Smart Health Consultation and Record Management

Jatin kumar Chaurasia*, Utkarsh Shukla **, Urvi Verma **, Ashish Kumar Pandey**

* Computer Science & Engineering, IET Dr. RML Avadh University, Ayodhya, India
** Computer Science & Engineering, IET Dr. RML Avadh University, Ayodhya, India

DOI: 10.29322/IJSRP.12.08.2022.p12852
http://dx.doi.org/10.29322/IJSRP.12.08.2022.p12852

Paper Received Date: 3rd August 2022
Paper Acceptance Date: 18th August 2022
Paper Publication Date: 24th August 2022

Abstract- There is currently a lot of study being done on the functioning of Electronic Health Records (EHR) software, and doctors are facing a lot of difficulties as they switch from a paper-based record management system to an electronic one. Our goal is to help healthcare providers embrace EHR software and improve the clinical and practise management aspects of their operations. The health reports of the individuals, which also include diagnostic data and medical prescriptions, are delivered in the form of papers, the subsequent hospital visit by the individual is blind to the individual's prior medical conditions and medications. However, this issue is lessened by storing a person's entire health record as a soft copy in the cloud. If they haven't already, healthcare providers are under increasing pressure to embrace an EHR. In order to avoid making a blind faith decision, providers should modulate their response to this pressure. In this study, examine 'what trust means and present a metric of dependability'. Cloud based EHR Rank is used in this work. The measure of trustworthiness quantifies how successfully someone. EHR addresses provider needs and essential operational requirements. The certainty is used as the trustworthiness metric. The standard of the evidence used to assess the EHR is a consideration. The reliability model offers a framework for contextualizing and ranking crucial choices issues, as well as using risk-reduction techniques decision-making while choosing an EHR should be improved.

Keywords- Electronic health records, Cloud computing trust, EHR policies, Risk mitigation.

I. INTRODUCTION

Today, everyone's life revolves around their health, and compared to the last several years, health issues have sharply increased. In spite of the fact that Indian doctors are doing a fantastic job at reducing health issues, many patients are losing their lives because the country's poor population cannot afford the proper care from the appropriate physician at the appropriate time. Now technology has advanced quickly, and our government is working to make sure that everyone in the nation has access to the internet. Using these facilities, we have created a central hub that houses all patient data, including diagnostic results and doctor-prescribed medications. It functions as a cloud, from which any doctor, with the patient's consent, can retrieve data from any location. The use of the internet has allowed us to create a central hub that stores all patient data, including diagnostic reports and prescriptions from doctors. This hub serves as a cloud from which data can be accessed from any location and by any doctor with the patient's consent. Today, technology has advanced quickly. Our government is working to bring internet access to every part of the nation. The doctors can learn about the patients' prior medical issues with the use of this, and they can treat the patients quickly by taking into account these requirements and the medications they used .We also provide you the chance to review the hospitals based on the experiences of the people who received care there. Numerous legislative, insurance, legal, and governmental measures aimed at encouraging the widespread implementation of health information technology are transforming the healthcare sector (HIT). Here are a few instances: The American Recovery and Reinvestment Act (ARRA) of 2009 set up nearly $17 billion to pay qualifying hospitals and healthcare providers back for costs associated with implementing electronic health records systems (EHRs) through 2016, these reimbursement incentives are available [1,2,3]. After then, penalties in the form of lower Medicare reimbursement rates will take the place of the incentives. The Patient Protection and Affordable Care Act (PPACA) of 2010 revised the False Claims Act (FCA) by adding additional measures for penalties, criminal fines, and jail time to deter fraud and abuse among providers participating in Medicare, Medicaid, and the Children's Health Insurance Program (CHIP)[4] . EHRs gather the evidence required to back up claims made to government health care programmes and show that patient care complies with or exceeds industry standards. Receiving the greatest rates on malpractice insurance and reimbursements from patient care insurance is a perk for providers who utilise government-certified EHRs [5]. A growing number of healthcare professionals are being persuaded by these activities to revaluate their reliance on paper-based clinical and practise management record keeping systems. By a ratio of nine to one, providers have avoided EHRs thus far. The causes are numerous and

include when used incorrectly, EHRs expose the practise to risks and liabilities. Health Insurance Portability and Accountability Act (HIPAA) [5] regulations that apply to EHRs are more stringent than those that apply to paper-based recordkeeping. Last but not least, EHRs are pricey, with acquisition expenses per qualifying provider ranging from $10,000 to $100,000. Finally, EHRs frequently require a lengthy learning curve. EHR selection, deployment, and maintenance are technically demanding; typically, physician productivity drops by 30% or more when EHRs are first deployed and does not increase until the system has been utilized for six to twelve months. Between 40% and 60% of EHR deployment initiatives are thought to fail. EHRs are available as on-site or cloud-based systems. Locally, in the practice office, an onsite EHR is kept up to date (s). This strategy necessitates a substantial investment in technical support personnel, computer hardware, and software. A third-party hosting service manages and backs up software and data files through a cloud-based solution releasing providers from their obligations. In order to access the cloud using a web-enabled browser, providers must maintain end-user PCs and network connectivity; nevertheless, this is far simpler and less expensive than installing an entire on-site EHR. In general, providers are wary about cloud-based EHRs because they believe they are more dangerous and unreliable than on-site EHRs . When depending on a third party to gather, retain, and secure clinical and practise management data, physicians have valid concerns about preserving patient privacy and confidentiality as well as the requirement to adhere to HIPAA and other governmental regulations [16]. However, many medical institutions, particularly small ambulatory clinics, lack the funds and knowledge necessary to keep an in-house EHR safe. They may actually be more vulnerable if the necessary systems, methods, and procedures aren't in place [3] than if these duties were delegated to a trustworthy, competent outsider. Providing healthcare workers with the resources they need to make knowledgeable decisions about health information technology is one of the objectives of the authors' research. As a result, the adoption of EHRs is neither outright rejected out of fear nor adopted without the necessary due diligence. The choice to use an EHR is ultimately based on the practitioner's confidence that the advantages will exceed the drawbacks. Choosing a solution that is well aligned to the providers' technical, functional, governance and compliance requirements is essential to building confidence.

Rest of this paper is organised as follows: II. Trust-blind or not ?, III. Strategies for mitigating risk, IV. Requirement and importance of cloud based smart health consulting, V. Data analysis, VI. Proposed methodology, VII. Conclusion

II. TRUST – BLIND OR NOT?

Numerous views and academic fields, such as psychology, sociology, economics, computer science, and decision theory, have investigated the concept of trust extensively in the literature. The idea of trust is nuanced, multifaceted, and situational. Trust may be founded on factual information, personal opinion, and previous experience [6,7,8,9]. There is no single, comprehensive definition of trust that can effectively capture all of its facets. According to [11]"assurance" and confidence that people, data, entities, information, or processes will work or behave in expected ways, trust revolves around these concepts. Trust can exist between humans, machines, humans and machines, and machines and humans. Trust may be seen, at a deeper level, as a result of achievement of security or privacy goals. Both known and unknown threats exist throughout the cosmos, as seen in Figure 1. Ideally, explicit knowledge of known knowns and known unknowns should serve as the foundation for confidence. .Without it, faith is blind. Unknown unknowns result in unforeseen issues and prevent preventative remedial action. When providers are unaware of their own needs and the constraints of HIT, unknown unknowns develop. For instance, providers who buy EHR solutions based solely on referrals from peers or other outside parties without further investigation do so at their own risk. There are numerous anecdotal reports of providers signing long-term contracts only to discover that the chosen solution does not match their demands. While useful, industry certifications and evaluations of EHR offerings do not provide a comprehensive picture. For instance, in order for EHRs to be certified as meeting Meaningful Use requirements, the Office of the National Coordinator - Authorized Testing and Certification Body (ONC-ATCB) has created standards. Physicians that accept Medicare and Medicaid patients can qualify for government Meaningful Use (MU) incentives by using an EHR system that has been approved by the ONC-ATCB. The bigger question of whether the EHR is appropriate for the practice or incorporates industry best practices for online security and privacy, however, is not addressed by the EHR's support for MU standards.

For the past 20 years, ICSA Labs, a separate branch of Verizon Business, has offered trustworthy "independent, third-party product assurance for end users and organizations. Many of the best security product developers and service providers in the world have used ICSA Labs to provide vendor-neutral testing and certification for hundreds of security products and solutions [6]. Businesses all over the world depend on ICSA Labs to establish and implement impartial testing and certification standards for evaluating product compliance and performance. On its website, ICSA Labs offers free access to the certification outcomes for EHR software. Notably, the surveys don't include many popular EHRs with sizable market shares. There are numerous EHR products available. Many of the facts necessary to decide intelligently about their functioning, safety, privacy, and resilience are hard to get or not available in a way that allows for straightforward comparison. Cloud-based EHRs are deceptively challenging to secure and susceptible to a wide range of internal and external attacks. Providers who are thinking about using a cloud-based EHR must deal with a lot of unanswered questions. To aid in quantifying these uncertainties, a multi-criteria decision model is described in the next section.

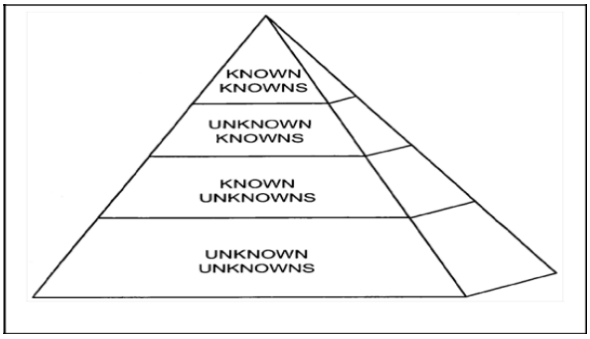

Figure 1: Universe of Unknowns and Knowns [21]

III. STRATEGIES FOR MITIGATING RISK

Risk mitigation techniques may be helpful in making up for EHR flaws discovered during the review process. Risk can be managed in three ways: by reducing it, controlling it, and transferring it. Using a disaster recovery and data continuity strategy, for instance, can help with risk reduction and risk control. Transferring risk includes transferring responsibility for exposure to a different entity, frequently through outsourcing or insurance. When an EHR solution that uses the cloud is used, system data is kept at the hosting service, most likely in an unidentified location. Physicians are nonetheless accountable under HIPAA rules if protected data is breached by unauthorized individuals, even though they are delegating the duty of data maintenance to a third party.

In order to prevent unauthorized individuals from reading protected, confidential, or sensitive health information and practice management data, providers must ensure secure end user computers and network connectivity. This article's description of a thorough due-diligence evaluation is an example of risk minimization. It lessens the possibility of choosing a subpar EHR. The methodology put forth here offers a framework for contextualising and ranking crucial factors. This tool should only be used after carefully reviewing the needs of the practise and with the guidance and support of knowledgeable information technology professionals and legal counsel. Following the computation of the Trustworthiness ratings outlined in the previous section, a straightforward graphical analysis is advised. Comparing and visualizing the relative advantages and disadvantages of each EHR is made simpler by a bar chart representation of the weighted Dj. components of the top ranked EHRS. According to Fig. 2 , EHR #1 outperforms EHR #2 in all categories besides functioning. EHR #2 would most likely win if a provider were to base their choice only on functionality, despite serious doubts about the vendor's reliability and the security of the system. Both options should be chosen if the capability offered by EHR #2 is essential to the success of the EHR implementation and is not supported by EHR #1.

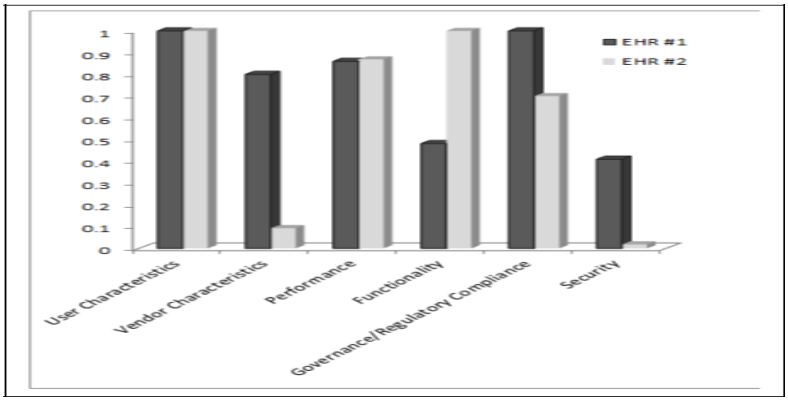

Figure 2: Comparison of Decision Factors in Top Ranked EHRs [21]

IV. REQUIREMENT AND IMPORTANCE OF CLOUD BASED SMART HEALTH CONSULTING

Every person in our country has an individual identifying number provided by their Aadhar card. Using this number, we may keep that person's data independently in the cloud. Every hospital, medical store, and diagnostic facility must have a distinctive identification number to be recognised. With this number, they can log into the cloud and enter reports using the person's Aadhar number. Each

hospital is required to keep their database up to date so that all patient information can be saved there. The hospital's database's information must be uploaded to the cloud. The patient's information will be saved on a cloud server in each city and village, which will be connected to the central hub [19].

- **Cloud data storage**

Data can be entered into the cloud using laptops, smartphones, and other devices.
The data storage diagram [17,19] in the cloud is shown below:

Figure 3: Storing data into cloud [17,19]

- Check that the cloud we are utilising is current;
- Verify that the distant servers are operational and have access to the internet.
- Verify that the cloud is receiving data updates from the remote servers.

Hospitals, diagnostic facilities, and retail medical businesses must first authenticate with the cloud before submitting data. In other words, customers must provide their password and unique government-issued ID to connect in to the cloud. With the aid of their Aadhar number, patients' information must be entered into the cloud when they attend hospitals.Doctors need computers so they can write up prescriptions for patients and enter the information (the prescription) immediately into the patient's cloud. The medical stores must fulfil the patients' requests for medications, and data must be entered in the cloud belonging to the patient.

By adhering to the following authentication criteria, the data security can be provided as the Aadhar cards are successfully deployed in our nation, they can offer each and every person an individual authentication. Every person must sign up for an account in the cloud using their Aadhar and provide a security password so that only they may access their data. In order to write prescriptions for patients and promptly enter the information (the prescription) into the patient's cloud, doctors need computers. Patients' orders for pharmaceuticals must be fulfilled by medical supply stores, and patient-specific data must be entered in the cloud.
The following authentication standards can be followed to guarantee data security:
The Aadhar cards can provide each and every person with a unique authentication as they are successfully implemented in our country.
Each person must create a cloud account using their Aadhar number and enter a security password to ensure that only they have access to their data. Only those who are permitted may enter data. The patient's data can be entered in the cloud by first verifying oneself and then using the patient's Aadhar card number.

Obtain data from the cloud:

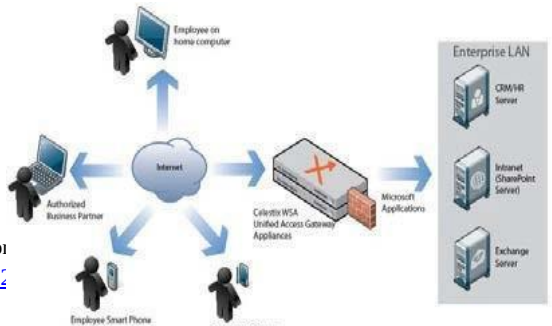

Figure 4: Retrieving data from cloud [19]

An individual can retrieve their own data by themselves. Smartphones, PCs, and laptops that are linked to the internet can access the data stored in the cloud. The individual must verify himself with the cloud by supplying his Aadhar id and the password in order to retrieve the data from it. He can access the cloud-based data when both the Aadhar ID and the password are accurate.

V. DATA ANALYSIS

The information that is gathered and stored in the cloud can be analysed to help the organization determine the patient's current state of health. With this knowledge, they can then advise their patients to follow certain lifestyle guidelines that are suitable for them based on their health conditions. Analytics can be utilized to suggest lifestyle changes for a particular patient. This places a high priority on the health of the patient, and I don't believe anyone will object to being reminded to take care of themselves. How to examine the cloud-based data: Unstructured data will make up the data saved in the cloud [15,19].

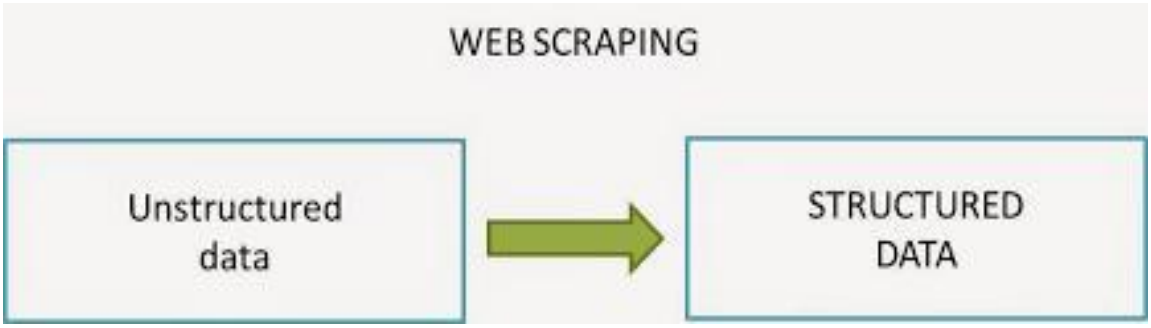

Figure 5: Converting unstructured data to structured data

By using data mining techniques like data cleansing, unstructured data should be transformed into structured data.

- Transformation of data.
- Pattern Recognition.
- Visualization of data.

After the unstructured data is converted into structured data, the data is compared to the standard values; if there is a difference between the standard value and the output, the patient is informed to take care and is given instructions on the precautions they should take.

The illustrations that illustrate how structured data can be seen are as follows:

• Table Format, Cluster Format, and Graph Format.

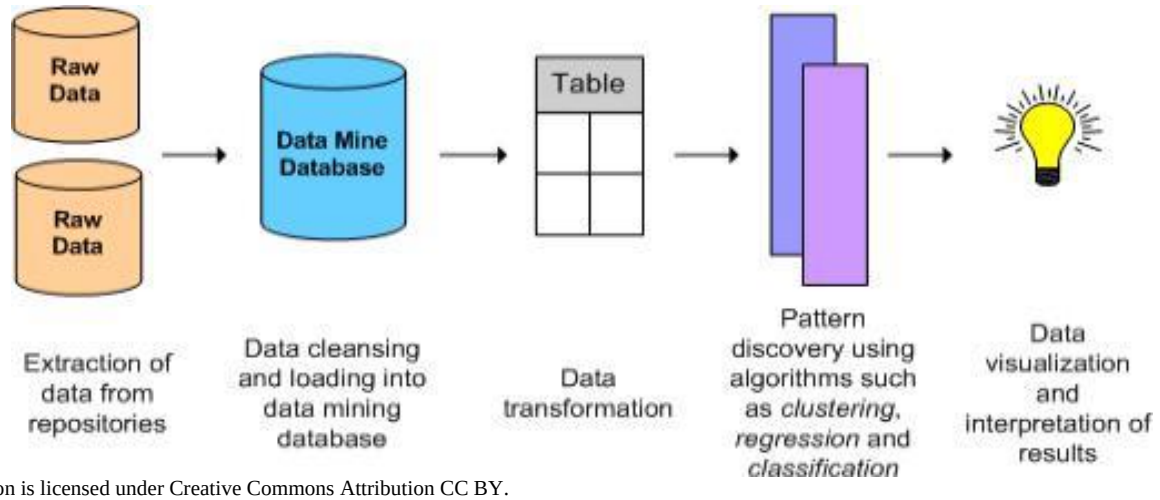

Figure 6: Data mining process [19]

VI. PROPOSED METHODOLOGY

In this section, explained the methodology of the proposed model represented in figure 7.

1. Home Context Manager

At this flow, the home context manager has a special function. Through various sensors or gadgets, it collects the information required based on the patient's conditions. The patient's smart device or an application connected to nurses or specialists will then receive these details and health records. Additionally, there is a database where all health information is maintained. From there, significant recommendations or alerts that may be deduced from patient health records and information history are given to patients, their loved ones, and occasionally clinicians.

2. Hospital Environment

Medical professionals must gather crucial and helpful clinical data before starting patient monitoring and treatment in a smart home environment. In a hospital setting, all patient-related health data will be gathered. In the project we've suggested, we've created a patient health record form that should be completed by nurse or physician. The patient health record (PHR) table will have an exhaustive collection of data . The PHR is centrally located within the cloud architecture to deliver the health data required for detection alerts and therapies based on expert medical analysis.

3. Cloud Structure

Our proposed structure has benefited greatly from the usage of the cloud in terms of accessibility, flexibility, globalisation, cost reduction, and other factors. The fundamental objective of utilising cloud computing in our framework is to create a patient management system that can be accessed from anywhere at any time. As a cloud infrastructure, we have suggested a public cloud similar to the Google App-Engine. The security and privacy of data is another crucial concern with cloud architecture. In order to safeguard all data and establish secure connections between all components of this model, we must also use a tool that offers a high level of safety and security.

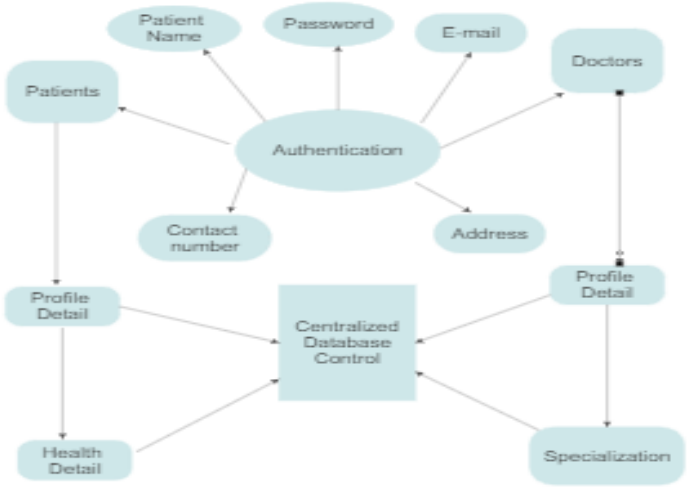

Figure 7: Proposed Model

VII. CONCLUSIONS

The proposed model makes the solution possible to decreases the disease in our country and also it would be easy to detect the ford which are taking place in the medical field easily and the patient health conditions are monitored, some suggestions can be given to the

patients to increase their health. For the goal of assessing and ranking cloud-based EHR solutions, a multi-criteria model is proposed to define trustworthiness. Even the best cloud-based EHRs might have their integrity compromised if users don't take the proper security measures (e.g., by not protecting system passwords and log-in identities, using insufficient physical protection of system computers and networking infrastructure, etc.). Unfortunately, from the perspective of the end user, convenience and security are inversely related. User education, training, and policies and procedures to enforce best practises are crucial in ensuring a dependable EHR system, despite the potential inconvenience. For their part, vendors must offer users monitoring, auditing, and reporting capabilities that enable on-going confirmation of the EHR's adherence to contractual obligations and user expectations. This openness creates a foundation for informed confidence and trust in the cloud-based EHR. Convenience is adversely correlated with security. Contrarily, increases in openness and communication between parties open up new sources of system vulnerability that need to be carefully addressed. Security can never be completely assured, even when there is a very high level of confidence between the parties. Risks that have been calculated should be carefully compared to exposures and liabilities that may exist. From this study, a variety of risk reduction, risk control, and risk transfer techniques can be created that are suitable for the provider's needs and environment. Choosing an effective and reliable EHR solution necessitates careful evaluation of numerous decision-making variables.

ACKNOWLEDGMENT

I want to acknowledge my supervisor **Er. Ashish Kumar Pandey** who helped me in all possible ways. First of all we want to thank almighty God for all the blessings .Now I want to thank all people who helped in completion of my project. I extend my sincere gratitude to my teachers and guide who made unforgettable contribution. I thank all the non-teaching staff of our institution that was always ready to help in whatever way they could.

REFERENCES

[1] **The American Recovery and Reinvestment Act of 2009 (ARRA), p. 115, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname= 111_cong_ bills & docid=f:h1enr.pdf.**

[2] **Centers for Medicare and Medicaid Services, "Medicare And Medicaid Health Information Technology: Title Iv Of The American Recovery and Reinvestment Act http://www.cms.hhs.gov/apps/media/press/factsheet.asp?Counter=3466.**

[3] **Piliouras, T., A Guided Tour of: SOAP ware Clinical Suite Electronic Health Records & Practice Management Software, Technical Consulting & Research, Inc., October 2011.**

[4] **Federal False Claims Act, 31 USC 3729-3733, text available at: http://www.taf.org/federalfca.htm.**

[5] **Goedert, J., "In Health Care, Privacy & Security Emphasis Will Only Increase," Health Data Management, October 6, 2011, http://www.healthdatamanagement.com/news/hipaa-privacy-securityrule-ahima 433541.html?ET=healthdatamanagement:e2033:156345a:&st=email&utm_sou rce=editorial&utm_medium=email&utm_campaign=HDM_Daily_1006 11. ICSA Labs, https://www.icsalabs.com/about-icsa-labs.**

[6] **Mohammad Momani and Subhash Challa, "Survey of Trust Models in Different Network Domains," International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 1, no. 3, pp. 1-19, September 2010.**

[7] **Tzu Yu Chuang, "Trust with Social Network Learning in E-Commerce," in IEEE International Conference on Communications Workshops (ICC), Capetown, South Africa, 2010, pp. 1-6.**

[8] **Firdhous, M., Ghazali, O., Hassan, S., "Trust and Trust Management in Cloud Computing – A Survey," InterNetWorks Research Group, Universiti Utara Malaysia, Technical Report No: UUM/CAS/InterNetWorks/TR2011-01, http://www.internetworks.my/pubs/techrep/TR2011-01.pdf.**

[9] **Qing Zhang, Ting Yu, and Keith Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management," in International Workshop on Trust, Security, and Reputation on the Semantic Web, Hiroshima, Japan, 2004**

[10] **Ko, Ryan K L; Jagadpramana, Peter; Mowbray, Miranda; Pearson, Siani; Kirchberg, Markus; Liang, Qianhui; Lee, Bu Sung, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," HP Laboratories Technical Report,http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.**

[11] **Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese, and Paul Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges, Final Report," TR-933-EC, 30 November 2010, Prepared for Unit F.5, Directorate-General Information Society and Media, European Commission.**

[12] **Cloud Security Alliance, "Top Threats to to Cloud Computing Report (Ver.1.0)," 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf**

[13] **"2010 Data Breach Investigations Report - A Study conducted by the Verizon RISK Team in Cooperation with the US Secret Service," http://www.verizonbusiness.com/resources/reports/rp_2010-data-breachreport_en_xg.pdf.**

[14] **"2011 Data Breach Investigations Report – A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit," http://www.verizonbusiness.com/resources/reports/rp_data-breachinvestigations-report-2011_en_xg.pdf**

[15] **Piliouras, T.; Pui Lam Yu; Housheng Huang; Xin Liu; Siddaramaiah, V.K.A.; Sultana, N.; "Selection of electronic health records software: Challenges, considerations, and recommendations," Systems, Applications and Technology Conference (LISAT), 2011 IEEE Long Island, Issue Date: 6-6 May 2011.**

[16] **Ryan K L Ko, Bu Sung Lee, Siani Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," HP Labs, http://ryanko.files.wordpress.com/2011/06/acctcloud-hpls_final.pdf.**

[17] **Rubinson, Teresa C., A Fuzzy Multiple Attribute Design and Decision Procedure for Long Term Network Planning, Ph.D. dissertation,**

Polytechnic University, June 1992.

[18] T Jayadeep and Soonar Mohammad Farooq "An E-Health Information System Using Cloud Computing" International Journal Research in computer science ISSN:2349-3828. 2 July 2018.

[19] Sepideh Poorejbari "Smart Healthcare System on improving the efficiency of healthcare Services 30-31Oct 2019 Dubai,UAE, DOI:10.1109/ICSPIS48135.2019.9045894.

[20] Teresa Piliouras; Pui Lam (Raymond) Yu; Yang Su; and Vijay Kumar Ajjampur Siddaramaiah" Trust in a Cloud-Based Healthcare Environment".

AUTHORS

First Author – Utkarsh Shukla, B.Tech Student, utkarsh3vns@gmail.com
Second Author – Jatin Kumar Chaurasia, B.Tech Student, jatinchaurasia97@gmail.com
Third Author- Urvi Verma , B.Tech Student, urviverma09071998@gmail.com

Correspondence Author – Ashish Kumar Pandey, ashishkumarpandey@rmlau.ac.in, 7317441066