INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

A Research on cloud computing-based health care facilities

[1]CHILAKALA NARASIMHA REDDY, [2]M. SAMUEL SANDEEP REDDY

[1]PG Scholar, Dept. of MCA, Newton's Institute of Engineering, Guntur, (A.P)

[2]Associate professor, Dept. of CSE, Newton's Institute of Engineering, Guntur, (A.P)

Abstract: The body of literature tends to raise awareness of the use of cloud computing in the medical field by discussing the traditional method of storing the data, the extent in using cloud computing in the medical field, the companies that are providing the platform of cloud computing in the medical field, as well as the annual expenditures on such projects and the companies providing them. Data security in cloud networks and servers is the focus of this study, which examines the current state of the art to determine where improvements may be made and proposes a strategy for doing so.

Keywords: cloud computing, medical records, EHR's, AWS, data processing

I. INTRODUCTION

Cloud Computing, the latest internet platform, provides secure online data storage for any kind of information. In this case, the cloud represents a symbol for the worldwide web. Companies like Google, IBM, Sun, Amazon, and Microsoft offer a platform for cloud computing research, making it a prominent topic in the academic community. Cloud computing's popularity in the IT industry continues to skyrocket. In this paper, we will examine the current state of the health care medical record storage system using cloud computing and propose our theoretical plan to easily access the data, with more security, because medical data is the most important data in the world today, and it is a very difficult task to ensure the safety of the data. The industry for cloud computing has a lot of potential for growth. However, current information and reports show that its rapid expansion is allowing greater opportunities for data theft. A recent paper predicted expanding applications for cloud computing in healthcare, and it offered many prototypes and frameworks for doing so. Cloud computing's research and development panel has uncovered the automation wherein the framework transmits patient vital data through a network or set of sensors attached to medical equipment, and then delivers the

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

data to the cloud where it can be stored, processed, and disseminated by medical centres. The system's most notable advantages are the ease with which users may obtain data and make necessary corrections. Signal processing and security for mobile devices through multimedia sensors; patient data storage for the medical industry via cloud computing; quick access to information. Redundant data storage ensures that your data is safe and can be accessed quickly and easily. The medical industry is increasingly recognising the benefits of cloud computing.

II. LITERATURE SURVEY

The k-Nearest Neighbour (kNN) classifier is widely used in supervised learning systems (Lin et al., 2014). The only thing you need for this method is a difference you can point out between two specific cases. k-nearest neighbours (kNN) are a classification method that assigns a label to an input item based on how similar it is to the labels assigned to the k-nearest models in a collection of training examples. Its theoretical simplicity and straightforward handling, which perform marvellously in a variety of pattern recognition tasks, are also major contributors to its widespread renown. When there are more than two components in the set of possible labels, this works well to reduce the discrepancy across classes (Mungai, 2013). In this regard, other protocols, such as Support Vector Machines, must choose a strategy to retrain for this scenario (Mungai, 2013). As a multi-class policy, kNN executes any kind of strategy customisation.

The kNN classifier is an example of an instance-based algorithm since it does not engage in a predetermined generalisation method (i.e., model building) in response to preliminary training data but rather immediately deliberates those cases for classification (Thilakanathan et al., 2014). Since it has been proved that the classifier maintains consistency as the number of training examples increases from 20 to infinity, its performance improves with the size of the training collection (i.e., Training sets) (Sultan, 2014). It would seem that the vast amount of data around our group has given us widespread recognition.

The information linked with contemporary technology has been growing steadily from the beginning (Li et al., 2017), with this effect becoming more noticeable in recent years. These extensive data sets might potentially be used by a kNN classifier to improve the effectiveness of categories.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

However, the kNN classifier requires less efficient use of category time and memory since it has a tendency to construct a range in between the input sample and every example of the training data. This is the major drawback of the aforementioned classifier, which becomes an insurmountable difficulty when dealing with training data on such a massive scale. The fundamental assumption is that an instance's k-nearest neighbours also belong to the same cluster. Therefore, the kNN pursuit may be efficiently completed in 2 steps: i) arriving at the adjacent cluster, and ii) identifying the k-nearest neighbours inside the cluster. In a large-scale scenario, this would save a great deal of wasted distance computations and make the technique considerably easier to implement overall (Singh and Liu, 2003). Still, if the kNN's components fall into a wide variety of clusters, there is a chance that this search or exploration may result in a loss of accuracy.

To alleviate this problem, a strategy is developed to greatly reduce the likelihood of this happening. Our idea is that groups of things aren't always completely separate, but that there are always special cases that may be made to fit into the bigger picture. To this end, we use a further step after the first clustering process: This procedure involves (i) focusing on one collection and iterating through all of the instances; (ii) for each component of the collection, inspecting the k-nearest neighbours allowing for the entire training set; (iii) in the event that any of the k neighbours of the instance at issue is not component of the collection being considered, we embrace it inside the cluster, thus potentially segmenting the area to something akin to an unclear clustering; and (iv) this procedure resulting This technique improves the likelihood of making all the k-nearest neighbours of a given set of test conditions cluster together. Also, remember that the clustering process and the hoped-for improvement are carried out simultaneously as a pre-processing step, so there is no impact on the efficacy of the category process.

III. RELATED RESEARCH

Smart cities, which use cloud computing for data processing, are gaining popularity as a means of bettering the lives of city dwellers. In order to solve the issue of virtual machine and user mobility, a new model was presented called PRIMIO. This model finds the best way to relocate resources closer to the user no matter

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

where they are located. The transition from on-premises to cloud-based health services has a number of hurdles and possibilities, but [1] these problems and gains can be overcome with the right approach. The new model is more cost-effective, versatile, and efficient. Using the HC2 SP paradigm that has previously been presented, we may enlist the aid of major providers like Microsoft, Google, and Amazon to ensure the system's safety.[2] With recent advances in medicine and quality of life, the average human longevity is expected to rise, making daily health monitoring of sick and healthy individuals all the more important. With the current health care system, this is frequently impossible. They also lacked the means to track their progress towards their health and wellness objectives by having access to data on their results. Wireless gadgets that may be utilised in the comfort of one's own home are therefore in high demand. The recent decade has seen the widespread use of what are known as medical speciality wearable devices. Many factors contribute to this, but high-profile examples include increasing health care costs, growing patient wait times, and a heightened public awareness of the need of living longer, healthier lives.[3] In the modern period, what is known as the Internet of Things (IoT) is in high demand since it encompasses a system with interconnected objects, people, time, places, and networks. Before this, it was impossible to keep tabs on a patient's health in real time from far away. Some of the most pressing concerns we face today are those related to people's quality of life, the security of our systems and procedures, and our right to privacy. A unified strategy is expected to be established after studying the existing approaches to authentication protocols, access management, and energy-efficient access control mechanisms separately.[4] Every day, there's a lot more information to process in healthcare, such new texts, sounds, and visuals.

Therefore, it has become a required and difficult problem to store and retrieve this data.

They reported that the NoSQL database, which is model-based, will improve productivity.[5] Illnesses brought on by polluted air. Air pollution is a major contributor to the rise in diseases and deaths in the modern era. Air quality indicators (AQIs) are a novel tool that has been implemented.[6]

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

Barriers to Implementing a Mobile Health Monitoring System

There are three parts to the framework: the data storage layer, the annotation layer, and the analyser layer.

To provide the highest level of safety, a multiple access technique was enhanced in the data storage layer. The process mining technique is implemented in the Data Analyzer Layer to back up the individual treatment plan. Electronic health records include built-in privacy and security, as stated in [7]. The safety is tested in three different conditions. The influence of small and medium-sized enterprise (SME) migration on service resilience in cloud computing is the answer to this issue.[8] A novel method using attribute-based encryption was presented for managing cloud-based information systems. Patients may choose whatever parts of their PHR to share with their doctors using this technology, and the doctors never need to know the whole details. To bridge the gap between the theoretical and actual implementations of this mode, three extensions have been suggested.

To safeguard patient confidentiality, [9] electronic health records must include access controls. Models in the categories of (1) electronic health record access control, (2) interoperability control, and (3) risk analysis control were addressed. Granular access control based on roles, taking into account semantic, geographical, temporal, dynamic, and probabilistic factors. Three models were examined for interoperability and risk. [10].

IV. RECENT DEVELOPMENTS IN CLOUD COMPUTING AND THE MEDICAL SECTOR

Given the country's projected GDP growth, the Indian healthcare sector has the potential to expand to 8.6 trillion rupees by 2022. In FY14, government spending was raised from 1.2% to 1.4%; by 2025, India hopes to have raised it to 2.5%. The healthcare industry in India is expanding at a rate of roughly 20% annually. There was USD 1.1 billion in direct investment in healthcare facilities and testing centres between 2000 and 2011.

Fig 1. Market of cloud computing

According to Global market Insights, the healthcare cloud computing industry would be worth more than USD 55 billion

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

by 2025.In 2018, the cloud computing market was dominated by North America due to rising demand for electronic health records in the healthcare sector and robust private sector involvement in the industry's expansion. Markets & Markets found that in 2011, cloud computing use in the healthcare sector increased from 4% to 20.5%.

The research claims that each cloud provider has less than a 5% share of the healthcare sector. Agfa Healthcare, Care Cloud, Dell, GE Healthcare, and Merge Healthcare are just few of the names in the healthcare industry.

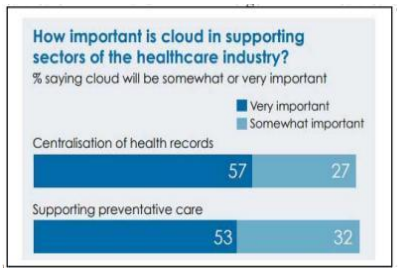


Fig 2. Importance of cloud computing

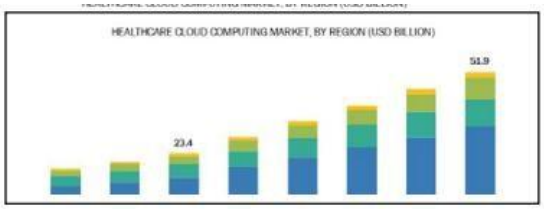


Fig 3. Market by Region

V. CHALLENGES IN THE PRESENT SOLUTION

The term "confidentiality" refers to the practise of shielding an individual's medical history from prying eyes. As more people get access to the cloud computing network, there is a greater chance that sensitive information may be stolen or somehow compromised. It is crucial that a patient have trust in the system to maintain the confidentiality of his or her data in order to have an effective and productive interaction with a doctor. The patient's ability to be as specific as necessary in future data sharing may be negatively impacted if he or she believes that the medical records information he or she supplies to the doctor is not protected and safe and that his or her privacy is threatened. If a doctor's or hospital's patient records are compromised, it may have a negative effect on the doctor-patient relationship. Gaining access to the record's controls and using encryption methods both enhance its privacy.

Respect for and control over sensitive health data:

When a record has integrity, it is reliable, devoid of mistakes, and cannot be tampered with in any way. Use of critical applications in the eHealth cloud is essential for ensuring their dependability. The data is owned by the investigator. Establishing ownership of patient data is

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

critical for safeguarding them against theft or misuse. Encryption and watermarking are two methods for protecting intellectual property.

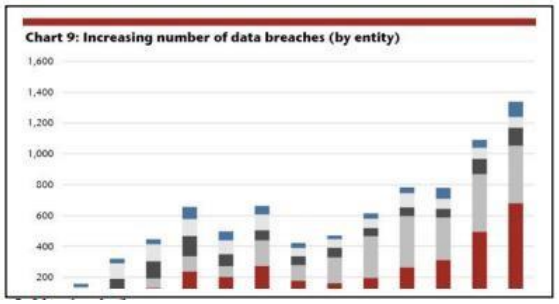


Fig 4. Identity theft as per year

TABLE I

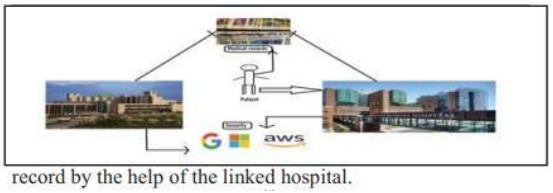
Data Leak Incidents in Recent Years (Data Source Is from the Dataset o
World's Biggest Data Breaches

Organization	Records	Breach Date	Type	Source	Industry	Estimated Cost
Anthem insurance	78 million	January 2015	Identify theft	Malicious outsider	Healthcare	$100 million
Yahoo	500 million	December 2014	Account access	State sponsored[1]	Business	$350 million
Home depot	109 million	September 2014	Financial access	Malicious outsider	Business	$28 million
JPMorgan chase	83 million	August 2014	Identify theft	Malicious outsider	Financial	$13 billion
Benesse	49 million	July 2014	Identify theft	Malicious insider	Education	$138 million
Korea credit bureau	104 million	January 2014	Identify theft	Malicious insider	Financial	$100 million
Target	110 million	November 2013	Financial access	Malicious outsider	Business	$252 million
Adobe System	152 Million	September 2013	Financial access	Malicious outsider	Business	$714 Million

SOURCE: AWS NETWORK

VI. OUR PROPOSED SOLUTION

Patient and doctor may view one other's medical records with only a login id and password, making the system more vulnerable to hackers. As shown in fig. 1, our suggested solution involves the hypothetical scenario of a person from India relocating to the U.S. state of California. Now that he needs access to his records, which are stored at a hospital in India, we'll set up a connection between hospitals in California and India; the security of this system will be handled by third-party providers like Google, Microsoft, and Amazon Web Services (AWS), making it less vulnerable to hacking and more private for the patient. Medical records are now more secure, and patients have easier access to them.



record by the help of the linked hospital.

Fig 5. Our proposed plan

The security providers like Google, Microsoft and AWS provides the best data security against the data stealth and hacking, which is being proved by the statistical data of the breach in security in the previous years.[10] Who were behind the attacks?

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

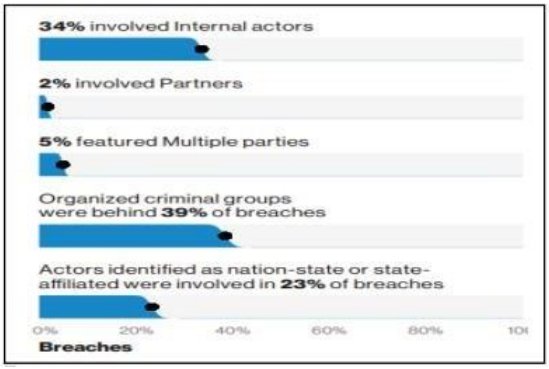


Fig 6. Who behind the breach

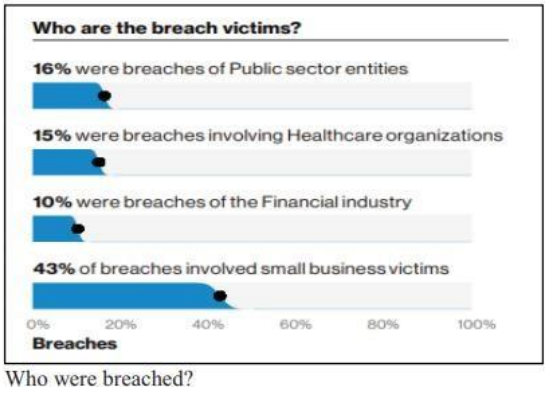


Fig 7. Victims of breach

How they were breached: As companies continue to transition from their emails and by simple transition techniques, Criminals simply shift their focus on the most valued information which is health records. Increase in the hacking of cloud-based email servers. It doesn't imply that cloud services are less secure;

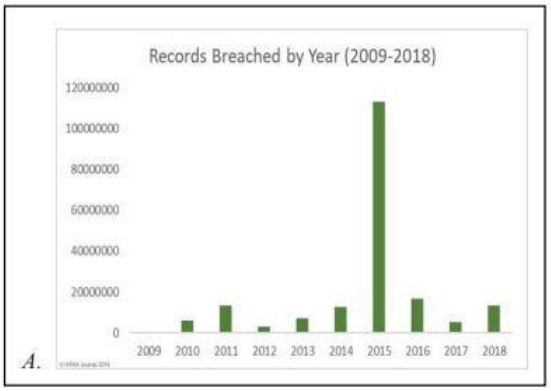


Fig 8. Records of breach by year

These security providers use a technique called LastPass which is a hashed algorithm that cannot be reversed which make it very difficult for the attacker to compromise.

VII. CONCLUSION:

Based on the preceding discussion, we have concluded that the traditional methods are more vulnerable to hacking because they rely on simple techniques like login and accessing the medical records by the patient or the doctor, whereas the method we have proposed is less vulnerable to hacking because it involves communication between hospitals rather than directly to the patient, who is more vulnerable to hacking because his or her information is not protected with security of tech co. The only drawback of this new method is that it is not as efficient as that for a long-distance idea, since for

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

short distance the person still has to go to the nearest hospital to get the data. However, as was shown in the introductory section, this kind of problem has been addressed before, albeit not in the same manner or with the same proposed plan as of this paper.

REFERENCES

[1]. Islam M, "Mobile Cloud-Based Big Healthcare Data Processing in Smart Cities," Research Gate"," Md. Mo fijul Islam". May 2017,pp 8-9.

[2].Mu-Hsing Kuo A "Opportunities and Challenges of Cloud Computing to Improve Health Care Services"," Journal of Medical research"VOL13., September 2011, pp 9-11 .

[3].Haghi M, MSc. centre for Life Science Automation "Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices"" The Korean Society of Medical Informatics", Health Inform Res., Jan 31, 2017, pp 7.

[4].Sharma S,Chen K,Sheth A, "Towards Practical Privacy-Preserving Analytics for IoT and Cloud Based Healthcare Systems" IEEE Internet Computing" Ohio Centre of Excellence in Knowledge-enabled Computing", Wright State University, Dayton, OH ,Jan 31 2017,pp 14.

[5]. Prasadu Peddi (2023), Using a Wide Range of Residuals Densely, a Deep Learning Approach to the Detection of Abnormal Driving Behaviour in Videos, ADVANCED INFORMATION TECHNOLOGY JOURNAL, ISSN 1879-8136, volume XV, issue II, pp 11-18.

[6].Chen M, Yang J, Hu L, Shamim Hossain M, Muhammad G" Urban Healthcare Big Data System based on Crowdsourced and Cloud-based Air Quality Indicators"" IEEE COMMUNICATIONS MAGAZINE, VOL. XX, NO. YY", October 2018,pp 9-11.

[7]. Xu B, Xu L, Jiang L,Luo J,Gu L." Challenges faced in m-Health Monitoring System"" Enterprise Information Systems"" , 15 June 2015,pp 11-12).

[8].Casola V, Castiglione A, Choo K, Esposito C." Electronic Health System is underlying security and privacy." "" Daniele Chatted and Giles Hogben"" Anise European Network and Information Security Agency", December 2016,pp 6.

[9].Xhafa Email Jingwei F, ZhaoJin L, Chen Duncan L, Wong S" Designing cloud-based electronic health record

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

system with attribute-based encryption”” Department of Computer Science City University of Hong Kong Kowloon Hong Kong”, 11 February 2014,pp7-10.

[10] Jayabalan M, O’Daniel, T “Access control and privilege management in electronic health record :-a systematic literature review.”” Asia Pacific University of Technology and Innovation Kuala Lumpur Malaysia”” Thomas O’Danie”, 08 October 2016, pp-8cited.

[11] Prasadu Peddi (2021), “Deeper Image Segmentation using Lloyd’s Algorithm”, ZKGINTERNATIONAL, vol 5, issue 2, pp: 1-7.