ISSN: 2278-4632
Vol-13, Issue-08, August 2023

SECURING CLOUD-BASED INFORMATION SHARING WITH TWO-FACTOR AUTHENTICATION

[#1]BARLA REKHA,

[#2]Dr.P.VENKATESHWARLU, ***Associate Professor,***

[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA.

ABSTRACT:-This study proposes a methodology for improving security and predictive analytics for hospital management systems by utilizing cloud-based clinical and patient records with sufficient storage capacity, data access for only authorized users, low-cost medical services, and implementation. Authorized users gain access to the upgraded system using two-factor authentication (password and token). Specifically designed to increase the level of security in hospital management systems by providing greater security for essential information transmission. The application was built using the Django framework, a machine learning approach, and the Python programming language. When tested, the created model was shown to be more effective than previous ones in terms of security, stakeholder participation, access control, data protection, and adaptability. Accessing a patient's medical data takes an average of 10.95 seconds, according to tests on token authentication and verification times, which is not long enough to risk security.

Keywords:-*Cloud Computing, Electronic Medical Record,DataMining,Two-Factor Authentication.*

1. INTRODUCTION

Cloud computing refers, in general, to utilizing remote servers to provide various computing functions. It provides a shared pool of reconfigurable computing resources with an on-demand network access architecture that is simple to distribute. The advent of cloud computing and the associated business practices ushered in significant transformation across several sectors in the twenty-first century. Cloud computing allows a group of end users to share computing resources and data storage. Cloud computing has flourished thanks to advancements in technologies like distributed computing, parallel computing, grid computing, virtualization, utility computing, IaaS, PaaS, and SaaS. By utilizing cloud computing, it is not necessary to have specialized software in order to monitor the sharing of information and apps. All that is required is an internet connection. In Figure 1 we see what a typical cloud computing setup looks like.

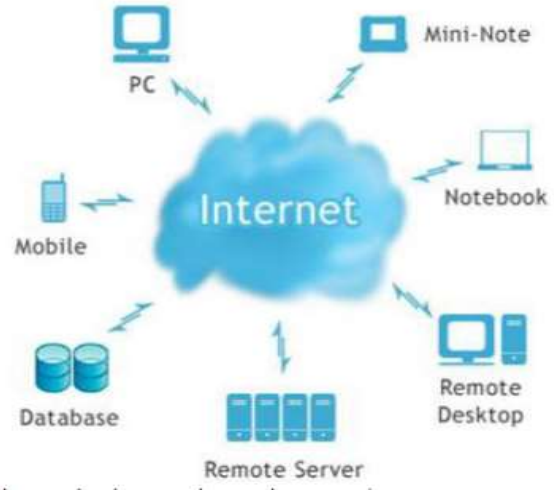

Fig1:-Cloudcomputingenvironment (Source: Mansoretal.2013)

Data mining is the practice of sifting through large datasets in search of meaningful information. A

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

reliable method of data collection, storage, and processing is required for data mining. For a long time, effective data collection and processing has been a major concern due to the exponential growth of data, which can range between Petabytes and Exabytes.

A patient's medical record is a confidential document that is kept by a doctor or other healthcare provider. Information such as the patient's name, residence, and date of birth are included in this summary, as are the patient's symptoms, diagnosis, therapies, and outcomes. The primary function of a patient's medical record is to document their experiences with healthcare providers for the purpose of improving their future treatment.

The technical connections between automated data mining and cloud storage are simple to establish.Convergence streamlines the retrieval of massive amounts of data from disparate sources in a short amount of time [6]. Data from patients, such as glucose and blood pressure levels, are initially stored on the cloud. The technology is designed to be used by both the medical staff and the patient. Information on a patient can be safely stored in a variety of formats, including text, X-ray images, and scans. Medical records for registered patients are kept in the cloud where they may be accessible by any licensed doctor in the area whenever they need them.

2. LITERATUREREVIEW

Electronic Health Record

EHRs, or electronic health records, are digital versions of a patient's medical history that may be accessed in a number of different medical facilities. Health information is gathered, created, and stored digitally in electronic health records. This system makes it simple to transmit and store sensitive medical information in remote servers or the cloud. There has been a sluggish adoption of EHRs among medical professionals.

Clinical documentation can be more trustworthy, trackable, billable, and codeable with the use of electronic health records. You are free to carry these documents with you as well. Biodata, medications, allergies, vitals, prior lab results, doctor visits, and administrative data are just some of the information that may be found in an electronic health record. Electronic health record (EHR) systems are networks of connected medical institutions such as labs, medical imaging facilities, pharmacies, schools, and workplace clinics that clinicians can access from any legitimate healthcare facility or private company in the country.

Two-Factor Authentication

Two-factor authentication (2FA) is a way of verifying a user's identity that requires them to present proof of their identity from two independent sources. This occurs in the course of several transactions, including registration. Two-factor authentication makes use of biometric verification and behavior-based permission. Inherence-based authentication relies on a user's possession of a token or knowledge of a password to verify their identity. Verification of the Information Pool (Point 10). Two-factor authentication (2FA) is an extra security measure put in place to make it more difficult for an intruder to access a restricted area, network, or database. If one defense is breached, progress cannot be made until all others are also removed.

Related Work

according to B. Kamala (2013), users can gain access to valuable data from a virtually integrated data warehouse while saving money on infrastructure and storage by integrating data mining services into cloud computing (IDMCC) and using case studies such as hospital-based electronic health records (EHRs), community-based health information sharing, personal health records (PHRs), and patient accounting, financial, and billing systems. Kamala's plan helps small firms who utilize the IDMCC.

An improved method of linking HDOs in low-income countries to the cloud was developed by Samuel et al. (2013). With issues like medical data security and a lack of data mining resources, this was done to aid these institutions. Their

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

proposed approach aimed to build a Data Security and User Authentication Engine (DSUAE) that employs common encryption and decryption technology to keep patients' medical records private from prying eyes. In their conclusion, Samuel et al. (2013) noted that the management of Health Delivery Organizations or other interested parties might use the model's data to make educated decisions that would contribute to the social and economic stability of developing countries.

Security and privacy concerns have been significant obstacles to the system's development from the start. Using the Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC) security models, Gajanayake et al. developed an access control design for the electronic health system. Their software facilitates access to and management of electronic health records for both individuals and medical professionals. This approach only works for electronic health records, which is the biggest drawback.

Using cloud computing, the healthcare industry may now safely offload its patients' sensitive data to a remote server. Kester et al. (2015) investigated the business application of encryption for safeguarding personal information and authentication procedures. This was accomplished by developing an encrypted and watermarked system for processing medical photographs. They also developed new watermarking and reverse-encryption techniques tailored to particular fields. This is how protected medical imaging data is stored digitally. The framework is limited to images and cannot process text or audio.

To authenticate users and shield sensitive information, Guo et al. (2012) proposed PAAS (Privacy-Preserving Attribute-Based Authentication System), which relies on users' independently verified qualities. This is due to the fact that the preexisting e-health system did not preserve the confidentiality of patients' personal attribute information while maintaining the original capabilities of medical services. They devised a two-way administrative system, unlike the standard centralized approach, in which both the patient and the doctor are participating in the authentication and permission processes. Users have access based on their rights and are not required to identify themselves or explain their medical condition. Their approach considers a wide range of users and their respective privacy and safety concerns. However, the ease with which medical data can be shared across domains is uncertain. The authors acknowledge that it will be challenging to demonstrate the viability of this paradigm in the actual world through its application.

Single Point of Contact (SPOC) is a crucial component of the Data Capture and Auto Identification Reference (DACAR) platform that was established after extensive research by Fan et al. (2014). This is another evidence that the security of the e-health system must be strengthened. It is claimed that this feature enables claims-based authentication and authorisation, which in turn enables dependable cloud-based e-health services. This system produces satisfactory results. However, their proposed fix isn't available to more than a select few.

The Attribute Based Encryption (ABE) Technique is being reevaluated in light of Kumar et al.'s (2013) revised proposal for an electronic health architecture. They devised a system to classify individuals as either "Public Domains" or "Private Domains." In this architecture, a user can only access and decrypt information within its own private space. However, a user in the public domain can employ multi-authority ABE to increase the safety of these domains. This is an excellent plan of action. A major hurdle for scalability and individuality is the addition of attribute-based encryption to the Electronic Health Record system, which is a massive and complex administrative undertaking.

CHALLENGESFACINGCLOUD-BASEDMEDICALRECORDSYSTEMS

The objectives of any system, manual or electronic, used to keep medical records are the

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

same. However, these approaches vary considerably in terms of how the user enters and retrieves information from the record and how they interact with the system. While electronic health records (EHRs) have been heralded as a tool to improve the healthcare system and increase efficiency, they have also been shown to cause a slew of new, significant issues. The time it takes to diagnose a patient's condition could be reduced with the help of EHRs, as could the likelihood of adverse drug reactions and the overall quality of care provided. This is significant due to the widespread practice of patients seeing multiple primary care physicians and specialists over the course of a year. However, many people are concerned that their personal information would be compromised if their data are made public. Some high-profile patients still won't sign on for this treatment despite its many advantages. The patient must be viewed as an integral part of the team if this movement is to get widespread support. Patients need to give their permission for a health official to utilize 2FA to access their medical records.

3. MATERIALS AND METHODS

Stakeholders worked with developers using the Object-Oriented Methodology (OOM) to create a comprehensive electronic hospital administration system hosted in the cloud.OOM is a method of construction that promotes and facilitates the reusing of software components. A modular computer system can be constructed in this manner. This facilitates component sharing and the reuse of individual components. More people can be served by combining these elements in various ways.

Set up

This plan aimed to establish an EHR system that met the highest standards of security, adaptability, and dependability. The EHR system is overseen by the individuals who care about it the most: the approved health officials and the patients. After verifying their identity at a certified hospital, patients will be given unrestricted access to all hospital services. He is currently recruiting doctors to join his team. The patient's Token Verification security system may also allow the health officer (HO) access to the patient's cloud-based medical records.

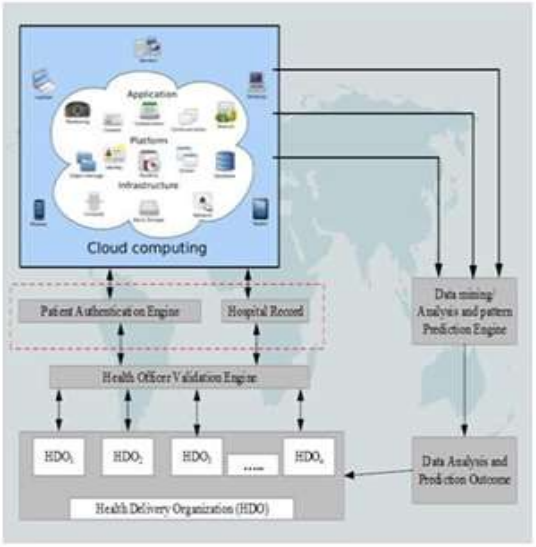

Fig. 2:- Secured Cloud-Based for Electronic hospitalmanagementsystem.

Figure 3 depicts a subset of the system components, including the Health Delivery Organizations (HDOs), the Cloud, the Data Mining/Analysis and Pattern Prediction Engine (DMAPPE), and the Two-Factor Verification Engine (DFVE) for patients and health officials.

Many different HDO departments, including hospitals, radiology, laboratories, pharmacies, billing, etc., contribute data to each EHR kept by each HDO. It's also crucial to remember that HDOs are the means by which users of the platform connect to the cloud.

Patient records and other essential healthcare data are safely stored in the cloud. In addition, it provides authorized users with access to numerous services. The computational component also provides the required network support.

Authentication of Users: Users can be anyone from patients to medical professionals to scientists to technicians to other researchers. Data security and privacy are apparent concerns given the widespread adoption of cloud computing. Each user was identifiable in their own special way, hence a multi-factor approach was adopted. DMAPPE takes a look at the query and cross-references it with its stored information to see if

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

it's similar to anything it already knows.

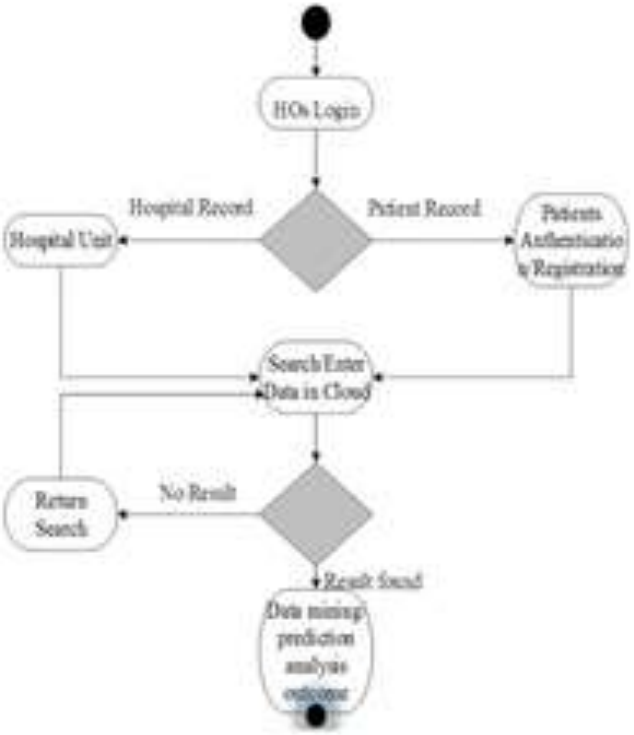

Fig.3.UseCaseDiagramforthedevelopedsystem

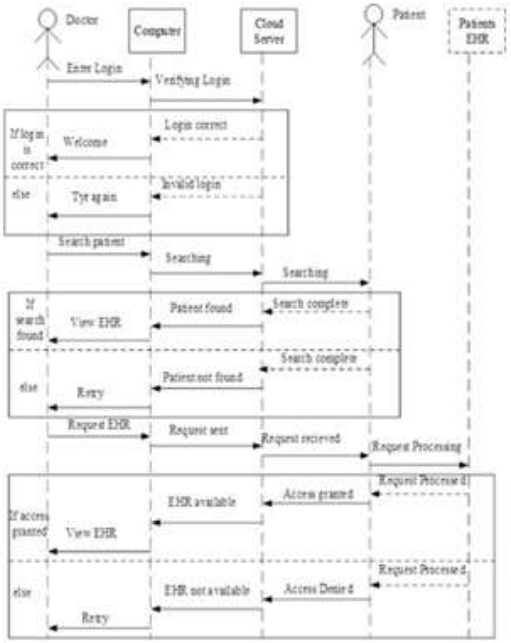

Fig.4.Sequence Diagram for the developed system.

4. RESULTS AND DISCUSSION

Table1:-System Metrics Indicator

Features	Rate	Scale
Access Control	XXX	30
Security Analysis	XXXX	40
Data Privacy	XXXX	40
Data Integrity	XXXX	40
Flexibility	XXX	30
Data Sharing	XXX	30

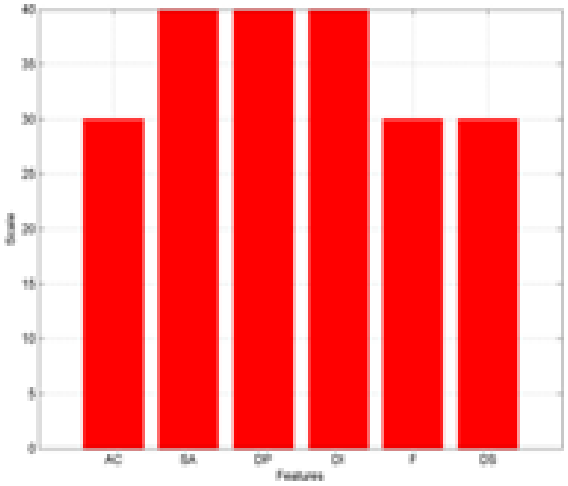

Fig.5.SystemPerformanceIndicatorChart

Use Case, Unified Modeling Language, and Sequence Diagram analyses were used to quantify the system's level of security and performance. You'll need performance metrics to determine the severity of the security threat. The current state of security in the system is shown by these metrics. Access management, security analysis, privacy, integrity, adaptability, and data sharing are all critical success factors.

Assuming that X = 10 is correct, we can convert each statistic to a numeric value to better understand the system. The system's level of security is displayed in both tabular (Table 1) and graphical (Figure 5) formats.

Table 2: Token Time Interval

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

Patients	Time Sec	Patients	Time Sec
1	9	11	10
2	11	12	7
3	5	13	5
4	7	14	10
5	15	15	13
6	8	16	15
7	20	17	6
8	15	18	7
9	10	19	16
10	18	20	12

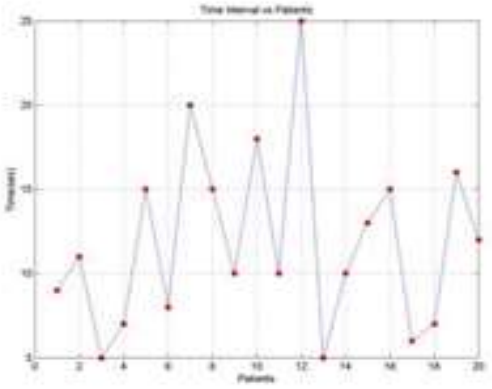

Fig.6.TokenTimeInterval

One of the most important features of this system is how quickly the token can be sent, received, and validated in order to gain access to the patient's medical record. How quickly the token reaches the patient's device is affected by factors including the connection speed and storage capacity of the mobile device. Twenty persons from all over the United States were entered as patients into the electronic health record system.

The time it would take for a patient to send, receive, and log into an electronic medical record was then calculated using token identification and verification. In settings that prioritize patient privacy, the average of 10.95 seconds required to get a patient's medical records is not a security risk (see Table 2 and Figure 6).

5. CONCLUSION

Overall, health care delivery organizations (HDOs) have poor data management. The improper handling of clinical notes is responsible for numerous avoidable deaths annually. This is due, in part, to a number of factors, including but not limited to: high health care costs; limited access to educated health care workers and facilities; inaccurate diagnosis and treatment; and an inadequate system for storing clinical and medical data. Our work provides healthcare service providers with a safer and more reliable cloud-based infrastructure on which to execute their operations. The proposed system includes safeguards to prevent unauthorized individuals from accessing sensitive electronic health records. An OTP is used for this purpose. Important data can also be gleaned from the app's built-in machine learning prediction system.

REFERENCES

[1].Srinivasa, R., Nageswara, R., and Ekusuma, K.,2009.“Cloudcomputing:Anoverview,”JournalofTheoreticalandAppliedInformationTechnology(JATIT),Pp. 71-76.

[2].IBMCorporateMarketingWhitepaper,“Cloudcomputing:BuildinganewfoundationforHealthcare,”.ibm.com/cloud,2011.

[3].Zimmermann, H. J. (2006). Knowledge Management,Knowledge Discovery, and Dynamic IntelligentDataMining.CyberneticsandSystems:An InternationalJournal,37(6), pp. 509-531.

[4].BecerraFernandez,I.&Sabherwal,R.(2010).KnowledgeManagement:Systemsandprocesses...New York:MESharpe.

[5].DU,H.2010.DataMiningTechniquesandApplications: AnIntroduction.Hampshire:Cengage.

[6].K. ShanthaShalini, R. Shobana, S. LeelavathyandV.Sridevi.ACloudBasedApproachforHealthCareManagement.Int.J.Chem.Sci.:14(4),2016,2927-2932.

[7].Sanjay,P.A.,Sindhu,M.,andJesus,Z.2012.“ASurvey of the state of Cloud computing in Healthcare,”in Canadian Center of Science and Education,NetworkandCommunicationTechnologies;Vol.1,No.2;ISSN1927-064XE.

[8].Jun Zeng (2018). The Development and ApplicationofDataMiningBasedonCloudComputing.J.Phys.:Conf.Ser.1087032008
[9].MansorZauir, Mohamad M. Al Rahhal, Abdullah Al-Faifi, Alaaeldin M. Hafez, Hassan Abdalla (Jan, 2013).SurveyofDataMiningUsageinCloudComputing
[10]. TamaraSMohamed(2019)SecurityofMultifactorAuthenticationModeltoImproveAuthenticationSystems.CihanuniversitySulaimaniah,Iraq
[11]. B. Kamala, (2013) A Study on Integrated Approach ofData Mining and Cloud Mining. InternationalJournalofAdvancesinComputerScienceandCloudComputing,ISSN:2321-4058Volume-1,Issue-2,
[12].Samuel,O.W,Omisore,M.O,Ojokoh,B.A,Atajeromavwo,E.J,(2013)EnhancedCloudbasedModelforHealthcareDeliveryOrganizationsinDeveloping Countries.InternationalJournalofComputerApplications(0975–8887)Volume74–No.2,(July2013)
[13]. Gajanayake R, Iannella R, Sahama T. Privacy orientedaccess control for electronic health records. e-JHealthInf(2014);8(2):175–86.
[14]. Kester,Q,Nana,L,Pascu,A,Gire,S,Eghan,J,Quaynor, N. A Security Technique for Authenticationand Security of Medical Images in Health InformationSystems.In:2015 15thInternationalConferenceonComputationalScienceandItsApplications,Banff,AB,Canada, (2015), pp.8–13.
[15]. Guo, L, Zhang, C, Sun, J, Fang, Y. PAAS: A Privacy-Preserving Attribute-based Authentication System foreHealth Networks. In: 2012 32nd IEEE InternationalConferenceonDistributedComputingSystems,Macau,China, (2012), pp.224–233.
[16]. Fan, L, Lo, O, Buchanan, W, Ekonomou, E, Sharif, T,Sheridan, C., SPoC: Protecting Patient Privacy for e-Health Services intheCloud.(2014),pp.1–6.
[17]. Kumar M, Fathima M, Mahendran M. Personal healthdata storage protection on cloud using MA-ABE. IntJComputAppl(2013);75(8):11–6.