IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907097 |

A Survey Paper Data Protection Mechanism over Cloud Based System for Covid-19 Situation

Renuka Shinde, Lokesh Khedekar

PG Student, Dept. of CSE, RSCE, Buldana, Sant Gadge Baba Amravati University, Maharashtra, India

Assistant Professor, Dept. of CSE, RSCE, Buldana, Sant Gadge Baba Amravati University, Maharashtra, India

ABSTRACT: With the popularity of wearable devices and the development of cloud and cloudlet technology, the need for better medical care has grown. Data collection, data storage, and data sharing are all part of the medical data processing chain. This overview describes several researches done on health care system with the functions of cloudlet including privacy protection. This study shows that, there has been lot of development in the same area. Technology such as Big Data is taken into consideration for improvement.

KEYWORDS*:* Activities of Daily Living; Patients-LikeMe; Number Theory Research Unit; electronic health records; collaborative IDS

I.INTRODUCTION

With the rise of healthcare big data and wearable technology, as well as cloud computing and Communication technologies, cloud-assisted healthcare big data computing is becoming increasingly important to address users' ever-increasing demands for health consulting.

Personalizing unique healthcare data for various users in a convenient manner, on the other hand, is a tough challenge. Previous research recommended using social networks and healthcare services to help track the disease treatment process and get real-time disease data. Patients-LikeMe, a healthcare social platform, can acquire information from other similar patients via data sharing in terms of the user's own results.

While sharing medical data on social media can benefit both patients and doctors, sensitive data can be lost or stolen, posing privacy and security concerns. As a result, balancing privacy protection with the convenience of exchanging medical data becomes a difficult task. With advancements in cloud computing, a huge amount of data may be stored in a variety of clouds, including cloudlets and remote clouds, allowing for data sharing and heavy computations.

II. LITERATURE SURVEY

A. *Healthcare in the Smart Home: A Study of Past, Present and Future* [1].

With the home automation and sensor businesses evolving over the last few decades, the technology underpinning what many people envision as "The Smart Home of Tomorrow" is mostly available now. What's needed now is public acceptance and adoption, as well as the integration of these devices into the home and the collection of data. User-friendliness, ease of installation, and cost vs. value for the homeowner should all be considered in research into what would drive a more general acceptance and use of smart technologies in the home, but it might also be government legislation it starts the ball rolling.

This kind of project, similar to the British governments mandate to have a Smart Meter placed in every home in the UK by 2020, might pave the way for other smartness in the home. This kind of project, similar to the British governments mandate to have a Smart Meter placed in every home in the UK by 2020, might pave the way for other smartness in the home. Ubiquitous or pervasive computing is a concept that is becoming more widely used in the technology sector, and it is now making inroads into the consumer electronics space under the umbrella name "Internet of Things."

One area of interest is the addition of intelligent, networked sensors and computers to the home to create a Smart Home, which opens up a slew of new possibilities for the function of tomorrow's habitation. As the world's population

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907097 |

continues to live longer and so experience more medical-related problems, while institutional healthcare struggles to keep up, the Smart Home's function in monitoring a dweller's health and delivering any necessary intervention becomes increasingly important. This research examines the history of Smart Home Healthcare, as well as current research fields and anticipated future research areas.

An activity of Daily Living presents distinct categorizations (ADL) and Personal Sensors are discussed, as well as a detailed look at how Smart Home Healthcare can be used. Technology can supplement and, in some situations, totally replace traditional healthcare delivery techniques. Costs can be cut while medical adherence improves, all of which contribute to a more sustainable and effective care paradigm.

B. *Medical Data Sharing For Protection and Intrusion Avoidance in Cloudlet* [2].

A person's personal health record is an important tool for keeping track of medical data in an accurate, dependable, and thorough manner. Restorative information exchange is, for all intents and purposes, a fundamental and testing issue. As a result, they use cloudlet's adaptability to create a novel human services framework in this article. Cloudlet provides security insurance, information interchange, and an interruption location. Using the Number Theory Research Unit (NTRU) approach, they obfuscate the client's bodily information collected by the wearable device during the data gathering phase. That data will be sent to neighboring cloudlets in a vitality-efficient manner. Furthermore, they demonstrate another trust model that allows clients to select trustworthy partners with whom to exchange information stored in the cloudlet. The trust
exhibit also encourages similar patients to talk about their illnesses with one another. Finally, they divide our clients' medical information, which is kept in a remote billow of a healing facility, into three areas and provide them with proper insurance.

They looked into the issue of privacy protection and sharing significant amounts of medical data in cloudlets and the remote cloud in this project. In order to ensure secure data collecting and cheap transmission costs, they designed a system that prevents users from sending data to a remote cloud. It does, however, allow users to transfer data to a cloudlet, which initiates the process the process of data sharing problem in cloudlet. . To begin, they can gather data from consumers via wearable devices, and in order to preserve their privacy, they employ the NTRU mechanism to ensure secure data transmission to cloudlet. Second, in order to exchange data in the cloudlet, they employ a trust model to assess users' trust levels and decide whether or not to share data. Third, in order to safeguard the privacy of remote cloud data, they partition the data stored in the cloud and encrypt it in various ways, not only to assure data security but also to improve transmission efficiency. Finally, to defend the entire system, they propose a collaborative IDS based on cloudlet mesh. The user submits an online query to the doctor, who responds with an another.

C. *A security framework in G-Hadoop for big data computing across distributed Cloud data centers* [3].

For large-scale data-intensive applications, MapReduce is recognised as an appropriate programming approach. The Hadoop framework is a well-known MapReduce implementation that uses a cluster architecture to conduct MapReduce processes. G-Hadoop is a Hadoop MapReduce framework modification that allows MapReduce tasks to be distributed across many clusters. G-Hadoop, on the other hand, merely reuses Hadoop's user authentication and job submission mechanisms, which are built for a single cluster.

This paper presents a new G-Hadoop security model. The security model is targeted to distributed situations and is based on many security solutions such as public key cryptography and the SSL protocol. With a single-sign on approach, this security framework streamlines the users authentication and task submission procedure in the existing G-Hadoop implementation. Furthermore, the developed security framework includes a variety of security techniques to defend the G-Hadoop system from common assaults. This project created and implemented a security framework for performing MapReduce workloads in a distributed environment across many clusters. Users can submit jobs to G-Hadoop using a single-sign-on mechanism provided by the security framework. It also employs a number of security techniques to safeguard the G-Hadoop system from assaults, as well as abuse and misuse. These security methods are based on current security solutions, such as SSL and cryptographic algorithms, or alternative security concepts, such as GSI.

Some concepts are used in this security framework as well, such as proxy credentials, user session, and user instance, to provide the framework's functionality. The proposed security architecture has the capacity to prevent the most frequent attacks, such as MITM, replay, and delay attacks, and enables secure communication of G-Hadoop over public networks, thanks to these security features. Furthermore, it employs a variety of techniques to prevent the misuse

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907097 |

or abuse of G-resources. Overall, it provides a secure and comprehensive solution for the user to access G-Hadoop through a single-sign-on process. To boost the complexity of cryptographic analysis by an adversary, task execution in Phase V, as well as encryption methods and keys, will be built as changeable.

D. *Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring* [4].

The burgeoning Internet of Things (IoT) technologies' tremendous potential for interconnected medical equipment and sensors has played a critical part in the next-generation healthcare industry's commitment to high-quality patient care. The growing number of aged and disabled persons necessitates the development of a real-time health monitoring system capable of assessing patients' healthcare data in order to avert unnecessary deaths. The Healthcare Industrial IoT (HealthIIoT) offers a lot of potential for achieving this kind of monitoring. HealthIIoT is a combination of communication technologies, interconnected apps, Things (devices and sensors), and people that would work as a single smart system to monitor, track, and store patients' healthcare data for continuing care. This study describes a HealthIIoT-enabled monitoring architecture in which mobile devices and sensors capture ECG and other healthcare data and securely send it to the cloud for seamless access by healthcare experts.

To prevent identity theft or clinical error by healthcare providers, signal augmentation, watermarking, and other associated analytics will be used. By installing an IoT-driven ECG-based health monitoring service in the cloud, the suitability of this technique has been proven through both experimental evaluation and simulation. Continuous monitoring from anywhere, at any time, using a range of devices is a new healthcare service that has the potential to transform the industry by improving access to patient information and offering high-quality patient care. Healthcare practitioners may be able to access, store, and analyse patient data in real time using HealthIIoT to monitor and follow the patient. However, security breaches can occur with interconnected there patient devices and healthcare data (such as ECG readings).

In order to do this, this paper provides a cloud-integrated HealthIIoT monitoring architecture in which healthcare data is watermarked before being transported to the cloud for secure, safe, and high-quality health monitoring. The suggested HealthIIoT monitoring framework will be tested for data security and alerting features in the future, as well as a test trial with real-world patients and health professionals.

E. *Security and Privacy Issues and Requirements for Healthcare Cloud Computing* [5].

In order to improve and enhance medical services while also monitoring costs, information technology is increasingly being used in healthcare. Healthcare is one of the sectors where having information available at the appropriate time and with high accuracy is critical. Building a secure EHR sharing environment has gotten a lot of attention in the healthcare sector and the academic community, thanks to the widespread usage of electronic health records (EHR).

One of the most widely used health IT infrastructures for simplifying EHR sharing and integration is cloud computing. Healthcare clouds open up new avenues for innovation, such as easy and ubiquitous access to medical data and new business models. They do, introduce additional risks and concerns in terms of security and privacy. In the cloud computing context, ensuring security and privacy is critical. They will describe current state-of-the-art research in this topic in this paper. They focused on various flaws in current healthcare solutions and standards, particularly in terms of platform security, privacy, and requirements, which is a critical facet of total healthcare IT system security.

F. *DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments* [6].

Dynamic Proof of Storage (PoS) is a cryptographic mechanism that allows a user to verify the integrity of outsourced files and update them quickly on a cloud server. Although various dynamic PoS solutions have been presented in single-user situations, the challenge in multi-user environments has not been fully addressed. When other owners of the same files have posted them to the cloud server, a viable multi-user cloud storage system requires the secure client-side cross-user deduplication approach, which allows a user to skip the uploading process and receive ownership of the files immediately. None of the existing dynamic PoSs, to our knowledge, can support this technique.

They present the concept of deduplicatable dynamic proof of storage in this research and suggest DeyPoS, an efficient structure for achieving dynamic PoS and safe cross-user deduplication at the same time. They use a new tool called Homomorphic Authenticated Tree to address the difficulties of structure diversity and private tag creation (HAT). They show that our structure is secure and theoretical analysis and actual findings show that it is effective in

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907097 |

practice. They developed the idea of deduplicatable dynamic PoS and recommended extensive requirements in multi-user cloud storage systems.

HAT is a revolutionary tool that is an efficient authenticated structure that they created. They presented DeyPoS, the first practical deduplicatable dynamic PoS method, and demonstrated its security in the random oracle scenario using HAT. Our DeyPoS implementation is efficient, according to theoretical and experimental results, especially when the file size and number of challenged blocks are big.

G. *Social Networks in Health Care: Communication, collaboration and insights* [7].

In the health-care field, public, Internet-based social networks can facilitate communication, collaboration, and information collecting and sharing. About a third of Americans who go online to investigate their health utilise social networks to connect with other patients and discuss their conditions1,2, and 36% of social network users analyse and leverage the knowledge of other customers before making decisions. 3 Because social networks may be utilised to reach stakeholders, aggregate information, and drive collaboration, they have a lot of potential value for health care organizations. This issue brief presents a high-level overview of social networking, its industry, and societal consequences; it also analyses social networking projects in health care and highlights major applications by health care sector.

H. *Joint Data Detection and Phase Noise Mitigation for Light Field Video Transmission in MIMO-OFDM Systems [8].*

Previous research on video transmission through wireless communication networks concentrated on mitigating the impacts of additive channel noise and fading channels without accounting for physical layer impairments such as phase noise (PHN). The performance of multi-input multi-output orthogonal frequency division multiplexing is hampered by oscillator phase noise (MIMO-OFDM) systems may fail to provide high data rates for video applications, resulting in decoding failure.

They propose a light field (LF) video transmission system for wireless channels and investigate joint data detection and phase mitigation in MIMO-OFDM systems for LF video transmission in this study. In the presence of several PHNs, the signal model and rate-distortion (RD) model for LF video transmission are examined. Furthermore, for joint data detection and PHN tracking, they present an iterative approach based on the extended Kalman filter. When compared to existing techniques, numerical results demonstrate that the proposed detector may greatly enhance the average bit-error rate (BER) and peak-to-noise ratio (PSNR) performance for LF video transmission. Furthermore, the suggested system's BER and PSNR performance is closer to that of the ideal scenario of flawless PHN estimation. Finally, the suggested system concept and algorithm are shown to be suitable for LF video transmission over wireless channels.

They looked at the joint data detection and phase noise mitigation of different PHN parameters in MIMO-OFDM systems for LF video transmission in this work. When compared to existing techniques, numerical results show that the proposed detector can greatly enhance the average BER and PSNR performance for LF video transmission. Furthermore, the proposed system's BER and PSNR performance they are closer to the ideal scenario of flawless PHNs estimate. The proposed system model and algorithm they shown to be suited for LF video transmission.

I. *Privacy and Security for Online Social Networks: Challenges and Opportunities* [9].

In recent years, online social networks such as Facebook, MySpace, and Twitter have grown at an exponential rate. These OSNs provide appealing ways for people to interact and communicate online, but they also create privacy and security concerns. The design issues for OSN security and privacy are discussed in this article. Facebook, MySpace, and Twitter are just a few instances of fast growing online social networks in recent years. These online social networks (OSNs) offer tempting methods to interact and communicate, but they also raise privacy and security concerns. This article discusses the security and privacy of OSNs.

They explored security and privacy design concerns on online social networks in this post, as theyll as a few research ideas for resolving design conflicts between OSNs' diverse design aims. Experts from the social science and network security areas, as well as industry, regulatory authorities, and other relevant communities, will be required for a final solution. This article is meant to serve as a jumping off point for creating secure and privacy-preserving OSNs. They hope that this work will inspire OSN academics and developers to pursue more innovative OSN designs that do not jeopardize users' data security and privacy.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907097 |

III. Conclusion

In this survey paper, we study several work done on the same topic. A vast research is done in this area and we can see that there has been a huge progress, a novel human services framework by using the adaptability of cloudlet. We may say that each system perform different depending the method used. And none is perfectly appropriate according to the recent scenario about the increasing need of healthcare system and simultaneously increasing demand of protection of user data over cloud. According to that we can conclude that each work has a scope for improvement. The current scenario about the increasing need of data protection need more work to done.

REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.

[3] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, "A security framework in g-hadoop for big data computing across distributed cloud data centers," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[4]M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[6] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.

[7] L. Griffin and E. De Leastar, "Social networking healthcare," in wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE, 2009, pp. 75–78.

[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data for light-field-based 3d telemedicine," IEEE Network, vol. 30, no. 3, pp. 30– 38, 2016.

[9]C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," Network, IEEE, vol. 24, no. 4, pp. 13–18, 2010.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details