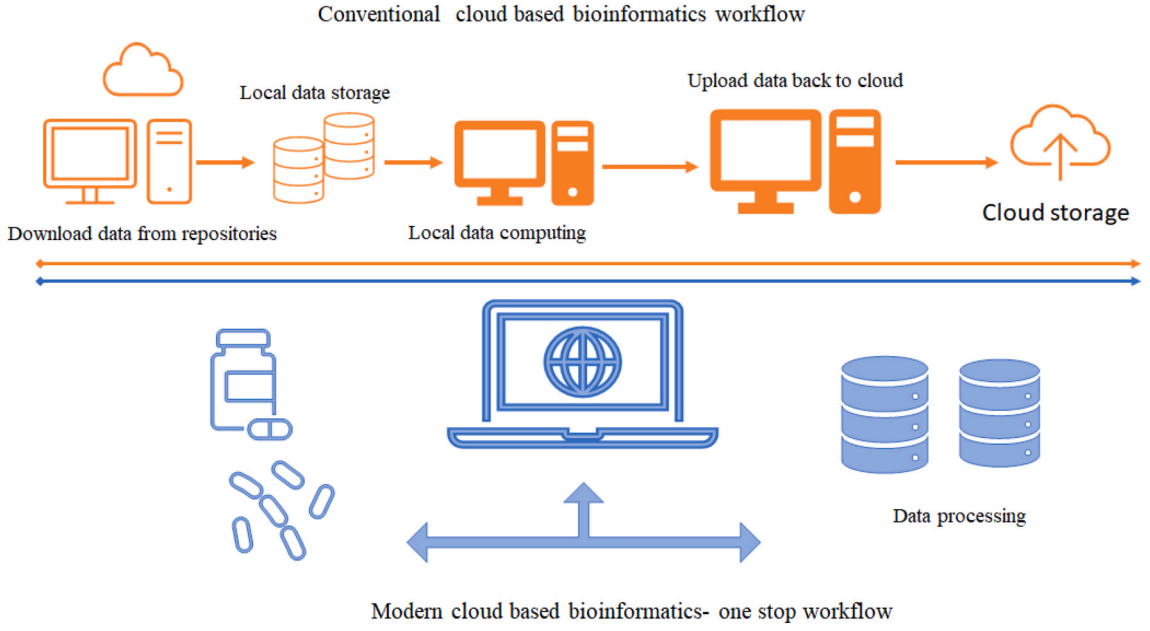

Fig. 3. Comparison between conventional bioinformatics and modern cloud-based road map.

capability to participate in and execute modern encryption, firewalls, and assessing abilities. Additionally, cloud platform developed for genomic data can improve data loading volume and provide effective handling, and extend genomic study via improving computing control, which can increase research especially novelty and circumvent the scientist challenges where they are restricted to limit their work to the infrastructure their organization made. Apart from cost effectiveness and efficiency cloud computing is becoming a much eco-friendlier solution via delivering power savings via external data storage and data bundling on robust workstation to build and deploy IT services.

5. Role of ProteoCloud in proteomics data analysis

Due to the huge expenses of the computational infrastructure required for investigating the findings obtained from protein-based research, high throughput proteomics has always been neglected. Advance mass spectrometers are proficient in producing data quicker in comparison to typical single desktop computers. To provide efficient hardware based computational infrastructure and to overcome these challenges many organizations have started capitalizing in computation clusters made up of morel processors to store more data and process it at a faster rate. However, development of this much expensive computational setup requires considerable expenditure in hardware, sufficient room to store the cluster, software license fees, and skilled manpower to run it. Among majority of computational labs, it's quite challenging to monitor the system in an order to make the cluster more robust to decrease "analytical backlog" through time of highest movement with no considerable underutilization through time of less activity. Proteomics research generally includes identification of proteins as well as peptides by using MS/MS sequence database search. Therefore, this tool is considered as a significant internal system in many proteomics research labs. To explore structural features tandem mass spectrometry (MS/MS) is generally used. Various approaches have been used recently for the interpretation of MS/MS data, mainly to understand the amino acid sequence of the peptides. One of the most popular approach is to utilize a search algorithm via shotgun proteomics search engine to distinguish peptides by comparing investigational and theoretical MS/MS data. This MS/MS database search algorithm is used to derive peptide sequences from in-silico digest of a protein sequence database and calculate theoretical fragmentation arrays against detected MS/MS data. For this purpose, various open database search engines have been used. An open-source option to marketable proteomics search programs called the open mass spectrometry search algorithm (OMSAA) has been developed and distributed by the National Institutes of Health team. OMSSA was further helped by Geer laboratory as well as recently an open mass spectrometry search algorithm results browser with a graphical user interface has been developed. Another open-source proteomics database search program was developed by Craig and Beavis entitled as X!Tandem, which was launched as open-source software under the "Artistic license" Now, OMSSA as well as X!Tandem have been extensively used by the researchers for the assessment of high throughput proteomics data. Various open database search engines have been introduced such as Comet, COMPASS, SEQUEST, MyriMatch, SpectraST, OMSSA, Andromeda, Tempest search, Sonar [36], MassMatrix, SALSA (The G. P. M. Organization TANDEM project), PeptideSearch [37], SCOPE (Amazon Amazon Elastic Compute Cloud), OLAV [36] and Mascot [36] search engine. In an order to further improve its performance MS/MS database search tools are coupled with statistical modeling tools like PeptideProphet [38], Percolator [39], and IDPicker [40]. Further recently top-down proteomics has been used for the analysis of intact proteins in their endogenous type devoid of proteolysis, conserving useful knowledge about post-translation changes, isoforms as well as proteolytic handling. Informed-Proteomics has been recently as an open-source software set for top-down proteomics study comprising of an LC-MS option for getting algorithm, a database search algorithm, and an interactive results viewer [41,42].

Due to the development of massive proteomics based raw investigational data and assumed biological findings, various integrated data repositories have been established that make the data and findings available to proteomics researchers. In late 19th century sequencing of first fully sequenced eukaryotic system i.e. yeast *Saccharomyces cerevisiae* was established using seminal mass spectrometry-based proteomics tools [43]. Various proteomics resources as well as repositories which have been reported recently such as BiblioSpec libraries, GPM X! Hunter libraries, NIST libraries, PeptideAtlas, PRIDE, Global Proteome Machine Database, SpectraST libraries, Tranche, YRC Public Data Repository. Alliance between cybersecurity, proteomics-based search engines/resources as well as repositories is required to protect the data from various vulnerabilities or cyber-attacks and set up as well as timely update the rule book to deal with existing or prevailing vulnerabilities or cyber-attacks.

6. Role of E-cloud computing in metabolomics

Metabolomics is the broad research to study the biological conversion of a variety of molecules in an organism. Due to the several advancements in metabolic research, new innovations have resulted in the development of unique, novel and highly sensitive information. Additionally, various Metabolomics Data Repositories such as MassIVE, MetaboLights has been maintained to store and protect massive data on a digital platform. With more advancements in this area, regular addition of more sensitive and new information over digital platform with both open as well as restricted access raised a major concern of data leak as well as make the data highly vulnerable against cyberattacks. Its computational rigorous environment has propelled needs for data storage area, open data formats, and data assessment tools. Also, restricted data systems, files stores, and data assessment devices are also maintained to restrict its access among limited users. Certain advanced solutions in the form of data analysis platforms such as PhenoMeNal have been created into the cloud. Such a solution can allow to connect a variety of independent, and at times unsuited, assessment procedures that are not easy to connect. PhenoMeNal (Phenome and Metabolome aNalysis) cloud-based E-infrastructure made for metabolomic study aims towards establishing an infrastructure to offer service that creates system-based, interoperable/scalable metabolomics data assessment programs into the cloud-based system. PhenoMeNal effortlessly assimilates a broad variety of present open-source devices that are analyzed as well as presented as Docker containers via the project's permanent assimilation procedure.

For metabolomics-based data, PhenoMeNal represents a supporting approach in cloud e-infrastructures accessible for metabolomics. PhenoMeNal is a distinctive as well as perfect service for developing electronic cloud-based infrastructures which can be scaled up as per the requirement [44].

7. Role of cloud computing in radiology

Due to features like broad, easily accessible, and reconfigurable resources, cloud computing has evolved recently in research and clinical settings. Healthcare professionals are expecting virtual cloud like services, to avoid tireless paper-based documentation and to manage, house, exchange, and utilize huge medical data. However, there are major ethical and security concerns associated with cloud computing vs medical settings. Main objective of cloud-based services while aligning with any health care service is to offer simple, scalable right to use computing as well as IT services as per the government requirements to safeguard confidentiality and safety of patient data and only allow access to authorized users. Cloud-based computing service for medical image-based data has progressed as a facility to offer cost effective recovery for stored data to completely introduced PACS. Further supplier-based neutral archiving facilities which can tackle the requirements of health care workers. Health care based professional global are currently assessing the cloud to disseminate medical based data such as images/reports/findings remotely to physicians/patients/radiologists via advanced reading tools. Cloud-based computing service can reduce huge expenses in equipment as well as its maintenance and control its operations remotely.

Healthcare systems marriage with cloud services permits storage of more data in a secure manner which can easily be accessible to end user and health care provider. Health care-based data such as clinical based radiological images require more storage, powerful connectivity, high resolution with sufficient display characteristics to the end users. These features can be obtained by cloud technologies where medical data and images such as X-rays, ultrasound, CTs and MRI images with reports can be stored, analyzed, managed and accessible to imaging workplaces. Providing imaging examinations from the cloud to zero footprint viewing applications gives imaging studies wherever they are required. A Cloud-Based PACS, or Cloud PACS, is a PACS system with three important components including an image archiving system, image visualization function, and workflow engine present in the cloud and is available to both users and administrators via Internet-based user interfaces. Cloud PACS offer the advantage of both site and device freedom. For Cloud PACS accessibility the radiologist must need a strong computer terminal and a high-performance network connection. Presently radiologists in imaging centers have total control software and hardware of the devices as well as their IT infrastructure as per their requirement.

However, cloud computing, enable end users to access these IT-associated networks with no understanding or control over the infrastructure that maintains and supports it [45] Additionally cloud-based IT-related networks allows radiology end users to assess expensive hardware as well as software kept remotely at Cloud from distant locations. With aid of cloud computing networks various

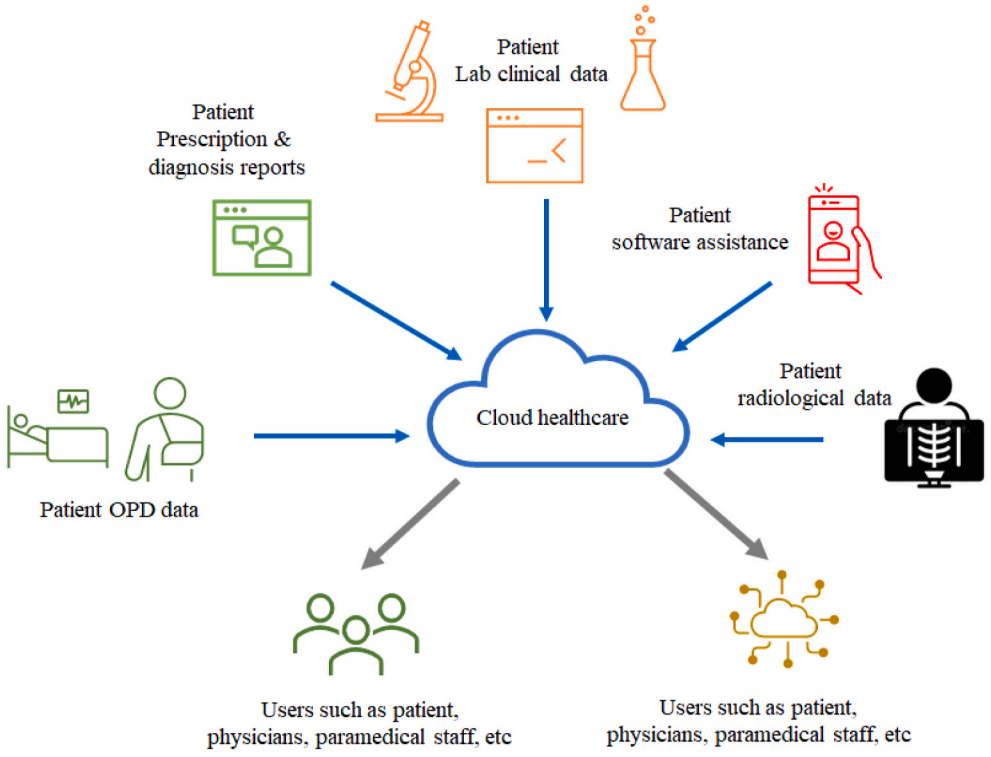

Fig. 4. Typical healthcare cloud.

services like maintenance of device and its regular upgradation can be done remotely by the supplier and different radiology and medical based products can be provided via internet which is termed as software as a service (SaaS)/on-demand software (http://en.wikipedia.org/wiki/Software_as_a_service). Cloud based network offers an interface where several services PACS, remote image analysis application (teleradiology), RIS, innovative 3D-workstation application, as well as invoicing application can be simultaneously used by end users remotely. Additionally, enable admin of radiology centers for actively installation and uninstallation of services or uploading as well as downloading data without affecting software and hardware. Data can be saved securely via regular program upgrades, and any bugs, malware or risks can be monitored as well as resolved remotely. To establish this imaging based virtual cloud radiologists doesn't require costly software and hardware, however, mere single central processing unit would be sufficient (http://www.gartner.com/it/page.jsp?id=707508). This cloud-based E-network enables radiologists to mainly concentrate on their practice as well as dealing with patients without worrying about how the service is processed, hosted, or routed. A typical Cloud computing-based radiology unit flowchart is shown in Fig. 4. Cloud healthcare data enables end users such as physicians, hospitals, patients, paramedical staff etc. and other networks to safely access the patient information and transmit that information safely to improve coordination between the different users and to increase the convenience of the patients.

7.1. Merits of cloud computing in radiology

Understanding related to operating of Cloud systems is important to assist a radiology supervisor to timely diagnose the complications. Radiologists in centers can be assisted from the Cloud by following manner.

➢ Data storage
➢ Improve productivity.
➢ Accessibility of latest software's extra storage when needed.
➢ Remote access to patient data such as billing, insurance, reports
➢ Educational organizations can store investigations, keep files, and perform online assessments.
➢ Teleradiology organizations can provide access control, handle invoicing, and maintain audit track.
➢ Easy access to Radiologists and physicians which can improve their coordination to diagnose complication more correctly.
➢ Reduced expenses on infrastructure owing to a pay-per-use prototype.
➢ Professional agencies, especially suppliers, can maintain systems, improve performance and security.

7.2. Flaws in cloud computing

With the aid of cloud computing patient databases can be stored and protected at all in simulated sections in the storage media to improve the coordination between the users and convenience to access data at different locations. Patient databases can be transmitted and obtained to and from the main server via the internet. That's how different users can access this data safely and conveniently. However, saving data at e-cloud system can possibly increase the data vulnerability to security violation. Following information enlisted below reveals the threats commonly faced in cloud computing with possible explanations to prevent possible risks:

Major concerns are associated with data protection and confidentiality which can be reduced by data encryption while loading, transmit as well as linking with the server by protected URL for example those URLs starting with https.

- Managing data as per the regulatory framework and compliance, audit trail, biometric tests required to allocate regulated access.
- In case of disasters, archive security must be reviewed with the Cloud computing service provider.
- Via maintaining mirror servers, data loss or disruption in services can be avoided due to server failure.
- Image based data and other data with more size require high broadband speed and connectivity which require acquisition with various Internet service providers to avoid interruption of service and improve efficiency.

8. Cloud computing in pharmaceuticals

Cloud computing is the main solution to the problem of scalability as it allows for unlimited scalability as the storage capacity grows. Cloud computing is now being used in almost every industry, from healthcare to education. Cloud computing in healthcare is a relatively new emerging field. The benefits of cloud computing are manifold, including the ability for hospitals, clinics, and medical facilities to store their health records online where they can be accessed anywhere by authorized healthcare providers. The cloud has made electronic medical records accessible from anywhere. This facilitates greater collaboration between providers and forces them to adhere to federal guidelines for sharing patient information. One of the biggest challenges in healthcare is identifying the patient's actual medical condition and accurately identifying the disease, which is not easy due to the large amount of data involved. In addition, the data may be difficult to access, and in some cases, there may be privacy issues. As a result, there is a need for a database system that is secure and reliable. The benefits of using cloud computing include easy management, access, and data protection at anytime, anywhere, faster processing of data, and seamless integration with other cloud-based services. Sensitive, intellectual, unique, and confidential information such as information based on clinical and drug discovery of new therapeutics require assistance of cloud computing to analyze data remotely in a secure manner. On another side structure activity relationship as well as identification of bindings sites of these unique therapeutics also require various computational tools based on quantitative structure-activity relationship (QSAR) and molecular docking. QSAR and molecular docking-based investigations offer an imperative method for

pharmaceutical and medicinal chemists to design and synthesize new drug. Recently software such as Schrödinger's, AutoDock, QSARINS, LQTAgrid, FlexX, VINA, USCF Chimera, Accelrys, CoMFA, CoMSIA, Google Cloud's high-performance computing resources, ICM-Pro, Schrodinger, Discovery Studio, MOE have been used for QSAR and molecular docking. These drug discovery and development-based computer aided drug discovery (CADD) approaches are being used in this work area with numerous plans. During the early stages of drug discovery pipeline, virtual screening is one of the most important used CADD approaches adopted in rational drug design. During virtual screening, the escalating figure of flexible and scalable cloud-based computational programs helps in the screening of large number of molecules. Such programs are planned to conduct virtual screening effectively, to screen lead compounds. With aid of advancement in cloud-based technologies, these lead compounds can be screened via virtual screening effectively using database in form of chemical datasets, libraries, and structure-based or ligand-based data. Also, with continues progress in science, high throughput screening can allow computerized assessment of huge number of compounds against a specific biological target. This part of the drug discovery process allows target detection, target authentication, lead recognition and lead validation resulting in creation of huge data in terabytes. Thus, there is an urgent requirement of cloud-based computing services to store, protect, manage, drill, analyze and provide secure access for this huge data to authorized users. This requires similar software as well as hardware services, while controlling the varying levels of required computational energy. Thus, to overcome this challenge "On-Demand Hardware" and "Software as a Service (SAAS)" are required. On demand computing also known as Cloud Computing which is presently changing the drug discovery research by improving flexibility, speed and efficiency and reduce overall expenses of the process [46].

Acceptance of cloud computing in the healthcare information system has been noticed recently with certain recent reports over establishing an outline for cloud-based E-prescription system by means of cloud computing network. Health insurance portability and accountability act has increased the requirement to implement a secure cloud technology platform. Recently android and a web application have been developed through which a physician can prescribe patients via android application utilizing stylus pen as well as other users including patients, pharmacists, as well as administrators interact with the system via their web accessibility. For such a type of service development integration between cloud computing tools utilizing Arduino as well as electronic-Health sensors and Internet of Things is required. In this service users can use the enrolled IoT tools which enable the healthcare participants, creating services that are more effective, accessible with less chances of errors.

9. Role of E-cloud computing in healthcare sector

Cloud computing has various applications in health care such as patient self-management, medical imaging, hospital management, telemedicine/teleconsultation, public health, and information systems, therapy, and secondary use of data. Timely health checking is important to identify any serious health condition or risk at an early stage. Real-time health intensive care for patients with prolonged health conditions using online telemedicine can be done for offsite diagnoses. This telemedicine based real-time health monitoring can be achieved by using smartphones technology comprising numerous services including location tracking, short message service, GPS and location supported facilities and access of WLAN/GPRS/3G which offers universal connectivity. However, the inconsistencies including calibration, making of false alarms, battery consumption have questioned the proficiencies of smartphone apps in the application of real-time health checking and diagnosis. Alternative to smartphone, intrinsic smartphone sensors as wearable sensors

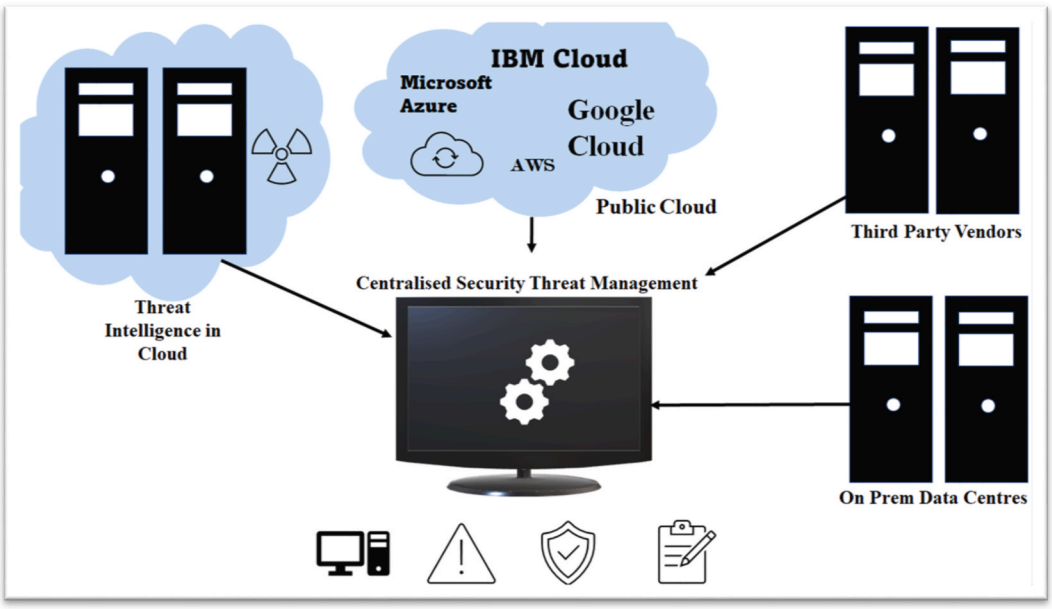

Fig. 5. Centralized security threat management workflow.

device which can be connected to mobile to continuously monitor, store, and share medical information to healthcare givers over distance could be a better solution. These wearable sensors can be used to monitor physiological, biochemical, and motion condition of a patient. Devices such as fitness bands, wirelessly connected devices like blood pressure, real-time electrocardiogram monitor, heart rate monitoring cuffs, glucometer etc. can be used for diseased individuals with prolonged conditions who live at considerable distances from their health service providers. Patients at remote locations can be monitored by integration between real-time health monitoring devices and cloud computing tools. Certain software tools are available in public domain which can be used monitored and analyzed data via cloud services such as ECG data were made available via cloud SaaS [47]. For the accessibility, storage, security one of the well-known services called as Microsoft Azure platform has been employed for a 12-lead ECG telemedicine service [48]. Other cloud computing services in health care such as NETAPP (real-time clinical data) support clinical processes and make them quick as well as more effective, MEDSPHERE (healthcare it services) to make electronic health record platform, CLEARDATA (data protection) guards subtle patient information via agreement protections, develops computerized based healthcare proficiency, NINTEX (automated operations) is robust facilities to healthcare based specialists to reduce paper work and rationalizes manual processes, MEDABLE (teamwork through technology) support clinical applications as well as save healthcare based data, CARECLOUD is a mobile applications which provide better care to patients via practice supervision, E-health archives, patient understanding, healthcare analytics, and profits cycle supervision. Cloud implementation is going to increase rapidly as big companies like Microsoft, Google and Amazon have instantly realized that the majority of hospitals will not continue working with servers that are privately owned as well as controlled. They confirmed their data centers for HIPAA (Health Insurance Portability and Accountability Act of 1996) and safe harbor agreement controls [49]. There are various EHRs (Electronic Health Records) based applications developed recently. Thus, alliance between cloud computing and health care is required (Fig. 5).

- To enhance a host centric healthcare-based operation including virtual care as well as telehealth
- For adherence to medicine
- To overcome drug fabricating as well as theft related practices
- To overcome resource incompetence
- Personal data privacy
- To maintain medical records uniformity
- To improve the data accessibility and storage
- To improve or decline their data storage capacity depending upon the number of patients.
- To access the information remotely, automation of backups and disaster recovery options
- Security and protection of data to fulfil with governing regulations such as Europe's General Data Protection Regulation for the safety of private data, or the US's Health Insurance Portability and Accountability Act for safe data portability, or the HITRUST Alliance's CSF, a commerce-facilitated provable standard for protecting sensitive information.
- Data Interoperability by using wearable devices (IoT-enabled devices) and online health tracking apps, together in Cloud, proved the advantage of data interoperability in healthcare.

Cloud computing allow storage as well as recovery of different health-based data medical images, implementation of picture archive and communication system modules were implemented in a community cloud [49]. These days numerous commercial merchants are intermingling with hospitals as well as healthcare providers to establish healthcare-based cloud computing networks.

Electronic health-based cloud computing network is considered as one of the emerging health care services which can transform the healthcare industry via offering various merits including cost-effective infrastructure, energy saving, fast deployment, flexibility, high speed, resource sharing and scalability [50]. Such type of network is easy to use and can be established easily at any location to enable more coordination, communication, and collaboration between various healthcare services [51]. Advance cloud-based health care system can be used in several healthcare-based services including hospital information systems, medical diagnostic systems, electronic health records, and healthcare monitoring [51]. This type of digital health care platform can provide storage resource assignment and computing technology. The cloud computing market is growing progressively and is likely to be estimated at about US$225 billion by 2020 [52]. Multinational organizations like IBM's Active Health Management and Aetna have established novel clinical data management systems in line with cloud computing structure [53]. Google as well as Microsoft services including Google Health and Microsoft HealthVault have been introduced for storing medical records [54]. Cloud computing systems integrated e-health networks are more suitable due to their responsiveness and portability, cost effectiveness, and can be applied in remote locations [55]. Nevertheless, e-health cloud computing system applications may revolutionize the healthcare industry in the future. (Marcolino et al. [56] investigated potential of e-health services in the management illnesses and showed mixed findings. E-health cloud computing services can improve healthcare service [57], via establishing efficient coordination between patient and health care provider (hospital, physicians, nurses, diagnostic professionals, clinicians, insurance agents) [58].

10. Artificial intelligence and cloud computing in developing medical based robots

With evolution and advancements in artificial intelligence and machine learning, it's now possible to improve patient services by using data so called as big data collected by health care practices. Artificial intelligence and machine learning offers various clinical research benefits by processing big data sets to predict early detection of diseases including cancer. Additionally, integration between wearable devices (e.g. heart rate monitors and fitness trackers) and artificial intelligence allows detection of early-stage heart disease. Further, with the aid of machine learning diagnosis of various complications can be done including big data products such as a data

analytics processor, IBM Watson collected data from medical journals and case studies to predict a patient's diagnosis. A more advanced form of AI to increase our understanding and discover new solutions, DeepMind was introduced by Google to mimic the human brain neural networks. Cloud robotics alliance with artificial intelligence and machine learning in medical science allows computing-based networks to ensure efficient working of robots. Various robots such as Vinci Surgical System for assisting in a variety of minimally invasive procedures; Spot, robotic products, allow patients to connect with others remotely; Ohmni Robot allow patients to safely connect with others; Xenex, light touch based robotic to make hospitals safer for patients and professionals; Heartlander, a small robot, that enters a small opening on the chest to achieve mapping and treatment over the surface of the heart; Care Angel's virtual nurse assistant for interacting with patients to directing patients have been developed by integration between artificial intelligence and machine learning and computing based network.

11. Challenges associated with cloud computing in health care

Cloud-biosecurity is an emerging solution in health care and biomedical filed, which can offer multiple services in the areas of bioinformatics, scientific digital data, patient care, pharmaceuticals, and radiology via controlling all the information through centralized security monitoring and management system in an order to control monitor threats, risks, vulnerabilities according to play books (Fig. 6).

The expanding digitalization of healthcare-based foundations and its rising reliance on internet-based platforms or interfaces has raised concerns related to data privacy and confidentiality. These foundations have been confronted with specific problems such as sensitivity of data, the specificity of networked equipment, the assortment of healthcare professionals (nurses, doctors, administrative staff, and others) and the IT abilities they have. However, apart from efficient services provided by cloud computing in health care, there are some significant challenges associated with cyber security. For an instance most famous instance of a ransomware attack which has badly affected various enterprises globally in May 2017 was the WannaCry outbreak or WannaCry hack in UK troubled almost 200,000 computers in an almost 150 nations. This outbreak resulted in huge financial loss in the UK (£92 million) and worldwide (£6 billion). This has raised serious concern over the involvement of cyber security in all sectors [59].

Even during COVID-19 pandemic apart from its considerable impact over the society and business, the pandemic also increased cyber-crime related incidents which has also badly influenced society and business. This sudden increase in the nature, number and range of cyber-attacks also raised an important concern about how cyber security tools are efficient in dealing with carefully craft and execute cyber-crime campaigns [60]. Recent study also showed the importance of cyber infrastructure (via integration smart devices or internet connected devices) in health care. However cyber infrastructures deal with like challenges like privacy, trust, security, etc. This type of network can build an automatic environment which can be implemented without the interference of human beings in an area like e-healthcare. In this e-healthcare system, these devices built the structure of medical cyber physical system (MCPS), which also face some considerable challenges like attacks (CPS, MCPS, mitigated attacks on same architecture). MCPS has become an important health care system where a network of medical devices is integrated to provide high-quality healthcare. It's an approach which allows the health care system to look after the process automatically and make independent judgments without the need to involve physicians and other medical staff. Due to its close association with patients' safety as well as the considering security of medical devices, mobile edge cloud computing – or fog computing – can be employed to advance the security of MCPS via allowing the implementation and supervision of useful resources into the network edge [61,62]. Recent study also demonstrated a considerable increase in healthcare data breaches. Since healthcare information breaches always involve the more risk of personal health information exposure, corruption or destruction, this area is important to the healthcare field. It was also found that there is a considerable association between organizational attributes and healthcare data breaches [63].

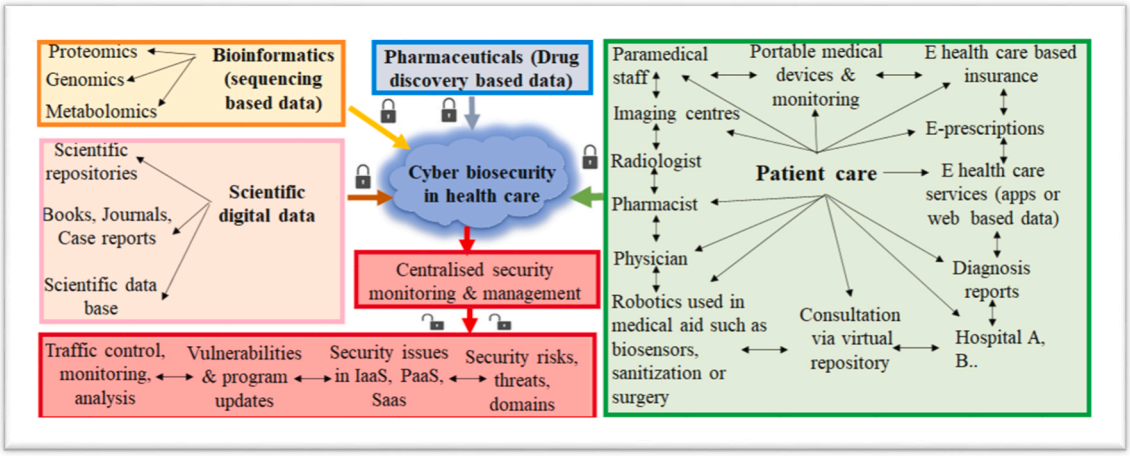

Fig. 6. Logical data flow of cloud biosecurity; Role of cyber biosecurity in bioinformatics, patient care, pharmaceuticals, scientific data management and developing strategies to monitor and manage data flow, vulnerabilities at centralized level.

12. Merits and demerits of cloud computing biomedical sciences and healthcare sector

Presently, biomedical science requires a reliable tool to process large amounts of data in real time with the help of information and communication technologies (ICT). Cloud computing offers numerous advantages for medical and health applications, yet it also presents certain challenges. On the positive side, cloud computing facilitates easy access to medical data and services from anywhere with internet connectivity, enhancing collaboration among healthcare professionals and enabling remote patient monitoring. It promotes scalability, allowing healthcare organizations to adjust resources according to demand, potentially reducing costs and improving efficiency. Moreover, cloud-based storage ensures data backup and disaster recovery, enhancing data security and reliability.

However, cloud computing in healthcare also poses some drawbacks. One concern is data privacy and security, as sensitive medical information stored in the cloud may be vulnerable to breaches or unauthorized access. Compliance with regulations such as HIPAA (Health Insurance Portability and Accountability Act) is crucial but can be challenging in the cloud environment. Additionally, reliance on internet connectivity raises issues of reliability and potential downtime, which could disrupt critical healthcare services. Furthermore, merits and demerits of cloud computing in health and medical applications are mentioned in Table 1. Further clouds could be helpful in saving, handling, protecting, sharing, and making a library of electronic health related documents, laboratory based clinical data system, pharmacy information system, and medical images. However, before discussing the emerging roles of cloud computing in the biomedical sector it's important to know the background of cloud computing. Overall, this cloud platform offers better care to the patients by coordinating with healthcare workers and updating all the information over system timely [64].

13. Conclusion

The integration of cloud computing within the healthcare system and biomedical sciences represents a transformative shift, offering a multitude of advantages that align with the dynamic needs of these fields. Cloud computing's scalability, flexibility, and cost-effectiveness have enabled more efficient data management, enhanced collaborative research, and improved patient care delivery. The PAYG model inherent in cloud services ensures that healthcare and research institutions can access necessary computational resources without the burden of significant upfront investments in IT infrastructure. In healthcare, cloud computing has facilitated the creation and sharing of electronic medical records, supported telemedicine initiatives, and enabled the use of IoT devices for real-time patient monitoring. The synergy between cloud computing and bioinformatics has also been pivotal, allowing for the secure storage and analysis of large-scale genomic, proteomic, and metabolomic data, which is crucial for advancing personalized medicine. However, alongside these benefits, the manuscript acknowledges the challenges and risks associated with cloud computing, particularly in cybersecurity. The sensitivity of health-related data necessitates robust security measures to protect against breaches, unauthorized access, and cyber-attacks. The development of cloud biosecurity strategies is essential to safeguard the integrity and confidentiality of medical and scientific data. In conclusion, cloud computing has emerged as an indispensable tool in the health care system and

Table 1
Merits and demerits of Cloud computing are summarized.

Cloud computing	
Merits	Demerits
➢ Eco-friendly, automated, cost effective and a novel approach. ➢ Low manpower requirement with more elasticity and scalability. ➢ Efficient in offering quick solutions and access. ➢ Helps in connecting users at distant places. ➢ Outdated features of the application can be updated with an advanced version. ➢ Patients and his related queries can be addressed at central level. ➢ Big data based on radiographical images can be stored, managed and analyzed from distant places. ➢ If lost data can be retrieved from the central level or repositories ➢ Can be accessed from portable smart devices. ➢ Chemical as well as biological data can be analyzed with more accuracy. ➢ Clinical data can be monitored live. ➢ Storage and accessibility of data at different locations can be done. ➢ Physiological signals can be monitored by using biosensors and bio-medical instrumentation. ➢ Artificial organs can be monitored. ➢ Radiological data can be processed. ➢ Analogue information in the form of a repetitive signal such as electrocardiogram can be monitored. ➢ Chemical, genetic, clinical and patient data analysis.	➢ Expense of execution and maintenance of whole system. ➢ It's difficult reassemble fragmented data depending upon the algorithm set for respective. ➢ Absence of regulations/laws requiring the use and protection of electronic health care. ➢ Absence of e-Health Cloud design and development standards. ➢ Changes in cloud provider always make data more insecure especially personal identification information data, as risks of existence of previous data with previous cloud provider is always there. ➢ Challenges associated Hybrid multiple cloud such as interdependency.

biomedical sciences, driving innovation and efficiency. As technology continues to evolve, it is imperative to address the cybersecurity challenges to fully harness the potential of cloud computing in advancing healthcare and scientific discovery.

Data availability statement

All the data is included in this review.

CRediT authorship contribution statement

Sonali Sachdeva: Writing – review & editing, Writing – original draft, Validation, Formal analysis, Data curation, Conceptualization. **Saurabh Bhatia:** Writing – review & editing, Supervision, Project administration, Funding acquisition, Conceptualization. **Ahmed Al Harrasi:** Validation, Supervision, Resources. **Yasir Abbas Shah:** Writing – original draft, Visualization, Methodology, Formal analysis, Data curation. **Khalid Anwer:** Validation, Methodology, Formal analysis. **Anil K. Philip:** Resources, Software, Supervision. **Syed Faisal Abbas Shah:** Methodology, Investigation, Conceptualization, Formal analysis, Writing – original draft. **Ajmal Khan:** Validation, Visualization, Writing – review & editing. **Sobia Ahsan Halim:** Project administration, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Sobia Ahsan Halim reports administrative support was provided by University of Nizwa. Sobia Ahsan Halim reports a relationship with University of Nizwa that includes: employment. Not applicable If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Sobia Ahsan Halim is currently associated with Heliyon as an Associate Editor for Section Pharmaceutical Sciences.

References

[1] C. Duane, Cloud computing History 101 (2010).
[2] Q. Yan, F.R. Yu, Distributed denial of service attacks in software-defined networking with cloud computing, IEEE Commun. Mag. 53 (4) (2015) 52–59.
[3] A. Patel, et al., Taxonomy and proposed architecture of intrusion detection and prevention systems for cloud computing, in: International Symposium on Cyberspace Safety and Security, Springer, 2012.
[4] N. Roy, A. Dubey, A. Gokhale, Efficient autoscaling in the cloud using predictive models for workload forecasting, in: 2011 IEEE 4th International Conference on Cloud Computing, IEEE, 2011.
[5] J. Haskew, et al., Implementation of a cloud-based electronic medical record for maternal and child health in rural Kenya, Int. J. Med. Inf. 84 (5) (2015) 349–354.
[6] C. He, X. Fan, Y. Li, Toward ubiquitous healthcare services with a novel efficient cloud platform, IEEE (Inst. Electr. Electron. Eng.) Trans. Biomed. Eng. 60 (1) (2012) 230–234.
[7] S.-L. Wang, et al., Design and evaluation of a cloud-based Mobile Health Information Recommendation system on wireless sensor networks, Comput. Electr. Eng. 49 (2016) 221–235.
[8] E.-M. Fong, W.-Y. Chung, Mobile cloud-computing-based healthcare service by noncontact ECG monitoring, Sensors 13 (12) (2013) 16451–16473.
[9] P. Sarosh, et al., A security management framework for big data in smart healthcare, Big Data Research 25 (2021) 100225.
[10] K. Antypas, S.C. Wangberg, An Internet-and mobile-based tailored intervention to enhance maintenance of physical activity after cardiac rehabilitation: short-term results of a randomized controlled trial, J. Med. Internet Res. 16 (3) (2014) e3132.
[11] R. Patan, et al., Smart healthcare and quality of service in IoT using grey filter convolutional based cyber physical system, Sustain. Cities Soc. 59 (2020) 102141.
[12] S. Mansfield-Devine, Leaks and ransoms–the key threats to healthcare organisations, Netw. Secur. 2017 (6) (2017) 14–19.
[13] M.R. Cheung, Lack of health insurance increases all cause and all cancer mortality in adults: an analysis of National Health and Nutrition Examination Survey (NHANES III) data, Asian Pac. J. Cancer Prev. APJCP 14 (4) (2013) 2259–2263.
[14] E. Haggerty, Healthcare and digital transformation, Netw. Secur. 2017 (8) (2017) 7–11.
[15] S. Arshad, et al., Analysis of security and privacy challenges for DNA-genomics applications and databases, J. Biomed. Inf. 119 (2021) 103815.
[16] A.J. Hung, et al., Telementoring and telesurgery for minimally invasive procedures, J. Urol. 199 (2) (2018) 355–369.
[17] V. Navale, P.E. Bourne, Cloud computing applications for biomedical science: a perspective, PLoS Comput. Biol. 14 (6) (2018) e1006144.
[18] H. Bhaskar, D.C. Hoyle, S. Singh, Machine learning in bioinformatics: a brief survey and recommendations for practitioners, Comput. Biol. Med. 36 (10) (2006) 1104–1125.
[19] D. Farbiash, R. Puzis, Cyberbiosecurity: DNA injection attack in synthetic biology, arXiv preprint arXiv 2020 (2011) 14224.
[20] D.S. Himmelstein, et al., *Sci-Hub provides* access *to nearly all scholarly literature*, Elife 7 (2018) e32822.
[21] D.A. Benson, et al., GenBank, Nucleic Acids Res. 33 (suppl_1) (2005) D34–D38.
[22] H. Sugawara, et al., DDBJ with new system and face, Nucleic Acids Res. 36 (suppl_1) (2007) D22–D24.
[23] T. Barrett, et al., NCBI GEO: archive for high-throughput functional genomic data, Nucleic Acids Res. 37 (suppl_1) (2009) D885–D890.
[24] M. Shumway, G. Cochrane, H. Sugawara, Archiving next generation sequencing data, Nucleic Acids Res. 38 (suppl_1) (2010) D870–D871.
[25] C. Brooksbank, et al., The European Bioinformatics Institute's data resources, Nucleic Acids Res. 31 (1) (2003) 43–50.
[26] M. Kapushesky, et al., Gene expression atlas at the European bioinformatics institute, Nucleic Acids Res. 38 (suppl_1) (2010) D690–D698.
[27] P. Flicek, et al., Ensembl's 10th year, Nucleic Acids Res. 38 (suppl_1) (2010) D557–D562.
[28] B. Rhead, et al., The UCSC genome browser database: update 2010, Nucleic Acids Res. 38 (suppl_1) (2010) D613–D619.
[29] J. Taylor, et al., Using galaxy to perform large-scale interactive data analyses, Current protocols in bioinformatics 19 (1) (2007) 10, 5. 1-10.5. 25.
[30] S.R. Engel, et al., Saccharomyces Genome Database provides mutant phenotype data, Nucleic Acids Res. 38 (suppl_1) (2010) D433–D436.
[31] L.D. Stein, The case for cloud computing in genome informatics, Genome Biol. 11 (5) (2010) 1–7.
[32] J.G. Reid, et al., Launching genomics into the cloud: deployment of Mercury, a next generation sequence analysis pipeline, BMC Bioinf. 15 (1) (2014) 1–11.
[33] E. Afgan, et al., Harnessing cloud computing with galaxy cloud, Nat. Biotechnol. 29 (11) (2011) 972–974.
[34] A.P. Heath, et al., Bionimbus: a cloud for managing, analyzing and sharing large genomics datasets. Journal of the American Medical Informatics Association 21 (6) (2014) 969–975.
[35] B. Langmead, A. Nellore, Cloud computing for genomic data analysis and collaboration, Nat. Rev. Genet. 19 (4) (2018) 208–219.

[36] D.N. Perkins, et al., Probability-based protein identification by searching sequence databases using mass spectrometry data, ELECTROPHORESIS: Int. J. 20 (18) (1999) 3551–3567.
[37] A. Weiss, Computing in the clouds, networker 11 (4) (2007) 16–25.
[38] A. Keller, et al., Empirical statistical model to estimate the accuracy of peptide identifications made by MS/MS and database search, Anal. Chem. 74 (20) (2002) 5383–5392.
[39] L. Käll, et al., Semi-supervised learning for peptide identification from shotgun proteomics datasets, Nat. Methods 4 (11) (2007) 923–925.
[40] Z.-Q. Ma, et al., IDPicker 2.0: Improved protein assembly with high discrimination peptide identification filtering, J. Proteome Res. 8 (8) (2009) 3872–3881.
[41] J. Park, et al., Informed-Proteomics: open-source software package for top-down proteomics, Nat. Methods 14 (9) (2017) 909–914.
[42] J.K. Eng, T.A. Jahan, M.R. Hoopmann, Comet: an open-source MS/MS sequence database search tool, Proteomics 13 (1) (2013) 22–24.
[43] A.-C. Gavin, et al., Functional organization of the yeast proteome by systematic analysis of protein complexes, Nature 415 (6868) (2002) 141–147.
[44] K. Peters, et al., PhenoMeNal: processing and analysis of metabolomics data in the cloud, GigaScience 8 (2) (2019) giy149.
[45] D. Krissi, Distinguishing Cloud Computing from Utility Computing, Ebizq. net, 2008. Retrieved from.
[46] V. Garg, S. Arora, C. Gupta, Cloud computing approaches to accelerate drug discovery value chain, Comb. Chem. High Throughput Screen. 14 (10) (2011) 861–871.
[47] S. Pandey, et al., An autonomic cloud environment for hosting ECG data analysis services, Future Generat. Comput. Syst. 28 (1) (2012) 147–154.
[48] J.-c. Hsieh, M.-W. Hsu, A cloud computing based 12-lead ECG telemedicine service, BMC Med. Inf. Decis. Making 12 (1) (2012) 1–12.
[49] L.A.B. Silva, C. Costa, J.L. Oliveira, A PACS archive architecture supported on cloud services, Int. J. Comput. Assist. Radiol. Surg. 7 (3) (2012) 349–358.
[50] O. Ali, et al., Cloud computing-enabled healthcare opportunities, issues, and applications: a systematic review, Int. J. Inf. Manag. 43 (2018) 146–158.
[51] G. Aceto, V. Persico, A. Pescapé, Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0, Journal of Industrial Information Integration 18 (2020) 100129.
[52] S. Shamshad, et al., A secure blockchain-based e-health records storage and sharing scheme, J. Inf. Secur. Appl. 55 (2020) 102590.
[53] T.S. Behrend, et al., Cloud computing adoption and usage in community colleges, Behav. Inf. Technol. 30 (2) (2011) 231–240.
[54] S.-C. Chang, et al., Evaluating the E-Health Cloud Computing Systems Adoption in Taiwan's Healthcare Industry. Life 11 (4) (2021) 310.
[55] M. Nobakht, et al., PGFit: Static permission analysis of health and fitness apps in IoT programming frameworks, J. Netw. Comput. Appl. 152 (2020) 102509.
[56] M.S. Marcolino, et al., The impact of mHealth interventions: systematic review of systematic reviews, JMIR mHealth and uHealth 6 (1) (2018) e8873.
[57] S. Kumar, et al., Mobile health technology evaluation: the mHealth evidence workshop, Am. J. Prev. Med. 45 (2) (2013) 228–236.
[58] S. Krishnan, S. Lokesh, M.R. Devi, An efficient Elman neural network classifier with cloud supported internet of things structure for health monitoring system, Comput. Network. 151 (2019) 201–210.
[59] A. Hockey, Uncovering the cyber security challenges in healthcare, Netw. Secur. 2020 (4) (2020) 18–19.
[60] H.S. Lallie, et al., Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Comput. Secur. 105 (2021) 102248.
[61] A.H. Celdrán, et al., Sustainable securing of medical cyber-physical systems for the healthcare of the future, Sustainable Computing: Informatics and Systems 19 (2018) 138–146.
[62] M.M. Nair, A.K. Tyagi, R. Goyal, Medical cyber physical systems and its issues, Procedia Comput. Sci. 165 (2019) 647–655.
[63] A. McLeod, D. Dolezel, Cyber-analytics: Modeling factors associated with healthcare data breaches, Decis. Support Syst. 108 (2018) 57–68.
[64] V. Sobeslav, et al., Use of cloud computing in biomedicine, J. Biomol. Struct. Dyn. 34 (12) (2016) 2688–2697.