TUNKU ABDUL RAHMAN
UNIVERSITY COLLEGE

BEYOND EDUCATION

TUNKU ABDUL RAHMAN UNIVERSITY COLLEGE

Faculty of Computing and Information Technology

A Review on Cloud Computing and its Application in Healthcare: IoT, Data Management, Security, Reliability, Energy Efficiency

Bachelor of Computer Science (Honours) in Software Engineering and Bachelor of Computer Science (Honours) in Data Science

Assignment (Part 1)

BAIT3273 Cloud Computing

2021

Name (Block capital)	Registration No.
FOONG GAH SENG	20WMR09451
KONG MUN JUN	20WMR08867
NELSON ENG YONG CHUENG	20WMR09499
LIM YIH FENG	20WMR08880
LEE JUN XIAN	20WMR08873

Grading Rubric for Written Assignments

Levels of Assessment

Criteria	Inadequate=D	Adequate=C	Above Average=B	Exemplary=A
Marks	**1 - 3% (Poor)**	**4 - 6% (Average)**	**7 - 8% (Good)**	**9 - 10% (Excellent)**
Organization	Writing lacks logical organization. It shows some coherence but ideas lack unity. Serious errors.	Writing is coherent and logically organized. Some points remain misplaced and stray from the topic. Transitions evident but not used throughout essay.	Writing is coherent and logically organized with transitions used between ideas and paragraphs to create coherence. Overall unity of ideas is present.	Writing shows high degree of attention to logic and reasoning of points. Unity clearly leads the reader to the conclusion and stirs thought regarding the topic.
Level of Content	Shows some thinking and reasoning but most ideas are underdeveloped and unoriginal.	Content indicates thinking and reasoning applied with original thought on a few ideas.	Content indicates original thinking and develops ideas with sufficient and firm evidence.	Content indicates synthesis of ideas, in-depth analysis and evidences original thought and support for the topic.
Development	Main points lack detailed development. Ideas are vague with little evidence of critical thinking.	Main points are present with limited detail and development. Some critical thinking is present.	Main points well developed with quality supporting details and quantity. Critical thinking is weaved into points	Main points well developed with high quality and quantity support. Reveals high degree of critical thinking.
Grammar & Mechanics	Spelling, punctuation, and grammatical errors create distraction, making reading difficult; fragments, comma splices, run-ons evident. Errors are frequent.	Most spelling, punctuation, and grammar correct allowing reader to progress though essay. Some errors remain.	Essay has few spelling, punctuation, and grammatical errors allowing reader to follow ideas clearly. Very few fragments or run-ons.	Essay is free of distracting spelling, punctuation, and grammatical errors; absent of fragments, comma splices, and run-ons.
Style	Mostly in elementary form with little or no variety in sentence structure, diction, rhetorical devices or	Approaches college level usage of some variety in sentence patterns, diction, and rhetorical devices.	Attains college level style; tone is appropriate and rhetorical devices used to enhance content; sentence	Shows outstanding style going beyond usual college level; rhetorical devices and tone used effectively; creative use of sentence structure and coordination

	emphasis.		variety used effectively.	
Format	Fails to follow format and assignment requirements; incorrect margins, spacing and indentation; neatness of essay needs attention.	Meets format and assignment requirements; generally correct margins, spacing, and indentations; essay is neat but may have some assembly errors.	Meets format and assignment requirements; margins, spacing, and indentations are correct; essay is neat and correctly assembled.	Meets all formal and assignment requirements and evidences attention to detail; all margins, spacing and indentations are correct; essay is neat and correctly assembled with professional look.

Levels of Assessment (Communication Skills)

Criteria	**Inadequate=D (Poor)**	**Adequate=C (Average)**	**Above Average=B (Good)**	**Exemplary=A (Excellent)**
Organization	Audience cannot understand presentation because of poor organization; introduction is undeveloped or irrelevant; relation to the rest of the team's presentation is unclear.	Audience has difficulty following presentation because of some abrupt jumps; some of the main points are unclear or not sufficient stressed;	Satisfactory organization; clear introduction; main points are well stated, even if some transitions are somewhat sudden; relation to the rest of the team's presentation clear.	Superb organization; builds on and provides support for the rest of the team's presentation; main points well stated and argued, with each leading to the next point of the talk.
Contact Mechanics	Slides seem to have been cut-and pasted together haphazardly at the last minute; numerous mistakes; speaker not always sure what is coming next;	Boring slides; no glaring mistakes but no real effort made into creating truly effective slides;	Generally good set of slides; conveys the main points well;	Very creative slides; carefully thought out to bring out both the main points of this part of the presentation as well as the relation to the rest of the team presentation; maintains audience interest throughout.
Delivery				

	Mumbles the words, audience members in the back can't hear anything; too many filler words; distracting gestures;	Low voice, occasionally inaudible; some distracting filler words and gestures; articulation mostly, but not always, clear;	Clear voice, generally effective delivery; minimal distracting gestures, etc., but somewhat monotone;	Natural, confident delivery that does not just convey the message but enhances it; excellent use of volume, pace etc.
Relating to audience	Reads most of the presentation from the slides or notes with no eye contact with audience members; seems unaware of audience reactions;	Occasional eye contact with audience but mostly reads the presentation; some awareness of at least a portion of the audience; only brief responses to audience questions;	Generally aware of the audience reactions; maintains good eye contact when speaking and when answering questions;	Keeps the audience engaged throughout the presentation; modifies material on-the-fly based on audience questions and comments; keenly aware of audience reactions.

Acknowledgement

This work is in part by Tunku Abdul Rahman University College under the subject of BAIT3273 Cloud Computing. We would like to provide our gratitude to our tutor, Mr. Low Choon Keat who provides suggestions to our assignment. We also would like to acknowledge our appreciation to our faculty for providing facilities such Library Online Databases and Google Scholar which provide us the permissions to access all the resources to achieve our works. A special thanks to all the teammates that cooperate to complete the research paper review and to our friends that provide suggestions.

Table of Contents

Abstract

In the era of Industrial Revolution 4.0, Cloud computing became the modern approach to efficiently delivering IT services. Cannot be denied that cloud technology did improve the quality of services in every industry, including healthcare and with the assistance of the Internet of Things, Cloud computing techniques developed rapidly to contribute to various health examination instruments. Therefore, various challenges needed to be faced when implementing or enhancing cloud computing techniques. Challenges such as medical decision-making, cloud service providers' data security, ensuring the reliability of the services. In this paper, we will be reviewing the current work that has been done on the application of cloud computing in healthcare. Hence, Efficiency of Internet of Things, Data Management, Security, Reliability, and Energy Efficiency of Cloud Computing will be made to compare the problem statement, techniques, data, and application of past research.

Keywords

Cloud computing, Data Management, Energy Efficiency, Internet of Things, Security, Reliability

1. Introduction

Cloud computing and health monitoring has been integrated properly together with the healthcare's equipment to provide a proper monitoring and collection of patient health records. In recent years, cloud computing was being used in various fields such as life stock, education, military, gaming, agriculture and healthcare. Services provided under cloud computing by the IT industry were Software as the Service(SaaS), Platform as a Software(PaaS) and Infrastructure as a Service(IaaS). These services were more functional than the traditional way. There are a lot of companies that provide cloud services such as NetApp that provide current clinical data, Medsphere that provide cloud-based answers for medical services establishment and others [1]. Other than cloud computing, the Internet of Things (IoT) has developed rapidly in recent years**.** IoT supports connections between smart devices and the sensors for data exchange between them. The rapid development of cloud computing and IoT has improved healthcare in patient safety, satisfaction of staff and operational efficiency in the medical industry. The adoption of the rapid development in IoT and cloud computing allows patient's health information to be streamed to caregivers in real time [2].

Energy Efficient in Cloud Computing

The energy consumption is increasing in cloud data centres day by day while the majority of the energy is used by the physical machines that host the virtual machines (VMs). Thus, it is important to manage the VMs that are not required and will need to put on sleep. Virtualization features allow running and managing multiple VMs on a single host to improve service management, resource utilization and saving cost [3]. It is important to reduce energy consumption with resources increasing day-by-day to operate businesses while able to save cost and provide better services from cloud computing.

Data Management

The task of data management in the healthcare sector is a gargantuan duty [6]. Every patient's information such as personal info, medical condition and medical history are needed to be stored individually and carefully from the sight of the public and convenient themselves to utilize the data in the future. Merging healthcare systems with cloud computing then became the preferable choice for better implementation as cloud computing technologies are much more flexible, energy saving, cheap, and fast deploying that can be beneficial for every industry and organizations [6]. However, maintenance of the quality of data and security of data are yet being explored to enhance the technology of cloud computing in data management. Therefore, to overcome these issues, industries need to implement proper management of data and

Security

Regardless of the infrastructure in use, data is at the top of the list when it comes to IT security risks. Cloud Computing is no exception, and because of its dispersed nature and multi-tenant architecture, it focuses on additional security considerations. The

Internet of Things plays an emerging role in all the fields such as making an ordinary city into a smart city, transportation region as an IoT enabled transportation field, hospital management turning into an e-healthcare system etc. It is also agreed that anyplace there are sensors to collect, process and store the information then there stands an IoT.

The purpose is to reveal the state of research and the assessment of expectations of cloud services in the health industry, which is absolutely increasing, and the advantages are surprisingly visible worldwide.

In the healthcare system, recent research development is to discuss numerous sensors that are set up in a human body to anticipate the heartbeats, blood pressure and variation in functioning of human body parts. The Internet of Things (IoT) is an organization of connected preparing devices, mechanical and propelled machines, things, animals or people that are given different identifiers and the capability to move data over a framework without assuming human-to-human or human-to-PC collaboration. Cloud computing and health monitoring is continuously being

cloud computing to cope with an ample amount of data and improve the analytics.

development, storage, use, dissemination, and destruction of data are all part of the data life cycle. Appropriate security measures must be taken to prevent unauthorised access to another person's data. Customers should also be able to see and audit the data backups that are employed to avert data loss. (Srijita Basu, 2018)

Internet of Things

engaged together as the healthcare equipment is giving appropriate monitoring and collection of the patient health record is being sent and collected using cloud computing services like SaaS which stands for storage as a service.

Reliability

Cloud computing has been beginning to extend and dominate all kinds of systems, including the ones that are part of the critical infrastructure and even just a very small system [5]. With it extending and becoming more and more popular, the measuring of reliability of cloud computing is becoming more and more difficult. Most of the assumptions about reliability of cloud computing can only be observed by users instead of being measured because the details of use of cloud computing and its infrastructure and hardware performance are hidden away from the consumer. Therefore, there are a lot of papers tackling the issue of measuring the reliability of cloud computing with many approaches and models.

2. Literature Review

2.1 Energy Efficiency

Energy Efficient Techniques

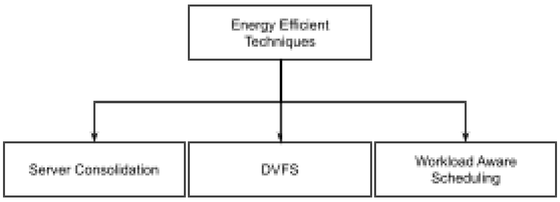

Figure 1: Energy Efficient Techniques

Consumption of energy in cloud computing is one of the major issues specifically for data centers. We will review the strategies for energy optimization in cloud data centers. There are few techniques to reduce the energy consumption in cloud computing as shown in Figure 1.

Server Consolidation

Server consolidation is one of the energy efficiency techniques by accumulating the workload of physical machines while turning off the remaining of the server machines. Low stacked PC frameworks are virtualized and will run in multiple physical machines but underloaded virtual machines (VM) will be migrated manually to one physical server. Server consolidation can be categorized into two migration techniques, regular migration and live migration [8]. The main strategy is to move VM from one host to another while delaying the initial utilized server. However, continuing on the target server while duplicating memory from the original server. The live migration techniques perform the same as the main strategy but do not need to stop the server. [9]

Dynamic Voltage Frequency Scaling (DVFS)

DVFS is an energy optimization dynamic technique to manage the power and mainly to reduce power consumption. DVFS basically adjusts the power and frequency settings of the computing devices to optimize the resource while maximizing the power savings when resources are not required. DVFS techniques are used in physical machines that host VMs together with the algorithm or the scheduling mechanism to reduce energy used by managing the power consumption of multicore processors, DRAM memories and other components. [12]

Workload Aware Scheduling

Nowadays, server farms have an expansive number of servers and when allocating heat the workload on a particular server would affect the heat dissemination and power utilization. Thus, workload aware scheduling is scheduling the incoming of the workload on the basis of the workload with appropriate resources. However, additional warmth dispersal of physical machines would expand the temperature in the data centre and extra cooling is necessary when inappropriate arrangement of the resources. [15] In this matter, we will review the workload aware scheduling techniques used to reduce energy consumption which results in energy efficiency for the cloud data centre.

Energy Efficiency for Cloud Computing in Healthcare Service

In recent years, cloud computing has become popular in Healthcare Service (HCS) applications. It is because cloud computing was capable of providing various medical services applications through cloud storage and a broad range of network resources delivered to customers [3]. Time delay for HCS stakeholder who run the medical demands in a cloud environment is one of the major challenges.

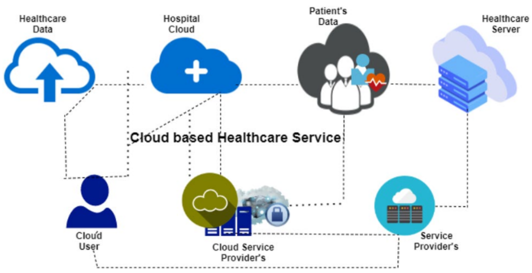

Figure 2: Cloud deployment for healthcare

In Prathap, R., Mohanasundaram, R [17], the author used the VM, Parallel Particle Swarm Optimization (PPSO) algorithm to improve the optimization model in cloud computing with the HCS system. The author proposed four components which are stakeholder devices, stakeholder requests, cloud broker and network administrator for the optimization model for the VMs. While the PPSO algorithm is proposed to be used in the model to set optimum VM selection. The author compared the proposed model with state-of-the-art model, the result posed a significant time execution and system performance in real time recovery improvements.

2.2 Data Management

Data management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively [18]. Whereas the process of data management is a technique that ensures the reliability of the indispensable data when the data is storing, validating, and processing. In this Cenozoic era, almost every industry deals with huge amounts of data which increases the urge for data management assistance. According to Kuceba and Chmielarz, data management is an important factor to ensure the security and viability of data for any organization as it assists in the growth of the organization [19]. Data management also helps the industries and organizations in taking care of the matter of data security which is vital protection for data and information when it involves private and confidential data. In the year of achieving Industrial Revolution 4.0, Various data management platforms and software have been offering enterprises and organizations a 360-degree view of stakeholders with a critical insight edge [6]. See (Figure 3).

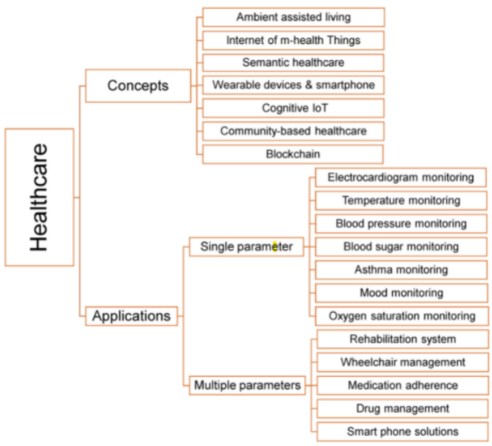

Figure 3: Classification of Healthcare sector.

In order to handle a plentiful amount of data, any industry or organization needs to ensure that they are managing well with the structured data as well as unstructured data [21]. According to Brous et al., data management can be beneficial for the industries in order to mobilize the power of the data and personalize the experiences [21]. With proper management of data in healthcare organizations, it can be amicable as it is able to provide more insightful value to the interactions with stakeholders [21]. In addition, proper data management also enables higher-level management to identify the root causes of the misfiring in split seconds and make quick decisions or necessary steps regarding that. Thus, with the proper implication of data management platforms in big industries or business organizations, customer engagement systems can be improved and provide a big help in harnessing the business [21].

Implementation of Cloud Computing

With the assistance of the internet, various applications and tools can be used to allow cloud computing in delivering different components. As mentioned by Amron et al., cloud computing is a tremendously useful application that can help any organization in long-term cost-saving and easy accessibility of data [22]. Therefore, managing an ample amount of data in a limited time can be one of the economic steps to be taken by any industry and organization. In order to chase up the trend of the economic situation, many organizations start to prefer using cloud computing technology for the cost and user-friendly access of details. Not only cost efficiency is the main advantage of cloud computing but also the speed of time provides useful information and knowledge for the organization from the service provided by cloud computing with just a mouse click [23]. Cannot be denied that by using cloud computing, information from all sorts of resources can be given and pressure from capacity planning can be taken off. Cloud computing can also be beneficial for the global scale as it can be able to provide scale elasticity [24]. See (Figure 4).

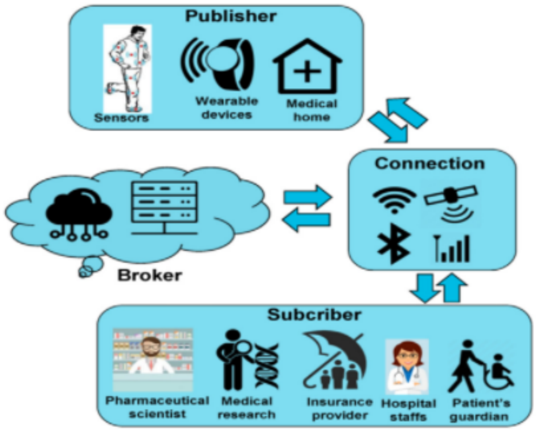

Figure 4: Topology of IoT framework for the healthcare sector.

Undeniably, cloud computing's productivity and its implementation are its greatest benefits, hence, cloud computing is very beneficial to every different sector as it helps the sectors to cope up with expansive amounts of data and its storage concerns [22](Amron, 2017). As per Amron et al., cloud computing can be implemented in various sectors such as the health sector, education sector, genomic projects for its usefulness and cost-friendly nature [22]. Various proper implementations in cloud computing are truly helpful for different sectors as the implementation of cloud computing can reduce the expenses regarding Information Technology(IT) for an organization as well as its cost for upgraded software and hardware services. See (Figure 5).

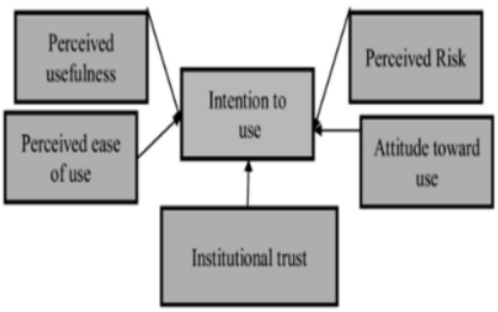

Figure 5: Cloud computing solution conceptual model

2.3 Security

Challenges of cloud computing security

Cloud computing service providers (CCSP) are always at danger of performance degradation. Users can rent computing capabilities using cloud computing infrastructure for a fraction of the expense of setting up and maintaining expensive hardware and software systems. The Internet's ubiquity and widespread reliance have created a slew of problems. The challenges of security and performance are particularly important. Clients dread policies that are hidden from them, according to Khorshed et al. Gaps in Cloud computing are defined as trust difficulties between customers and Cloud providers.Virtualization/multi-tenancy vulnerabilities, Internet protocol vulnerabilities, unauthorised access to management interface, injection vulnerabilities, and vulnerabilities in browsers and APIs are all major vulnerabilities in Cloud computing that can pose substantial dangers. (Umer Ahmed Butt, 2020)

These flaws have ramifications, such as permitting network assaults, providing intruders access control, allowing unwanted service access, and exposing private data. All of these flaws expose Cloud to risks, whether directly or indirectly, such as in the workplace. Changes in a business model that can obstruct the use of Cloud computing services, abusive use of Cloud computing, unsecured interfaces and API, malevolent insiders, data loss and leakage, service hijacking, and an unknown risk profile are just a few of these dangers. The assaults that can be conducted must be discovered and understood in order to protect the Cloud from those threats and prevent any damage. Denial of Service (DoS) assaults, zombie attacks, and phishing attempts are among the most commonly cited attacks in Cloud computing. There are currently many open problems in cloud computing security that should be addressed by cloud providers in order to convince end-users to use the technology. [2]

The most important concern is to guarantee that user data integrity and confidentiality is attained while they are stored in the cloud systems.It's impossible for an end-user to even establish what security methods are applied to data in the Cloud when there's a long, opaque supplier chain. [28]

Denial of service

Distributed denial-of-service (DDoS) is one of the most well-known and important cyberattacks today. It poses a significant threat to the current Internet community due to its simple yet incredibly potent attack techniques. From figure 6, we can see that the goal of DDoS assaults is to cause this disruption to the targeted users, who are referred to as "victims." [30]

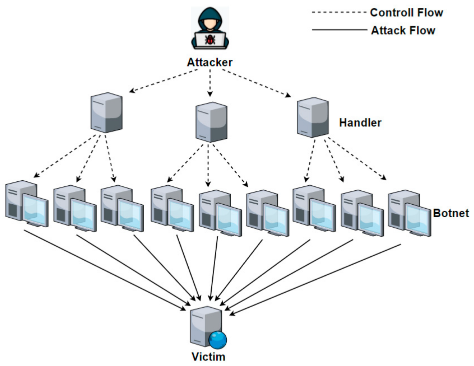

Figure 6: Flow of DDoS attacks

A DDoS attack, in general, seeks to prevent legitimate users from accessing a target system or service by overwhelming the resources. Attackers leveraging Internet apps or network layer services and protocols, for example, consume victims' networks or processing resources with a massive flood of packets. As a result, the victims' networks or processing capacities were unable to function normally, denying them services. Furthermore, if a thorough mitigation mechanism is not used, a DDoS victim may lose all or part of its services and files. A long-held idea that hackers may easily compromise as many computers as they desire has been disproved by recent study.Despite the fact that the number of bot footprints may be substantially larger, the number of active bots a botmaster can operate is limited to the hundreds or thousands due to anti-virus and anti-malware effort and software. [30]

Security of cloud computing in healthcare

The healthcare system is currently one of the application domains in IoT that has piqued the interest of industry, academia, and government. In the medical industry, the rise of IoT and cloud computing is enhancing patient safety, staff happiness, and operational efficiency. [29]

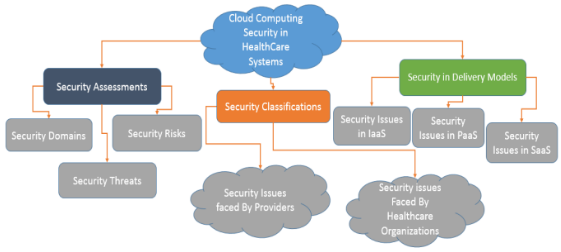

Figure 7: Cloud computing in HealthCare

Cloud computing provides the benefit of allowing health care providers, caregivers, and patients to communicate information in a more structured and organised manner, lowering the risk of medical records being lost. Healthcare services and apps have benefited from technological advancements such as Cloud Computing. It guards against DDoS attacks, for example. DDoS assaults are on the rise, and a top cloud computing security strategy is around tactics that prevent massive amounts of traffic from reaching a company's cloud servers. In this age of ever-increasing data breaches, a top cloud computing security arrangement has security standards in place to ensure sensitive data and exchanges are safeguarded. [27]

2.4 IoT Cloud Computing

Internet of Things and Cloud Computing for Healthcare 4.0

Healthcare proved to be among the most attractive areas for IoT application [39,38]. The accomplishment of this paradigm is refurnishing modern healthcare, with promising technological, economic, and social prospects: IoT is absolute the main enabler for distributed healthcare applications, thus giving an iconic contribution to the overall and decrease of healthcare costs while increasing the health outcomes,

For instance, IoT enables scenarios where smart devices connect with other smart objects in order to gain new knowledge and attention about both users and the environment for supporting decisions [40]. Inspired by the prime IoT paradigm, a number of varieties have been derived in the health field, each with its particularity. See (Table 1).

Table 1
Internet of Things paradigms in Healthcare.

IoT Paradigm		Year	Ref.
Internet of Medical Things	(IoMT)	2017	[45]
Internet of Health Things	(IoHT)	2016	[41]
Internet of Nano Things	(IoNT)	2015	[2]
Wearable Internet of Things	(WIoT)	2014	[44]
Internet of m-health Things	(m-IoT)	2011	[46]

"Cloud Computing" is a model that enables "Utility Computing", i.e. the leasing of computing resources (computational power, storage, and the related networking resources) in real-time, with minimal interaction with the provider.

However, several drawbacks of the Cloud Computing model have become visible over the years, mostly connected with the communication between the end device and the data center hosting the cloud services: latency, bandwidth, cost, and availability of the connection all contribute to limit the number of uses for Cloud Computing. Hence, fog computing upgrades on-time service delivery and significantly mitigates a number of issues related to the cloud such as cost overheads, delays, and jitter while information is transferred to the cloud [41].

Therefore, Fog computing is a dominant tool to support the decentralized and intelligent processing of unusual data volumes generated by IoT sensors deployed to sync physical and cyber environments, thus helping the IoT reach its vast potential.

Thanks to IoT, Cloud and Fog, as well as Big Data, researchers and practitioners are granted permission to construct novel solutions that are able to efficiently and effectively refurbish consolidated healthcare practices or even provide novel groundbreaking results to address and lessen long-lasting healthcare issues. In this section, the main health-related application scenarios enabled by these three ICT pillars and their convergence stemming from the scientific literature. See (Figure 8)

Figure 8: Main HC4.0 Application Scenarios

The new technological models assembled in the Industry 4.0 are generating a serious change in mindset and advance to traditional applications. This phenomenon is in development also for the sector of healthcare, which has already started a dynamic development towards ehealth, expected to further widen and spur in the HC4.0 scenario. The mindset change will involve the understanding of new possibilities and opportunities as well as new challenges and risks: in this section we discuss both aspects (summarized in Table 2), to encourage a deliberate and effective integration of new methods, technologies and tools in the healthcare processes.

Cloud computing approaches in health care

Distributed computing in medical care is evolving rapidly to the point that assessments put its worldwide market at almost $10 billion by 2020 and $45 billion by 2023.[35] A connected measurement, from Black Book Market Research, fixed medical care cloud selection at an intense 74 percent. Also, per a new story in Global Health magazine, 2019 is turning out to be the cloud's greatest year ever across the medical care range. [36]

Table 2
Main benefits and challenges from the adoption of I4.0 pillars in healthcare.

	Benefits
IoT	• enhanced electromedical devices (*closed-loop design*, *predic* • interoperability, evolvability thanks to *open* *communicatio*
Cloud/Fog Computing	• *infrastructure for high-level functions* (data analysis, informa • *paradigmatic model* for offering of services to patients or t
Big Data	• new insights and *actionable information* from new data sou • natural transformation of *descriptive* research into *predicti*

It has proved to be beneficial for both medical services suppliers just as the patients. On the business side, Cloud processing has manifested profitability for marking down operational costs while permitting suppliers to bring high-caliber, customized care. Cloud services likewise raise patient commitment with their own wellbeing plans by giving them access to their own medical care information, consequently bringing about improved patient results. The democratization of medical services information and its outlying availability let loose suppliers just as patients and separates area hindrances bounding admittance to medical services.

The production of cloud demand in the healthcare industry has increased. Rising demand for cloud information is expected to increase as shown in the graph. In Figures 9 and 10 healthcare area cloud adoption has raised up so far also, nonstop selection of distributed computing by the medical care experts is likely to develop the industry in the forthcoming years

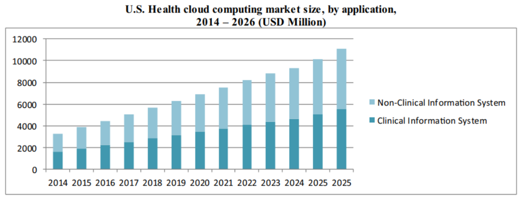

Figure 9: U.S Health Cloud Computing Market

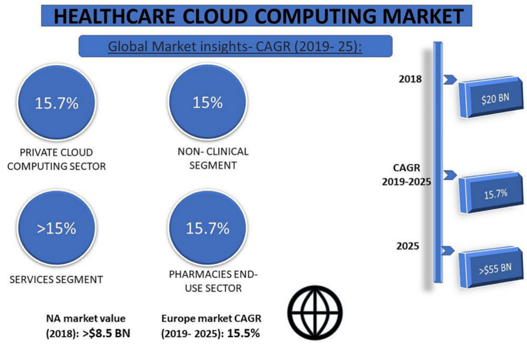

Figure 10: Healthcare Cloud Computing Market

Through distributed computing, there will be ease of collection or transferring of a patient's health record, through which one can save not just only the wage and time but also the juice. Keeping the current situation in mind, because of the pandemic maximum, people are restricted to show up at the same time at the hospital, which is very unsafe and infectious, with the help of the cloud web one can take advantage. It will be simple for doctors to keep the data, regardless of how long it can stay.

The Internet of Things technology provides a competent and methodical method to improve human health and comfort. One possible way to provide IoT-based medical services is to use a general health monitoring arrangement to show human health in real-time. This structure can gather biological signals from sensor nodes and commit the data to the gateway program through specific wireless communication. Then the real-time data is sent to the remote cloud server for real-time processing, visualization, and analysis. In this research paper, we advance this health monitoring system by wielding the concept of fog computing on a smart gateway that implements innovative technologies and services at the edge of the network, such as embedded data deletion, decentralized storage, and notification services.

Cloud computing equips a number of facilities to healthcare and healthcare to take assets from cloud computing as it is safe and secure, keeping the patient's history if you want, offers smart treatment, best for emergency situations, and supply chain maintenance. See [Figure 11].

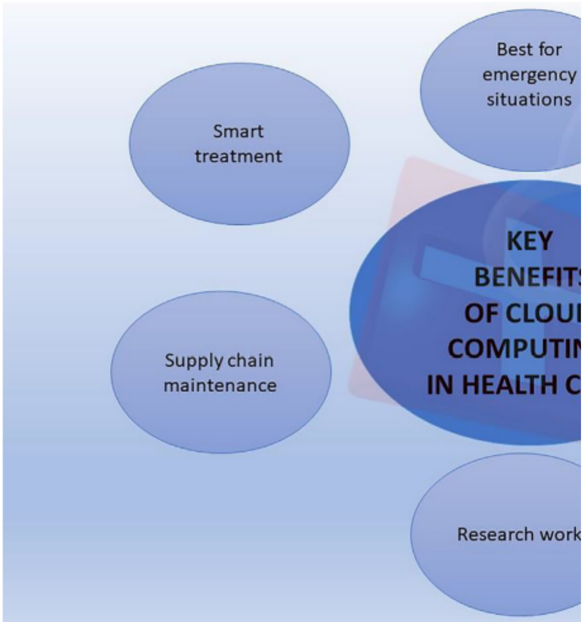

Figure 11: Key Benefits of Cloud Computing in Health Care

In Figure 12 Distributed computing is quite probably the current progressive innovation in the world. Cloud computing is built up step by step. The mix of distributed computing presents openings for developing medical services in a more powerful way. All outlines of the distributed or cloud computing idea identify with the cloud and provide comparable information assets.

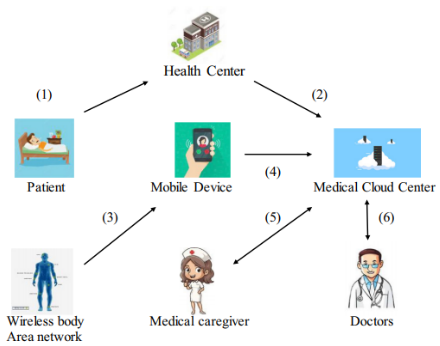

Figure 12: Medical Record Safe in Cloud

2.5 Reliability (Lee Jun Xian)

Reliability & confidentiality under uncertainties

Uncertainty refers to the epistemic situations that involve imperfect or unknown information or can be defined as the lack of sureness about something or someone. Tchernykh A, et al [44] indicates that uncertainties can be grouped into parameter (parametric) and system uncertainties. The parameter uncertainties arise from incomplete knowledge and variation of the parameters, for example, when data are not accurate or do not fully represent the phenomenon of interest, whereas the system uncertainties arise from incomplete understanding of the processes that control service provisioning, for example, when the conceptual model of the system used for service provisioning does not include all the relevant processes or relationships. It is stated that the parameter uncertainty is not reducible since it is a property of the system, but the system uncertainty can be reducible if more information is obtained.

Tchernykh A, et al [44] have listed and described the uncertainties that involve and relate to cloud computing. First is the Programming Uncertainty. It is stated that most cloud applications require availability of communication resources for information exchange between tasks, with databases or end users. However, providers might not know the quantity of data that can be managed, or the quantity of computation required by tasks. Though few approaches have been taken into consideration for this communication requirement but often in a highly abstract manner. If applications are to utilize the Cloud, the number of available machines, their location, their capabilities, the network topology, and effective communication bandwidth cannot be known ahead. To deal with these dynamics, either the programmers must explicitly write adaptive programs which are based on enormous programming efforts or cloud software must deal with the uncertainties. The paper also introduces a new Communication-Aware Directed Acyclic Graph (CA-DAG) model of cloud computing applications. It is said that the model overcomes shortcomings of existing approaches and allows to mitigate the uncertainties in a more efficient way.

Resource provisioning is also an uncertainty in Cloud computing. Tchernykh A, et al [44] stated the performance of cloud resources is hard to predict, because these resources are not dedicated to one particular user, and, besides, there is no knowledge of network's topology and also due to virtualization technique, it is impossible to get exact knowledge of the system.

Load balancing is one of the possible techniques to solve problems of the computing and communication imbalance associated with uncertainty. It can improve resource allocation. Tchernykh A, et al [44] stated that efficient load balancing helps to achieve high resource utilization and Quality of Service (QoS) by efficient and fair allocation of computing resources. Elastic load balancing distributes incoming traffic across multiple instances and achieves greater QoS. The elasticity allows handling unpredictable workloads and avoids overloading.

Tchernykh A, et al [44] stated there are numerous security and reliability issues for cloud computing as it encompasses many technologies. In this part, the approaches that minimize the risk of the environmental, deliberate and accidental threats and maximize productivity are discussed. Data replication is one of the approaches and its main advantages are high reliability and possibility to process the data in distributed fashion but its drawbacks are dramatic growth of data volumes and the need to protect each replication. Next is the Secret sharing schemes (SSS), methods by which a dealer distributes shares to recipients such that only authorized subsets of recipients can reconstruct the secret. They are important tools in cryptography that allow the build of secure distributed storage systems. The Redundant Residue Number System (RRNS) allows the builds of a reliable data processing system with multiple error detection and correction. Other than that, Erasure Code (EC) is an error correction code that is not homomorphic. It is suitable for building a reliable distributed data storage system but does not allow efficient data processing. Regenerating Code (RC) is a class of codes proposed for providing reliability of data and efficient repair (rebuild) of lost encoded fragments in distributed storage systems. RC can significantly reduce the total traffic required for repairing and obtain reasonable trade offs between storage and repair bandwidth. Homomorphic Encryption (HE) is an encryption technique that carries out computations on ciphers generating an encrypted result which matches the result of operations performed on the original numbers after decryption.

3. Application of Cloud Computing in Healthcare

3.1 Application in Energy Efficiency

Server Consolidation

Parminder Singh, et al [10] proposed workload based dynamic threshold (WBDTH) technique which is a hybrid of VM migration and Dynamic Voltage and Frequency Scalling (DVFS) techniques. The methodology of the VM migration stated by the author is based on 4 live migration stages to determine the threshold of the VM is underloaded or overloaded. Thus, the algorithm will put the underloaded VM into the migration map and the overloaded VM will continue the checking algorithm while using WBDTH algorithm to determine the host is underloaded or overloaded by calculating and comparing the scale of workload with change of rate and ls-norm. This can reduce the unnecessary migration of VMs with the scale of workload based on the scale of incoming workload.

Bryan Harris, at el [11] proposed Monte Carlo based server consolidation approach to improve energy efficiency in cloud data centers. The author reduced energy consumption by performing optimal resource allocation based on Monte Carlo method and Shannon Entropy to predict the resource bottleneck. The proposed technique does not require prior assumptions to dynamically adjust to resource utilization variations such as low, medium or high. Monte Carlo heuristic rank items based on the restrictiveness of placement option where restrictiveness taken from random sampling that measured with Shannon Entropy. The evaluation done by comparing with existing methods, the result showed that the proposed methods outperformed the existing methods.

Dynamic Voltage Frequency Scaling (DVFS)

Georgios L. Stavrinides, et al [13] proposed energy efficiency by utilizing per-core DVFS on the underlying heterogeneous multicore processors and approximate computations to fill in the schedule gap. Their goal was to provide timeliness and energy efficiency but trading off precise of the result while remaining the quality of the result and reasonable cost of the monetary cost required for the job execution. The authors used two scheduling strategies, task selection phase and VM selection phase. In the task selection phase, the task is prioritized based on the Earliest Deadline First (EDF) policy in which the task with the earliest deadline will be selected by the scheduler first. In the VM selection phase, the task will be allocated to the VM after the task is selected by the scheduler which can provide the earliest estimated finish time (EFT). The proposed techniques outperformed other two baseline scheduling policies which contribute to energy efficiency, lowest Service Level Agreement (SLA) violations rate and total monetary cost.

Sambit Kumar Mishra, et al [14] proposed modified DVFS based task scheduling algorithm to allocate tasks with optimal energy consumption and reduce completion time of the system. There are two phases of the author's proposed techniques. In the first phase, the scheduling algorithm will generate expected energy consumption (EEC) and expected time to completion (ETC) matrix for the second phase of the algorithm. In the second phase, the algorithm will mainly change the voltage frequency pairs for each task to minimize the overall energy consumption and completion time. Thus, the purpose is to reduce the energy consumption for overall task allocation of the system. The proposed algorithm compared with random allocation algorithm and first come first served (FCFS) algorithm, the result of the proposed algorithm has greater energy saving than other techniques.

Workload Aware Scheduling

Lin, W., Zhang, Y., Wu, W. *et al* [16] proposed a power consumption model called adaptive workload-aware cloud server power consumption measuring method (WSPM) which basically classified the workloads and selected appropriate power models. It proactively selects the appropriate power models for the upcoming workloads with workload clustering, forecasting and classification. The result is positive which is able to reduce real-time power estimation lag.

3.2 Application in data management

FDTM scheme

As mentioned, data is very important for organizations to make decisions as such, hence, faulty data is not tolerated in cloud computing applications. Therefore, FTDM scheme are proposed by the author which consists of 4 core components, (a) Data Collector, (b) Data Analyzer and Scheduler, (c) Fault-Tolerant Provider, and (d) Decision Maker. The FTDM scheme not only organizes and manages healthcare data (such as Blood Pressure, RespiratoryRate, Heart Rate, and Body Temperature) generated by IoT devices but also provides two-level fault tolerance at tasks and devices/nodes level [46]. See Figure 13.

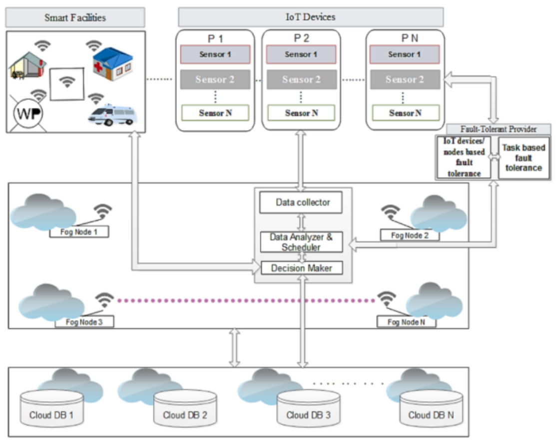

Figure 13: Fault-tolerant Data Management Scheme

The component “Data Collector” is in charge of collecting various healthcare data generated by the IoT devices related to the patients. The collected data will soon pass into the “Data Analyzer and Scheduler” component to be examined and scheduled. The component will also allocate the data to its appropriate resources in its environments. If the data are successfully executed, the results will be sent to the “Decision Maker” component, else the “Fault-Tolerant Provider” component will be executed. The “Fault-Tolerant Provider” component will perform two main mechanisms which are “Task-based fault tolerance” and “IoT devices/nodes based fault tolerance”. In the Fault Tolerance Provider component, “Task-based fault tolerance” will be executed first and once the tasks are failed at any node, they will be re-executed at other nodes, since, it is assumed that the Scheduler will retain a copy of the task when it is assigned to the nodes until its complete execution [46]. However, in “IoT devices/nodes based fault tolerance”, when the nodes in its environment fail, the task in the failed node will be transferred to another working node. In addition, the “Decision Maker” component will classify the data received from the “Data Analyzer” into two parts, normal and abnormal data [46]. The normal data is data with reasonable value and information of patient health and will be stored in a data center. However, the abnormal data which are inappropriate and unsafe for patient health, the model will then generate an alarm for action to the patient’s device as well as on the device of the patient's consultant [46].

Patient’s Smart Contract with Ethereum Network

The proposed e-health system by the author suggested using Ethereum Network to be implemented as Ethereum supports the implementation of smart contracts and offers the possibility to choose between different consensus protocols, Proof of Work (PoW) and Proof of Authority (PoA) [25].

The PoW offers firm security for the e-health system in which public networks also can be secured but it needs a significant quality of hardware resources to meet the computational requirements. Whereas PoA permits the development of a private and permissioned blockchain with low energy consumption [25].

When the Patient’s Smart Contract is configured using the Ethereum network, the data from the wearable device of the patient will get the proposal request (Transaction proposal) and sent to validating peers (miners) in the network to get the approval of the transaction and the value will be added into the smart contract. Soon, in the consensus protocol, the miners will then decide the validation of the transaction. If the data is valid, the peers will pass the transaction and add it to the new block. New health information entries will also be stored in the smart contract once the transaction is validated. Mobile applications also will notify the successful transaction. See Figure 14.

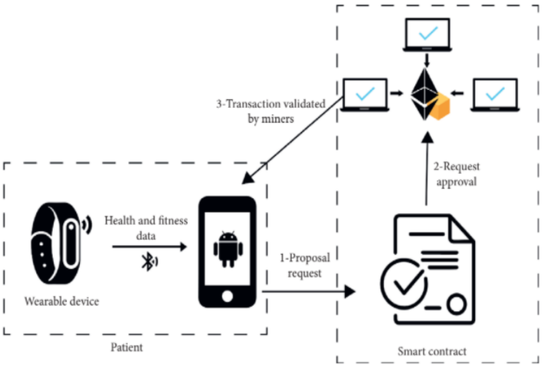

Figure 14: Patient’s smart contract configuration with Ethereum

As mentioned by the author, this configuration will be applied with two applications, first application will be the patient’s mobile phone to function as syncing data from the wearable devices and uploading the data to the blockchain, while the second application is a web application for health professionals to visualize their patient’s health information [26].

In the first application, the synchronization of the data will be requested by the users from his/her wearable device and uploaded into the blockchain. The health insights generated from the wearable device will be visualized from the patient mobile application. Then, the insights will be executed and uploaded to the smart contract function which then forms as a transaction and delivers to the blockchain network to allow validation from peers [26]. A response from peers will be sent out regarding the transaction validity. With this response, the smart contract will then notify the application while new data entry is added to the smart contract.

In the second application, health experts will monitor their patient’s information through the connection of a web application. The health experts also allow redirecting to a full list of patient information from the patients that authorized him to access their data. The web application also will request patient information from a patient smart contract using the health professional Ethereum credentials [26]. The smart contract will verify that this request is authorized and will give a response that corresponds to the health professional access level [25]. When the request is authorized, the data will be visualized to the dashboard page of the web application.

3.3 Application in Security

Security of cloud computing in healthcare

The healthcare system is currently one of the application domains in IoT that has piqued the interest of industry, academia, and government. In the medical industry, the rise of IoT and cloud computing is enhancing patient safety, staff happiness, and operational efficiency [29].

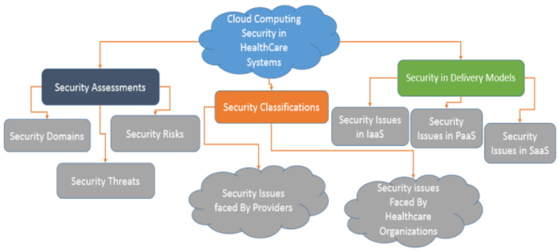

Figure 15: Healthcare cloud computing security

Cloud computing provides the benefit of allowing health care providers, caregivers, and patients to communicate information in a more structured and organised manner, lowering the risk of medical records being lost. Healthcare services and apps have benefited from technological advancements such as Cloud Computing. It guards against DDoS attacks, for example. DDoS assaults are on the rise, and a top cloud computing security strategy is around tactics that prevent massive amounts of traffic from reaching a company's cloud servers. In this age of ever-increasing data breaches, a top cloud computing security arrangement has security standards in place to ensure sensitive data and exchanges are safeguarded [27].

3.4 Application in IoT

Cancer prediction system using cloud computing

Effiok et al. [37] indicate a prostate cancer care process in the field of IoT. Risk predictive modelling has been compiled which consists of the concept of predicting the risk of prostate cancer. Figure 16 defines their overall system structure which involves several factors such as age, family history, and geographical region to regulate the level of vitamin D, animal fat and diabetes mellitus to sum up the risk associations. Authors implement the semantic description of the risk associations.

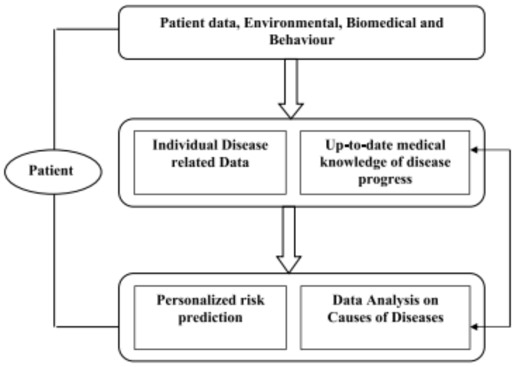

Figure 16: Prostate cancer care process

Figure 17 appears as the cancer prediction system using IoT in conjunction with cloud computing. Numerous sensors set up in a human body are used to examine the abnormality in the temperature and blood pressure. These collected data are then reserved using any local processing system which is evaluated to be the visible clinical data. This proposed system is especially favourable for predicting cancer hence the blood test report or mammogram report after classifying the variation in blood cells and temperature are used here for preparation. Features from the blood test report are obtained for classification since the features of a blood test may correspond to a normal person or a person who is overwhelmed by cancer.

For classification, it is desirable to use any deep learning tool such as Alexnet, VGG 16 and GoogleNet. Accuracy of different cancer types such as breast cancer, lung cancer, blood cancer and others will be predicted by training the interpreted neural network architecture. In this research work, blood test reports or any healthcare record are used as the input which is encrypted using the AES algorithm for generating validated encrypted data. These encrypted cancer details are saved in the cloud area for remodelling the result of the e-healthcare system since any patient can move from his/her hometown for any reason. If the data is stored in the cloud, then the patient does not need to ask the hospital for the treatment details to be followed and advanced. Patients can directly access the stored e-healthcare data in the cloud which could be accessed at any time from anywhere without any delay and huge processing. The main objective of this research work is to increase the security and flexibility of connecting the cancer patient details when it is stored in cloud areas. CloudSim is used for replicating the results and storing the encrypted cancer patient details into the cloud. In future, various cancers such as breast cancer, lung cancer, blood cancer, skin cancer and so on are going to be handled and forecast by using any deep learning tool.

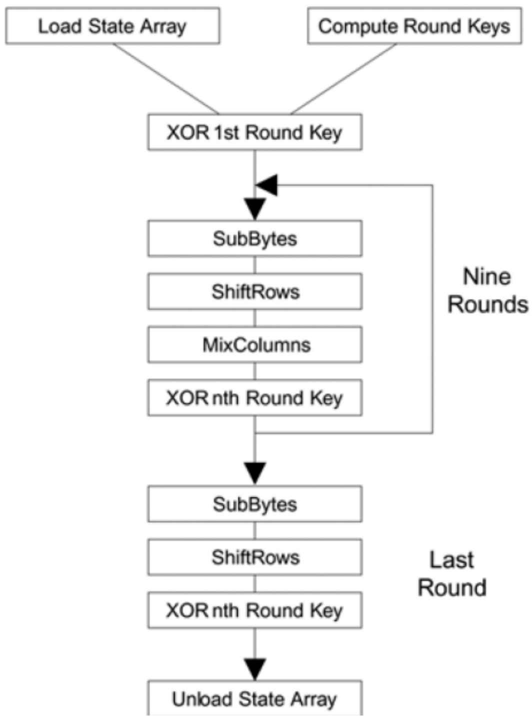

Figure 17: Flow chart of cancer prediction system using IoT.

Smart maternal healthcare services with wearable devices and cloud computing

The aim of this paper is to build and establish an Internet of Things platform that serves smart maternal healthcare services with wearable devices for pregnant women and cloud computing techniques. It is able to obtain all-weather, all-round monitoring and early warning for pregnant women during the perinatal session, mainly for the high-risk pregnant women. Through clinical practise such as screening, monitoring and emergency response and relevant clinical criteria, this platform will scale down high-risk conditions and unfortunate residuals caused by carelessness, emission or moratorium, making up for the perinatal care in China, especially the condition of inadequate management of high-risk pregnancy.

Wearable medical devices created for pregnant women are portable accessories that have a clinical health monitoring function. This latest medical device which is an accessory comes with cutting-edge technologies including advanced materials, sensing, circuit design, information transmission and information processing. They can implement the monitoring function while giving a comfortable and favourable experience.

As for pregnancy correlated with high-risk factors, such as pregnancy with diabetes, elderly pregnant women' anaemia, gestational hypertension, placenta presentation, giant foetus, multiple pregnancies, etc. Pregnant women should use a wearable foetus voice meter after 28 weeks of pregnancy to progress self-monitoring at home for intimate dynamic detecting, then sync foetal heart monitoring online. As Figure 18 shows, doctors are able to inspect the foetal monitoring data at the mobile smart terminal APP at any time and interpret it to provide targeted advice. Additionally, for those pregnant women who are advanced age, nervous, or have received infertility treatment with artificial assisted reproductive technology to perceive, it may be more adequate for them to use wearable remote foetal heart rate monitor at home and transfer the foetal heart map to let the medical staff know the foetus's current status.

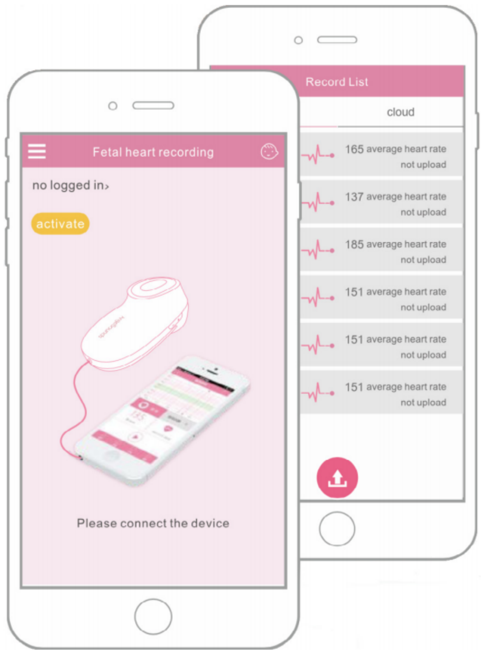

Figure 18: The interfaces of a mobile application of the IoT-based computerised interpretation system for home use

Monitoring management system links with wearable intelligent foetal heart monitoring devices that use mobile internet and combine with IoT technology to make the real-time logical joint of hospitals, doctors and pregnant women come true, which on the basis of data. Hence, this platform can extent the foetal supervision service to families, which can greatly boost the level of health management during the perinatal period and cut back the maternal mortality rate. Remote monitoring management systems can supervise three parameters, which are maternal foetal heart signal, uterine contraction signal and foetal movement signal. Without going to hospitals, pregnant women are able to reach out to their doctors who are in hospitals by means of smartphone mobile APP and information management platforms.

The platform engineered in this paper mainly consists of the perception layer, network layer and application layer. Its construction is shown in Figure 19.

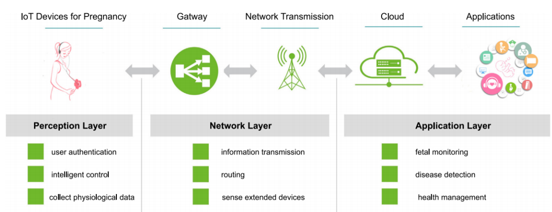

Fig 19: Three Layers of Platform Architecture

For the IoT smart platform, it is usually noticed that the data accuracy of the physiological parameters of pregnant women detected by wearable devices is the biggest problem. However, other issues in the aspect of device management cannot be neglected as well.

Wearable devices designed for pregnant women and emerging In-home health monitoring modes may bring massive revolution to the future medical model. Various wearable devices combined with a corresponding health management system can easily and smoothly record the physiological parameters of pregnant women in real-time, which borders the space of pregnant women health management and medical research.

3.5 Application in Reliability

Anomaly Detection & Analysis

Samir A, et al. [42] conducted an investigation of a framework for autonomous anomaly analysis that determines possible causes of consumer-observed anomalies in an underlying provider-controlled cloud infrastructure. They use Hierarchical Hidden Markov Models (HHMM) to map the observed performance anomalies to hidden resources and identify the root causes of the observed anomalies for the improvement of reliability. It is stated that consumers may experience anomalies in performance that may lead to performance degradation and application failure e.g., change in cluster node workload demand or configuration updates may cause dynamic changes or reallocation or removal of resources may affect the workload of system components.

Anomalies or faults describe an exceptional condition occurring in the system operation that may cause one or more failures. It is a manifestation of an error in the system. Failure is the inability of a system to perform its required functions within specified performance requirements. Therefore, both can be derived as e.g., fluctuations in workload are faults that may cause a slowdown in system response time which are an observed failure [42].

In order to evaluate the autonomous anomaly analysis framework, Samir A, et al. [42] conducted an experiment consisting of three Virtual Machines (VMs). Each VM is equipped with the same hardware specifications along with an agent. The Agents serve the purpose of collecting the monitoring data from the system e.g., host metrics, container, performance metrics, workload etc. All VMs are connected via a 100MBps network. For each VM, we deployed two containers, and we ran into them TPC-W benchmark for the use for resource provisioning, scalability and capacity planning for e-commerce websites. The TPC-W emulates an online bookstore that consists of 3 tiers: client application, web server and database. The data collected via these experiments are the CPU and Memory Utilization from the web server and the response time from the client application. The experiment ran for 300 minutes and obtained 2000 records. The gathered datasets are classified into training and testing datasets 50% for each. The model training lasted 150 minutes.To stimulate real anomalies of the system, they wrote a script to inject different types of anomalies into nodes and containers. The start and end time of each anomaly injection is logged. The 3 main types of anomalies are CPU Hog, Network packet loss and Workload contention.

After the experiments in [42], they compared their model performance with other techniques such as Dynamic Bayesian Network (DBN), and Hierarchical Temporal Memory (HTM). Some common measures in anomaly detection are used to evaluate the effectiveness e.g, Root Mean Square Error (RMSE), Mean Absolute Percentage Error (MAPE), Correctly Detected Anomaly (CDA), Correctly Identified Anomaly (CIA), Incorrectly Identified Anomaly (IIA), Recall and lastly the number of the normal identified component which has been misclassified as anomalous by the model (FAR). Their result are depicted in table 1 below:

Metrics	HHMM	DBN	HTM
RMSE	0.23	0.31	0.26
MAPE	0.14	0.27	0.16
CDA	96.12%	91.38%	94.64%
Recall	0.94	0.84	0.91
CIA	94.73%	87.67%	93.94%
IIA	4.56%	12.33%	6.07%
FAR	0.12	0.26	0.17

Table 1: Autonomous anomaly detection model validation result [42]

In conclusion, the results show that the proposed framework is able to automatically detect and identify anomalous behaviour with more than 96%.

5G Multi-access Edge Computing (MEC) Reliability

Fifth generation (5G) mobile telecommunication network has been expected to be involved in Multi-Access Edge Computing (MEC). MEC has evolved from mobile cloud computing, which shifts the important computation and storage tasks from the core network to the access network. Thus, mobile services can gain superiority of low latency, power efficiency, context-awareness, and enhanced privacy protection. The main objective of 5G is delivering a flexible next generation telecommunication system. Hence, the authentication and authorization processes can also exist at the edge of the network to increase the subscriber authentication efficiency and the reliability to the overall system. Generally, authentication, authorization and accounting (AAA) processes require a certain amount of cost from the system per registration of a subscriber. If these processes were to process at the edge of the network, it would increase the efficiency of subscriber authentication and authorization. Collecting valuable information helps to understand the context of the overall network situations, connectivity availability and also traffic patterns. With such information, the overall system reliability can be increased with minimal operation cost [45].

Han B et al [45] proposed a solution integrated in their 5G AAA approach which enables the execution of Authentication and Key Agreement (AKA) functionality at the Edge Cloud (EC), in order to support better deployment of 5G MEC services. They introduced the Trust Zone i.e., an innovative EC security architecture that enhances the 5G AAA with a cognitive access management with respect to the backhaul connection quality. When the backhaul is healthy, the Access and Mobility management Function (AMF) is invoked at the Virtualized-AAA (V-AAA) Manager in the central cloud. When the backhaul connection is seriously limited or unavailable, the Trust Zone relies on the V-AAA server that executes local AMF to maintain MEC services. There are 5 entities that can be found in the Trust Zone System e.g., Central CLoud Connection Monitoring (CCCM), Zone Management (ZM), Local Access Assistant (LAA), Security Auditing (SA) and Emergency Services (ES). The core of the Trust Zone lies in the ZM entity which implements most of AMFs and is connected with all other Trust Zone Entities. When ZM receives reports about updated backhaul status, it triggers and coordinates the state transition in the Trust Zone.

Furthermore, Han B et al [45] indicated that there is a conflict between the interests of subscribers (MEC service reliability) and of Mobile Network Operators (operating cost) and to tackle this concern, they designed a context-aware mechanism of synchronizing subscriber authentication information to local subscriber databases, which can help to reduce the backhaul network traffic generated by the Trust Zone. Several factors should be considered to estimate the Central Security Service Outage (CSSO) probability for a certain device in different ECs, e.g., User arrival, User stay time and backhaul reliability. Thus, from real-time information of devices (e.g., mobility and position) and ECs (e.g., coverage area, traffic model and backhaul throughput), high-level context information such as user motion pattern and backhaul outage probability are able to be extracted. These context information can be used to estimate the CSSO risk in different ECs for every certain device.

Han B et al [45] conducted numerical simulations to validate the effectiveness of the Trust Zone approach and the simulation showed that their approach and proposed method can effectively improve the reliability of Edge Computing services in the context of unstable security network functions in central cloud, while being capable to keep a flexible balance between MEC reliability and the operation cost.

4. Related Work

Reliability Analysis

Nguyen T A.et al [43] propose a hierarchical modeling framework for the reliability and availability evaluation of tree-based data center networks. The hierarchical model consists of 3 layers, including reliability graphs in the top layer to model the system network topology; a fault-tree to model the architecture of the subsystems; and stochastic reward nets to capture the behaviors and dependency of the components in the subsystems. But this review will only focus on the reliability evaluation that has been made in the paper.

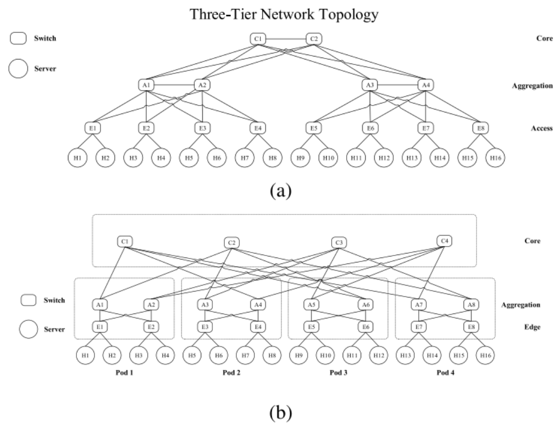

Figure 20: Data Center Networks topologies. (a) Three-Tier. (b) Fat-Tree. [43]

Nguyen T A.et al [43] introduced two representative Data Center Networks (DCNs) based on three-tier and fat-tree topologies which are popular in the industry. Figure 20 shows the 2 DCNs topologies respectively. The three-tier DCN has a less number of but more costly switches and more high-speed links in comparison to the fattree DCN. They consider a common practical case in high performance and high availability computing systems in Data Centers for both DCNs to be modeled. That is, the continuous data connection and transactions between compute nodes in a computer network requires high reliability/availability in parallel computing problems. In order to prolong the connection between the compute nodes, selecting an appropriate routing topology at a given time to avoid component failures will improve the availability/reliability of the connection. They also stated that the higher reliability/availability the system can achieve, the higher capability of connection the system can obtain.

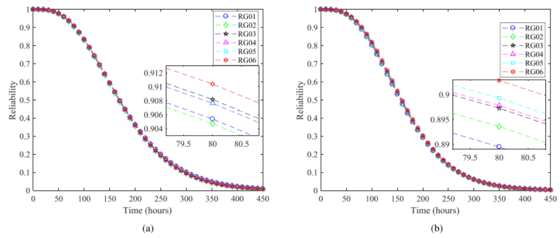

Figure 21: Reliability of DCNs. (a) Three-tier. (b) Fat-Tree. [43]

Nguyen T A.et al [43] conducted a simulation and came out with an reliability analysis of three-tier and fat-tree DCNs. The above figures are the illustrations of the dynamic behaviours of the overall system reliabilities (as a function of time) for the three-tier and fat-tree DCNs in all cases when the respective network configurations alter. Generally, the reliability of the system in all cases decays according to a certain varying curve as time proceeds with different speeds depending on the corresponding network configurations. This also shows the effects of compute node routing policies on the overall reliability. They conclude that the reliability of fat-tree DCN is lower than three-tier DCN at a certain time slice and the reliability of fat-tree DCN decays faster than three-tier DCN. They [43] stated that system design usually requires strict selection of more reliable and expensive components rather than less reliable and inexpensive ones to achieve the predefined dependability. Generally, there are always global policies to enable the system designer to improve the overall system reliability.

Table 1: Comparison of Energy Efficient Techniques

References	Techniques	Algorithm	Technology	SLA Agreement
[10]	Server Consolidation	Workload based dynamic threshold (WBDTH), DVFS and VM migration based energy- aware VM consolidation	CloudSim	Yes
[11]	Server Consolidation	Monte Carlo heuristics	Python supported by IBM's CPLEX LP solver	No
[13]	Dynamic Voltage Frequency Scaling (DVFS)	Scheduling algorithm	Own discrete-event simulation	Yes
[14]	Dynamic Voltage Frequency Scaling (DVFS)	Modified Task Scheduling algorithm	CloudSim, Single Data Centre	No
[16]	Workload Aware Scheduling	K-means algorithm	CloudMonitor	No
[17]	Server Consolidation	Parallel Particle Swarm Optimization (PPSO) algorithm	CloudSim	No

Table 2: Comparison of Data Management Techniques

References	Problem	Techniques	Data	Application
[26]	Enhance security and privacy of medical, paramedical, and personal data with less confidentiality.	Implementing Ethereum Network when proposing a contract optimizations from patients and health professionals	No Data were used in this study	Wearable devices, Mobile application, and Web Application
[46]	Enhance the scalability of data management when cost of communication increases.	Propose Fault Tolerant Data management scheme for Healthcare IoT to eliminate faulty data	Existing algorithm datasets for current, real testbed and real datasets in the future	Cloud Data Center, IoT Devices, and fog computing environment

Table 3: Comparison of Security Techniques

References	Problems	Techniques
[28]	Data security issues	Access control scheme is a technique to trust the data security in the cloud computing infrastructure.
[30]	DDos Attacks, a major threat of Internet based killer applications for non-cloud computing environment	Using a practical dynamic resources to counter DDos attacks that target cloud customer

Table 4: Comparison of IoT Efficiency techniques

References	Problem	Algorithm	Data	Application
[31]	Applying both IoT and Cloud computing in the e-healthcare system, particularly cancer disease prediction.	DNN Classification, Best Fit algorithm	Patient Data Acquisition	CloudSim

[32]	data accuracy of the physiological parameters of pregnant women detected by wearable devices	AI	Vital Signs Data of Pregnant women	Wearable Devices, Mobile Application
[33]	Energy, Scalability, Security, Availability	AI/Machine Learning	Healthcare Data	ICT, Mobile Application, Wearable Devices

Table 5: Comparison of Reliability Techniques

References	Problems	Techniques
[44]	Uncertainty that exist in the cloud computing system threatens its reliability	Identify the uncertainties And ways of delivering scalable and robust cloud behavior under uncertainties and specific constraints.
[42]	No direct insight into execution parameters at resource level, and only some quality factors can be directly observed while others remain hidden from the consumer.	Use of Hierarchical Hidden Markov Models (HHMMs) to map the observed failure behaviour of a system resource to its hidden anomaly causes.
[45]	5G MEC technology reliability and availability improvement	5G AAA with a cognitive access management and context-aware mechanism of synchronizing subscriber authentication information to local subscriber databases.
[43]	Data Center Network Reliability improvement	Hierarchical modeling framework for the reliability and availability evaluation of tree-based data center networks.

Conclusion

The paper has presented a comprehensive review of the current work that has been done related but not limited to the application of cloud computing in healthcare. The subtopic that has been covered are: the efficiency of Internet of Things, Data Management, Security, Reliability, and Energy Efficiency of Cloud Computing. Other than that, comparison between each subtopic research and methodology technique has been illustrated in table forms. That being said, the application of cloud computing in healthcare has endless possibilities and may even benefit and futurize the current healthcare system for it to be much more efficient and safe if all those conflicts and problems faced in cloud computing can be resolved.

References

1. Faridi, Farhan & Sarwar, Huzefa & Ahtisham, Md & kumar, Sarvesh & Jamal, Khalid. (2021). Cloud computing approaches in health care. Materials Today: Proceedings. 10.1016/j.matpr.2021.07.210.
2. Dang, L. Minh & Min, Kyungbok & Han, Dongil & Piran, Md & Moon, Hyeonjoon. (2019). A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics. 8. 10.3390/electronics8070768.
3. Singh, A., & Hemalatha, M. (2013). "CLUSTER BASED BEE ALGORITHM FOR VIRTUAL MACHINE PLACEMENT IN CLOUD DATA CENTRE."
4. P.Barham,B.Dragovic,K.Fraser,S.Hand,T.Harris,A.Ho,R.Neuge- bauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," in ACM SIGOPS operating systems review, vol. 37, pp. 164–177, ACM, 2003.
5. Srijita Basu, 2018, Cloud Computing Security Challenges & Solutions-A Survey , [online], Available at: <https://ieeexplore-ieee-org.tarcez.tarc.edu.my/stamp/stamp.jsp?tp=&arnumber=8301700>
6. The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique. (2021). Materials Today: Proceedings. [online] Available at: https://www.sciencedirect.com/science/article/pii/S2214785321052470.
7. Diez, O. and Silva, A., 2011. Reliability issues related to the usage of Cloud Computing in Critical Infrastructures. Advances in Safety, Reliability and Risk Management: ESREL.
8. C. Hsu, S.Chen, C.Lee, H. Chang, K. Lai, K. Li, C. Rong, "Energy – Aware Task consolidation Technique for cloud computing", published in IEEE 3rd International Conference on Cloud Computing Technology and Science, pp.115-121, 2011.
9. Singh, Sukhpal, and Inderveer Chana. "A survey on resource scheduling in cloud computing: Issues and challenges." Journal of grid computing 14, no. 2 (2016): 217-264.
10. P. Singh, P. Gupta and K. Jyoti, "Energy Aware VM Consolidation Using Dynamic Threshold in Cloud Computing," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), 2019, pp. 1098-1102, doi: 10.1109/ICCS45141.2019.9065427.
11. B. Harris and N. Altiparmak, "Monte Carlo Based Server Consolidation for Energy Efficient Cloud Data Centers," 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2019, pp. 263-270, doi: 10.1109/CloudCom.2019.00046.
12. Ismail, Leila, and Abbas Fardoun. "Eats: Energy-aware tasks scheduling in cloud computing systems." Procedia Computer Science 83 (2016): 870-877.
13. Georgios L. Stavrinides, Helen D. Karatza, "An energy-efficient, QoS-aware and cost-effective scheduling approach for real-time workflow applications in cloud computing systems utilizing DVFS and approximate computations", 2019
14. Mishra, Sambit & Khan, Md & Sahoo, Sampa & Sahoo, Bibhudatta. (2019). "Allocation of energy-efficient task in cloud using DVFS.", International Journal of Computational

Science and Engineering. 18. 154. 10.1504/IJCSE.2019.097952.

15. A. Kaur, V. P. Singh and S. Singh Gill, "The Future of Cloud Computing: Opportunities, Challenges and Research Trends," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, 2018, pp. 213-219, doi: 10.1109/I-SMAC.2018.8653731.
16. Lin, W., Zhang, Y., Wu, W. et al. An adaptive workload-aware power consumption measuring method for servers in cloud data centers. Computing (2020). https://doi-org.tarcez.tarc.edu.my/10.1007/s00607-020-00819-4
17. Prathap, R., Mohanasundaram, R. Hybrid optimization for virtual machine migration of utilizing healthcare text in the cloud. Int J Speech Technol 24, 359–365 (2021). https://doi.org/10.1007/s10772-021-09823-1
18. Oracle.com. (2014). What is Data Management? [online] Available at: https://www.oracle.com/database/what-is-data-management/.
19. Kucęba, R. and Chmielarz, G. (2018). Issues of personal data management in organizations – GDPR compliance level analysis. Informatyka Ekonomiczna, 1(47), pp.58–71.
20. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H. and Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, pp.73–80.
21. Brous, P., Janssen, M. and Herder, P. (2019). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, 51.
22. Amron, M.T., Ibrahim, R. and Chuprat, S. (2017). A Review on Cloud Computing Acceptance Factors. Procedia Computer Science, [online] 124, pp.639–646. Available at: https://www.sciencedirect.com/science/article/pii/S187705091732968X.
23. Mukherjee, S. (2019). Benefits of AWS in Modern Cloud. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415956.
24. Langmead, B. and Nellore, A. (2018). Cloud computing for genomic data analysis and collaboration. Nature Reviews Genetics, 19(4), pp.208–219.
25. Panicker, A., Divya, S., Thomas, Cyriac, I. and Sasidaran, A. (2021). Enhancing the Security of Cloud-Enabled Healthcare Portal using Decoy Technique. International Journal of Innovative Science and Research Technology, [online] 6(7). Available at: https://ijisrt.com/assets/upload/files/IJISRT21JUL337.pdf.
26. Frikha, T., Chaari, A., Chaabane, F., Cheikhrouhou, O. and Zaguia, A. (2021). Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform. [online] Journal of Healthcare Engineering. Available at: https://www.hindawi.com/journals/jhe/2021/9978863/ .
27. Guddu Kumar, 2019, A Review on Data Protection of Cloud Computing Security, Benefits, Risks and Suggestions, [online], available at: <https://uijrt.com/articles/v1/i2/UIJRTV1I20004.pdf>
28. Umer Ahmed Butt, Muhammad Mehmood, Syed Bilal Hussain Shah 2020, “A Review of Machine Learning Algorithms for Cloud Computing Security” [online] Available at: <https://www.mdpi.com/2079-9292/9/9/1379>
29. Ashraf Darwish, 2019, The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems, [online], Available at: <https://link.springer.com/article/10.1007/s12652-017-0659-1>
30. Shui Yu, 2014, Can We Beat DDoS Attacks in Clouds?, [online], Available at: <https://ieeexplore-ieee-org.tarcez.tarc.edu.my/stamp/stamp.jsp?tp=&arnumber=6567859>
31. Anuradha, M., Jayasankar, T., Prakash, N., Sikkandar, M., Hemalakshmi, G., Bharatiraja, C. and Britto, A., 2021. IoT enabled cancer prediction system to enhance the authentication and security using cloud

computing. Microprocessors and Microsystems, 80, p.103301.
32. Li, X., Lu, Y., Fu, X. and Qi, Y., 2021. Building the Internet of Things platform for smart maternal healthcare services with wearable devices and cloud computing. Future Generation Computer Systems, 118, pp.282-296.
33. Aceto, G., Persico, V. and Pescapé, A., 2020. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. Journal of Industrial Information Integration, 18, p.100129.
34. Faridi, F., Sarwar, H., Ahtisham, M., kumar, S. and Jamal, K., 2021. Cloud computing approaches in health care. Materials Today: Proceedings,.
35. Chen, T., Liu, C., Chen, T., Chen, C., Bau, J. and Lin, T., 2012. Secure Dynamic Access Control Scheme of PHR in Cloud Computing. Journal of Medical Systems, 36(6), pp.4005-4020.
36. Chen, Y., Lu, J. and Jan, J., 2012. A Secure EHR System Based on Hybrid Clouds. Journal of Medical Systems, 36(5), pp.3375-3384.
37. Effiok, E., Liu, E., Yu, H. and Hitchcock, J., 2015. A Prostate Cancer Care Process Example of Using Data from Internet of Things. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing,.
38. Botta, A., de Donato, W., Persico, V. and Pescapé, A., 2016. Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, pp.684-700.
39. Aceto, G., Persico, V. and Pescapé, A., 2018. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications, 107, pp.125-154.
40. Santos, J., Rodrigues, J., Silva, B., Casal, J., Saleem, K. and Denisov, V., 2016. An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. Journal of Network and Computer Applications, 71, pp.194-204.
41. Kumari, A., Tanwar, S., Tyagi, S. and Kumar, N., 2018. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. Computers & Electrical Engineering, 72, pp.1-13.
42. Samir, A. and Pahl, C., 2019. Anomaly detection and analysis for clustered cloud computing reliability. CLOUD COMPUTING, 2019, p.120.
43. Nguyen, T.A., Min, D., Choi, E. and Tran, T.D., 2019. Reliability and availability evaluation for cloud data center networks using hierarchical models. IEEE Access, 7, pp.9273-9313.
44. Tchernykh, A., Schwiegelsohn, U., Talbi, E.G. and Babenko, M., 2019. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science, 36, p.100581.
45. Han, B., Wong, S., Mannweiler, C., Crippa, M.R. and Schotten, H.D., 2019. Context-awareness enhances 5G multi-access edge computing reliability. IEEE Access, 7, pp.21290-21299.
46. Saeed, W., Ahmad, Z., Jehangiri, A.I., Mohamed, N., Umar, A.I. and Ahmad, J. (2021). A Fault Tolerant Data Management Scheme for Healthcare Internet of Things in Fog Computing. KSII Transactions on Internet and Information Systems, [online] 15(1), pp.35–57. Available at: http://itiis.org/digital-library/24229.