ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

DSAS: A SECURE DATA SHARING AND AUTHORIZED SEARCHABLE FRAMEWORK FOR E-HEALTHCARE SYSTEM

Mrs.T.Venkata Lavanya [1], Narra Vishnu Vardhan (21S15A6710) [2], Kummari Shivanand (21S15A6709) [3], Adepu Nithin (21S15A6704) [4], Vamshi A Reddy (20S11A6746) [5],
ASSISTANT PROFESSOR [1], UG STUDENTS [2,3,4,5,]
DEPARTMENT OF CSE(DATA SCIENCE)
MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE,
Maisammaguda, Medchal (M), Hyderabad-500100, T. S

ABSTRACT

In e-healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, one of the important issues is that the encrypted PHRs prevent effective search of information, resulting in the decrease of data usage. Another issue is that medical treatment process requires the doctor to be online all the time, which may be unaffordable for all doctors (e.g., to be absent under certain circumstances). In this paper, we design a new secure and practical proxy searchable re-encryption scheme, allowing medical service providers to achieve remote PHRs monitoring and research safely and efficiently. Through our scheme DSAS, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of PHRs; (2) only authorized doctors or research institutions have access to the PHRs; (3) Alice (doctor-in-charge) is able to delegate medical research and utilization to Bob (doctor-in-agent) or certain research institution through the cloud server, supporting minimizing information exposure to the cloud server. We formalize the security definition and prove the security of our scheme. Finally, performance evaluation shows the efficiency of our scheme.

INTRODUCTION:

In today's rapidly evolving healthcare landscape, the effective management and secure sharing of patient data are paramount for delivering quality care and facilitating medical research. Traditional methods of data sharing in e-Healthcare systems often face significant challenges related to security, privacy, and accessibility. To address these challenges, the proposed project introduces DSAS: A Secure Data Sharing and Authorized Searchable Framework for eHealthcare Systems. The DSAS framework is designed to revolutionize the way healthcare data is shared, accessed, and managed, offering advanced features and technologies to enhance security, privacy, and search capabilities. By integrating state-of-the-art encryption techniques, fine-grained access control mechanisms, and searchable encryption algorithms, DSAS aims to provide a comprehensive solution for secure and efficient data sharing in the healthcare domain. This introduction outlines the context, problem statement, objectives, and scope of the DSAS project, highlighting its significance in addressing the critical needs of modern e-Healthcare systems. Through the implementation of DSAS, healthcare organizations can ensure compliance with privacy regulations, mitigate the risk of data breaches, and improve the overall quality of patient care.

LITERATURE SURVEY

AUTHORS: J. L ahteenm€ aki, J. Lepp anen, and H. Kaijanranta,

The establishment of the Meaningful Use criteria has created a critical need for robust interoperability of health records. A universal definition of a personal health record (PHR) has not been agreed upon. Standardized code sets have been built for specific entities, but integration between them has not been supported. The purpose of this research study was to explore the hindrance and promotion of interoperability standards in relationship to PHRs to describe interoperability progress in this area. The study was conducted following the basic principles of a systematic review, with 61 articles used in the study. Lagging interoperability has stemmed from slow adoption by patients, creation of disparate systems due to rapid development to meet requirements for the Meaningful Use stages, and rapid early development of PHRs prior to the mandate for integration among multiple systems. Findings of this study suggest that deadlines for implementation to capture Meaningful Use incentive payments are supporting the creation of PHR data silos, thereby hindering the goal of high-level interoperability.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Applying cloud computing model in PHR architecture.

AUTHORS: S. Kikuchi, S. Sachdeva, and S. Bhalla,

In recent years, some practical and commercial Personal Health Records and some related services such as Google Health [1] and Microsoft HealthVault [2] have been launched. On the other hand, Cloud Computing has matured more and become the major streams to realize a more effective operational environment. However so far, there have been few studies in regards to applying Cloud architecture in the PHR explicitly despite generating volume data. In this paper, we review our trial on the general architecture design by applying the Cloud components for supporting healthcare record areas and clarify the required conditions to realize it.

Health Information Privacy, Security, and Your EHR.

AUTHORS: M. Bellare

If your patients lack trust in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), feeling that the confidentiality and accuracy of their electronic health information is at risk, they may not want to disclose health information to you. Withholding their health information could have life-threatening consequences. To reap the promise of digital health information to achieve better health outcomes, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure. Your practice, not your EHR developer, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR system.

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

AUTHORS: C. Ng and P. Lee.

Revdedup Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. In this paper, we propose a secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group

ADVANCE SECURITY TO CLOUD DATA STORAGE

AUTHORS: P. Lee, and W. Lou

The proposed system is an effective and flexible distributed Scheme with explicit dynamic data support to ensure the correctness of user's data in the cloud. To fully ensure the data integrity and save the cloud users computation it is of critical importance to enable public auditing service for cloud data storage, so that users may depend on independent third party auditor to audit the outsourced data. The Third party auditor can periodically check the integrity of all the data stored in the cloud .which provides easier way for the users to ensure their storage correctness in the cloud

EXISTING SYSTEM:

Effective health information exchange needs to be standardized for interoperable healthϖ information exchange between hospitals. Especially, clinical document standardization lies at the core of guaranteeing interoperability. It

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

takes increasing amount of time for the medical personnel as the amount of exchanged CDA document increases because more documents means that data are distributed in different documents. This significantly delays the medical personnel in making decisions. Hence, when all of the CDA documents are integrated into a single document, the medical personnel is empowered to review the patient's clinical history conveniently in chronological order per clinical section and the follow-up care service can be delivered more effectively. Unfortunately for now, a solution that integrates multiple CDA documents into one does not exist yet to the best of our knowledge and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology.

DISADVANTAGES OF EXISTING SYSTEM:

The HIS development platforms for hospitals vary so greatly that generation of CDA documents in each hospital invariably requires a separate CDA generation system. Also, hospitals are very reluctant to adopt a new system unless it is absolutely necessary for provision of care. As a result, the adoption rate of EHR is very low except for in a few handful countries. Unfortunately for now, a solution that integrates multiple CDA documents into one does not exist yet to the best of our knowledge and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology. To establish confidence in HIE interoperability, more HIS's need to support CDA. However, the structure of CDA is very complex and the production of correct CDA document is hard to achieve without deep understanding of the CDA standard and sufficient experience with it.

PROPOSED SYSTEM:

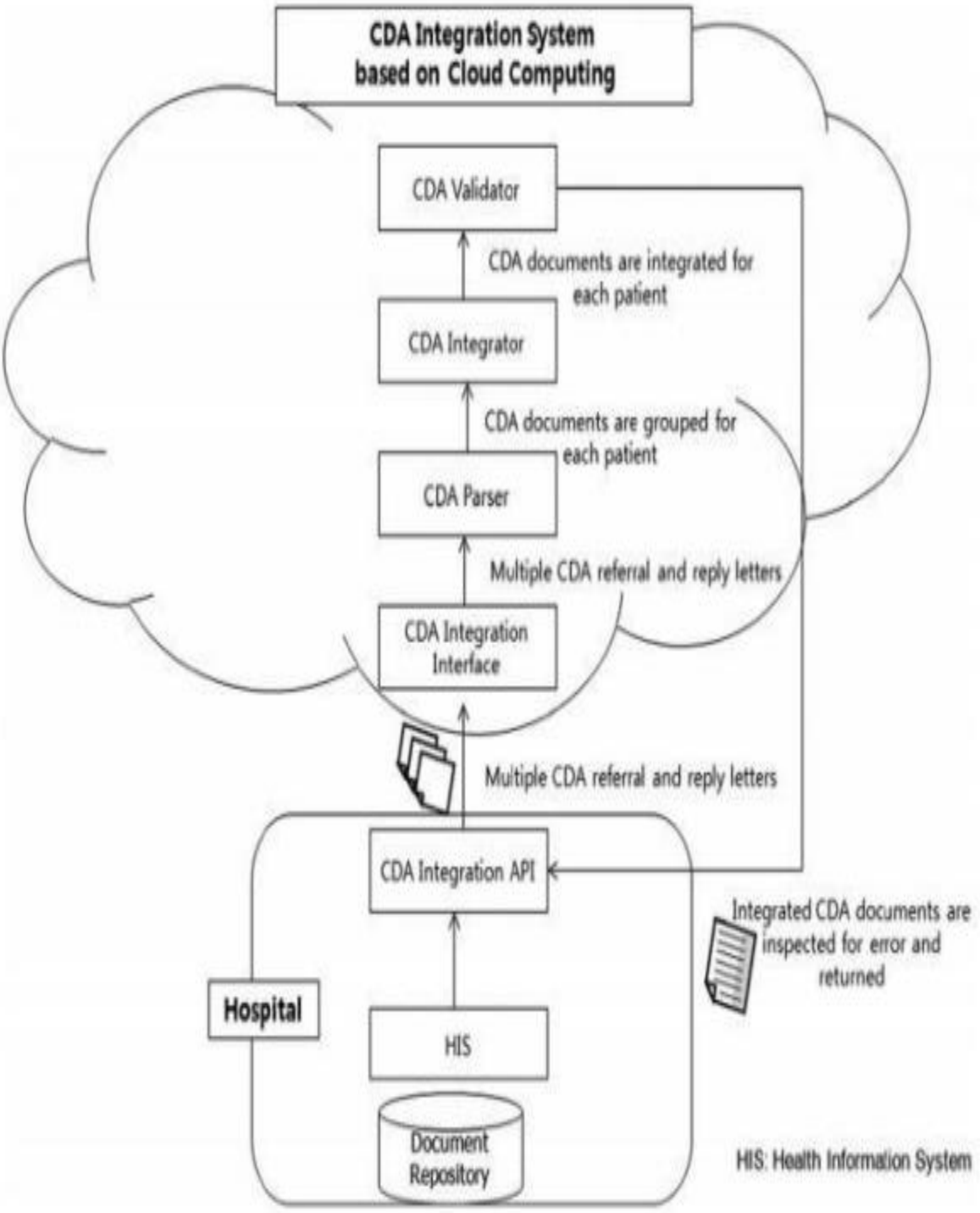
In this paper we present (1) a CDA document generation system that generates CDA documents on different developing platforms and (2) a CDA document integration system that integrates multiple CDA documents scattered in different hospitals for each patient. CDA Generation API generates CDA documents on cloud. CDA Generation Interface uses the API provided by the cloud and relays the input data and receives CDA documents generated in the cloud.Template Manager is responsible for managing the CDA documents generated in the cloud server. Our system uses CCD document templates. CDA Generator collects patient data from hospitals and generates CDA documents in the template formats as suggested by the Template Manager. CDA Validator inspects whether the generated CDA document complies with the CDA schema standard.

ADVANTAGES OF PROPOSED SYSTEM:

Hospital systems can simply extend their existing system rather than completely replacing it with a new system. Second, it becomes unnecessary for hospitals to train their personnel to generate, integrate, and view standard-compliant CDA documents. The cloud CDA generation service produces documents in the CDA format approved by the National Institute of Standards and Technology (NIST). If this service is provided for free at low price to hospitals, existing EHR are more likely to consider adoption of CDA in their practices. Interoperability between hospitals not only helps improve patient safety and quality of care but also reduce time and resources spent on data format conversion.

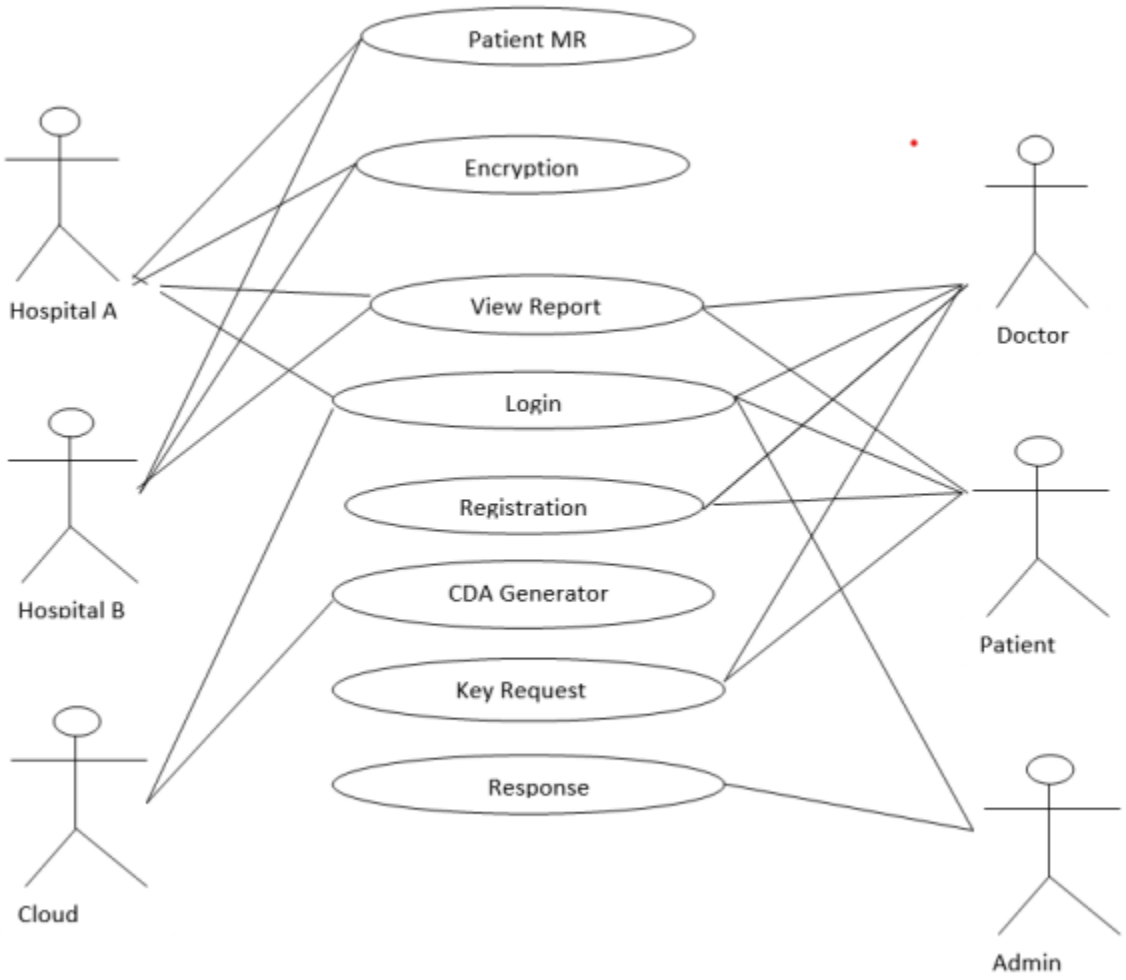
SYSTEM DESIGN

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024



ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Data Flow Diagram:



Hardware Requirements:

- Processor: i3 and above
- RAM: 4 GB
- Space on Hard Disk: 20 GB

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Software Requirements:

- Eclipse IDE
- JDK 1.8
- SQL YOG
- MYSQL
- TOMCAT

Operating Systems Supported:

- Windows 7
- Windows 10
- Windows 11

Technologies and Languages used to Develop:

- JAVA
- J2EE (JSP, Servlet)
- CSS
- HTML
- JAVA SCRIPT
- MySQL

Debugger and Emulator:

- Eclipse

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

INPUT AND OUTPUT DESIGN

Input Design:

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

Select methods for presenting information.

Create document, report, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

RESULTS

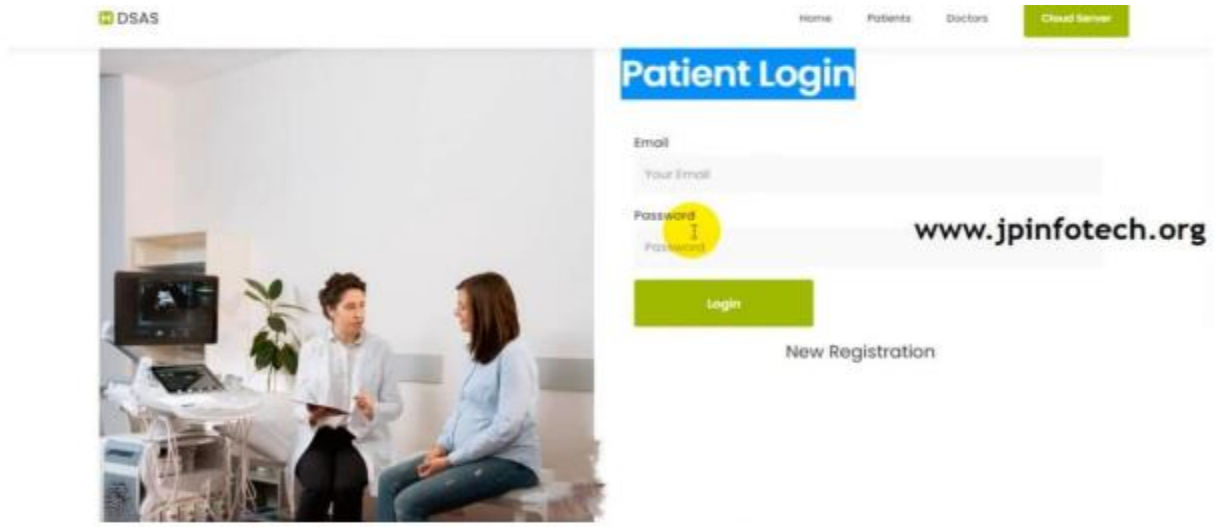


Fig-1: Patient Login Page

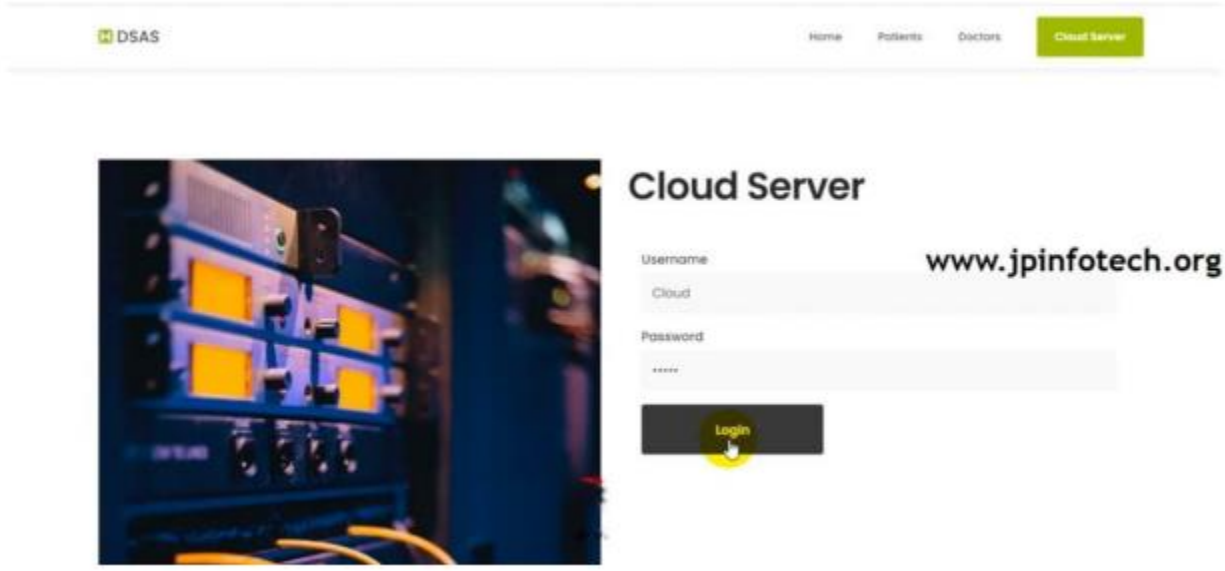


Fig-2:Cloud Login Page

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Fig 3: Patients Activation Page

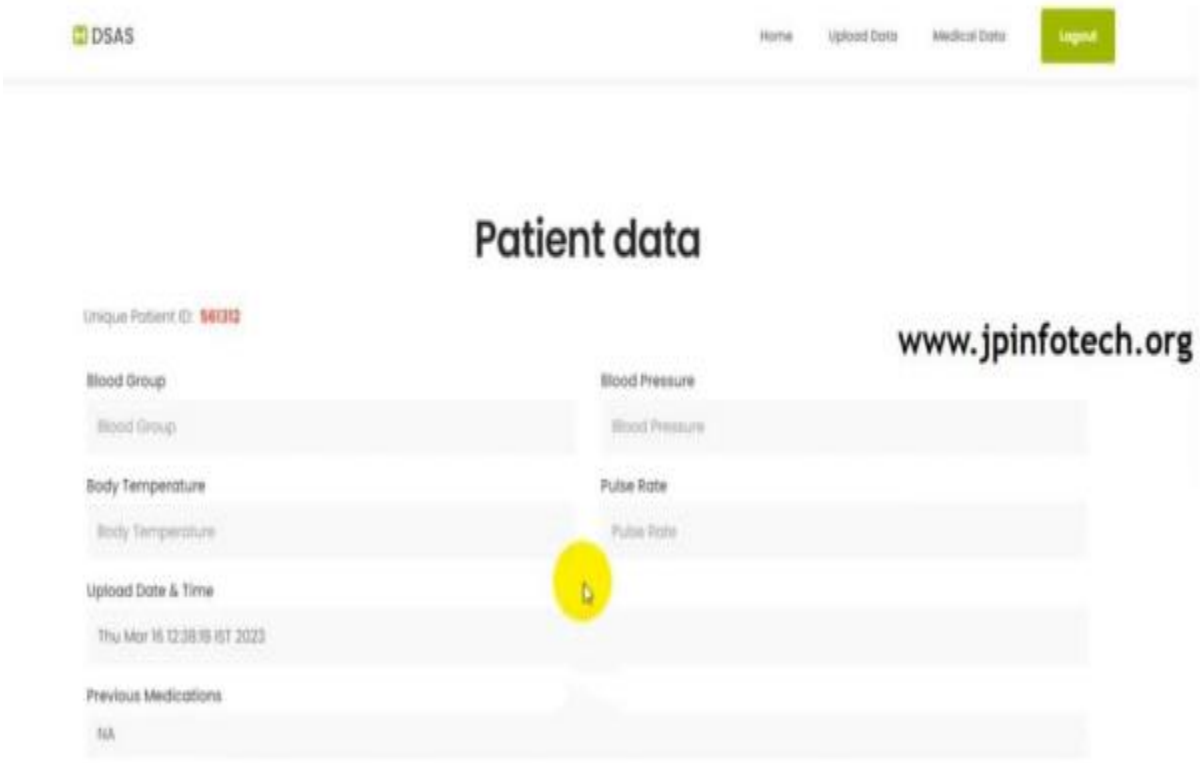


Fig-4: Patient Data Page

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

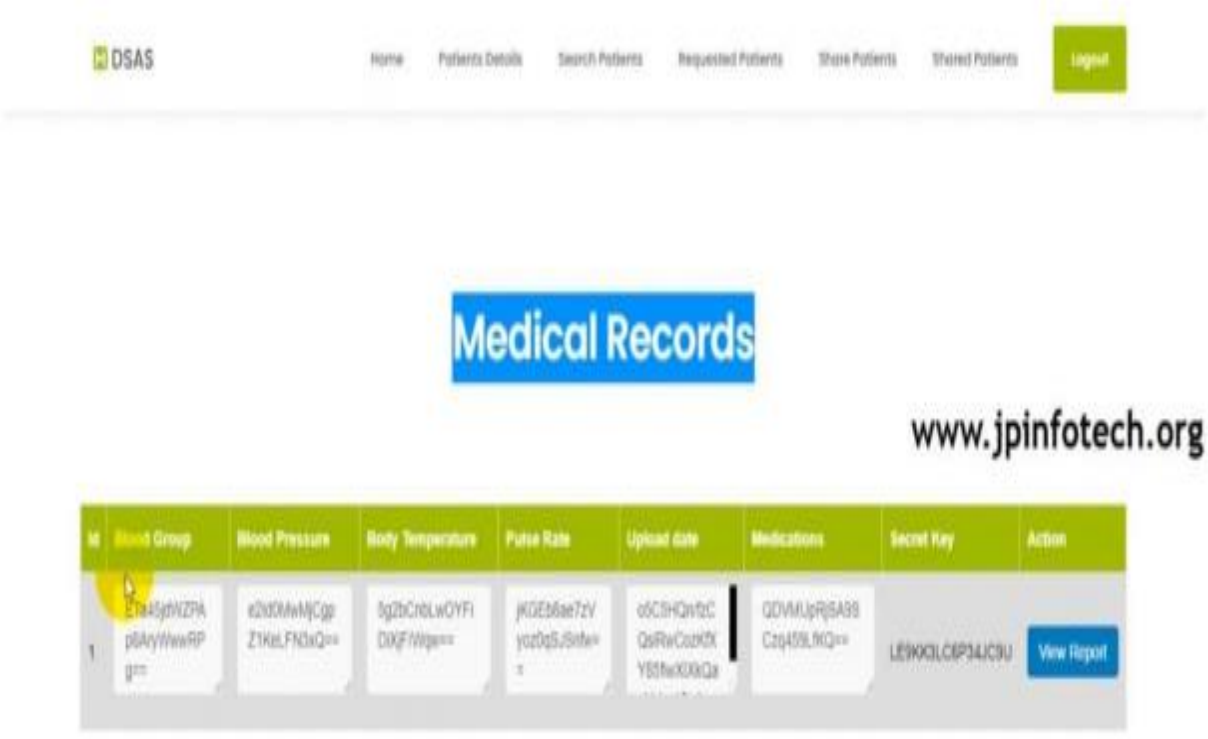


Fig-5: Medical Records Page

Fig-6: Doctors Login Page

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Fig-7: Doctor Activation Page

CONCLUSION& FUTURE ENHANCEMENT

Conclusion:

In conclusion, DSAS presents a robust solution for addressing the security and privacy concerns inherent in e-healthcare systems. By incorporating advanced encryption techniques and access control mechanisms, DSAS ensures that sensitive patient data remains secure throughout its lifecycle. Furthermore, its innovative searchable framework enables authorized users to efficiently retrieve relevant information while maintaining strict confidentiality. The implementation of DSAS not only enhances data security but also facilitates seamless collaboration and information exchange among healthcare providers, ultimately leading to improved patient care outcomes. As the digital landscape of healthcare continues to evolve, DSAS stands as a pivotal tool in safeguarding patient privacy and advancing the efficiency and effectiveness of e-healthcare systems.

Future Enhancement:

In the ever-evolving landscape of e-healthcare systems, future enhancements could focus on developing secure data sharing and authorized searchable frameworks (DSAS) to address privacy concerns and ensure efficient access to medical information. Such a framework would integrate advanced encryption techniques to safeguard sensitive patient data while enabling authorized healthcare providers to securely share and access relevant information as needed. Additionally, implementing robust authentication protocols would ensure that only authorized individuals can perform searches within the system, maintaining confidentiality and integrity. By prioritizing security and accessibility, DSAS could revolutionize the e-healthcare domain, fostering seamless collaboration among healthcare professionals while safeguarding patient privacy.

BIBLIOGRAPHY

1. Y. Kwak, “International standards for building electronic health record (ehr),” in Proc. Enterprise Netw. Comput. Healthcare Ind., pp. 18–23, Jun. 2005.
2. M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, and Laleci, “A survey and analysis of electronic healthcare record standards,” ACM Comput. Surv., vol. 37, no. 4, pp. 277–315, 2005.
3. T. Benson, Principles of Health Interoperability HL7 and SNOMED. New York, NY, USA: Spinger, 2009.
4. J. L€ ahteenm€ aki, J. Lepp€ anen, and H. Kaijanranta, “Interoperability of personal health records,” in Proc. IEEE 31st Annu. Int. Conf. Eng. Med. Biol. Soc., pp. 1726–1729, 2009.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

5. R. H. Dolin, L. Alschuler, C. Beebe, P. V. Biron, S. L. Boyer, D. Essin, E. Kimber, T. Lincoln, and J. E. Mattison, "The HL7 Clinical Document Architecture," J. Am. Med. Inform. Assoc., vol. 8, pp. 552–569, 2001.
6. R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F. M. Behlen, P. V. Biron, and A. Shabo, "The HL7 Clinical Document Architecture," J. Am. Med. Inform. Assoc., vol. 13, no. 1, pp. 30–39, 2006.
7. M. L. Muller, F. € Ũckert, and T. Burkle, "Cross-institutional data € exchange using the clinical document architecture (CDA)," Int. J. Med. Inform., vol. 74, pp. 245–256, 2005.
8. H. Yong, G. Jinqiu, and Y. Ohta, "A prototype model using clinical document architecture (cda) with a japanese local standard: designing and implementing a referral letter system," Acta Med Okayama, vol. 62, pp. 15–20, 2008.
9. K. Huang, S. Hsieh, Y. Chang, F. Lai, S. Hsieh, and H. Lee, "Application of portable cda for secure clinical-document exchange," J. Med. Syst., vol. 34, no. 4, pp. 531–539, 2010.
10. C. Mart ınez-Costa, M. Men arguez-Tortosa, and J. Tom as Fern andez-Breis, "An approach for the semantic interoperability of ISO EN 13606 and OpenEHR archetypes," J. Biomed.Inform., vol. 43, no. 5, pp. 736–746, Oct. 2010.
11. MR. Santos, MP. Bax, and D. Kalra, "Building a logical HER architecture based on ISO 13606 standard and semantic web technologies," Studies Health Technol. Informat., vol. 160, pp. 161– 165, 2010.
12. K. Ashish, D. Doolan, D. Grandt, T. Scott, and D. W. Bates, "The use of health information technology in seven nations,"Int. J. Med. Informat., vol. 77, no. 12, pp. 848–854, 2008.
13. G. J. Kuperman, J. S. Blair, R. A. Franck, S. Devaraj, and A. F. Low, "Developing data content specifications for the nationwide health information network trial implementations," J. Am. Med. Inform. Assoc., vol. 17, no. 1, pp. 6– 12, 2010.
14. K. Ashish, "Meaningful use of electronic health records the road ahead,"JAMA, vol. 304, no. 10, pp. 1709–1710, 2010.
15. S. M. Huff, R. A. Rocha, C. J. McDonald , G. J. De Moor, T. Fiers, W. D. Bidgood, A. W. Forrey, W. G. Francis, W. R. Tracy, D. Leavelle, F. Stalling, B. Griffin, P. Maloney, D. Leland, L. Charles, K. Hutchins, and J. Baenziger, "Development of the logical observation identifier names and codes (loinc) vocabulary," J. Am. Med. Inform. Assoc., vol. 5, pp. 276–292, 1998.
16. J. D. D'Amore, D. F. Sittig, A. Wright, M. S. Iyengar, and R. B. Ness, "The promise of the CCD: Challenges and opportunity for quality improvement and population health," in Proc. AMIA Annu. Symp. Proc., pp. 285–294, 2011.
17. KS X 7504 Korean Standard for CDA Referral Letters (Preliminary Version)
18. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.
19. S. Yi, A. Andrzejak, and D. Kondo, "Monetary cost-aware check pointing and migration on amazon cloud spot instances," IEEE Trans. Services Comput., vol. 5, no. 4, pp. 512–524, Nov. 2012.
20. S. Lee, J. Song, and I. Kim, "Clinical document architecture integration system to support patient referral and reply letters," Health Informat. J., Published online before print Jun. 2014.
21. "Test Data for x170.314(e)(2) Clinical summary—ambulatory setting only approved test data version 1.5," The Office Nat. Coordinator Health Informat. Technol., 2014 Edition, Jun. 2013.
22. J. Walker, E. Pan, D. Johnston, J. Adler-Milstein, D. W. Bates, and B. Middleton, "The value of health care information exchange and interoperability," in Proc. Health Aff., pp. 10–18, 2005.
23. S. R. Simon, R. Kaushal, P. D. Cleary , C. A. Jenter, L. A. Volk, E. G. Poon, E. J. Orav, H. G. Lo, D. H. Williams, and D. W. Bates, "Correlates of electronic health record adoption in office practices: A statewide survey," J. Am. Med. Inform. Assoc., vol. 14, pp. 110–117, 2007.
24. E. W. Ford, N. Menachemi, L. T. Peterson, and T. R. Huerta, "Resistance is futile: But it is slowing the pace of ehr adoption nonetheless," J. Am. Med. Inform. Assoc., vol. 16, no. 3, pp. 274–281, 2009.
25. "Healthcare SaaS vs. licensed software," Healthcare Technol. Online, Sept. 2009.
26. A. Dogac, G. B. Laleci, and T. Aden "Enhancing IHE XDS for federated clinical affinity domain support," IEEE Trans. Inf. Technol. Biomed., vol. 11, no. 2, pp. 213–221, Mar. 2007.
27. K. U. Heitmann, R. Schweiger, and J. Dudeck, "Discharge and referral data exchange using global standards—the SCIPHOX project in Germany," Int. J. Med. Inform., vol. 70, pp. 195– 203, 2003.
28. M. L. Muller, F. Uckert, T. Burkle, and H. U. Prokosch, "Crossinstitutional data exchange using the clinical document architecture (CDA)," Int. J. Med. Inform., vol. 74, pp. 245–256, 2005.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

29. P. ittorini, A. Tarquinio, and F. Orio, “XML technologies for the Omaha System: A data model, a Java tool and several case studies supporting home healthcare,” Comput. Methods Programs Biomed, vol. 93, pp. 297–312, 2009.
30. E. W. Huang, T. L. Tseng, M. L. Chang, M. L. Pan, and D. M. Liou, “Generating standardized clinical documents for medical information exchanges,” in Proc. IT Pro., pp. 26– 32, 2010.
31. W. S. Jian, C. Y. Hsu, T. H. Hao, H. C. Wen, M. Hsu, Y. L. Lee, Y. C. Li, and P. Chang, “Building a portable data and information interoperability infrastructure—framework for a standard Taiwan electronic medical record template,” Comput. Methods Programs Biomed., vol. 88, pp. 102–111, 2007.
32. B. Blazona and M. Koncar, “HL7 and DICOM based integration of radiology departments with healthcare enterprise information systems,” Int. J. Med. Inform., vol. 76, no. 3, pp. 425– 432, 2007.
33. J. Kim, S. Jeon, C. Lim, S. Park, and N. Kim, “Implementation of reporting system for continuity of care document based on web service,” in Proc. Inform. Control Symp., pp. 402– 404, May 2009.
34. P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, “Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption,” J. Am. Med. Inform. Assoc., vol. 13, no. 2, pp. 121–126, 2006.
35. S. Kikuchi, S. Sachdeva, and S. Bhalla, “Applying cloud computing model in PHR architecture,” in Proc. Joint Int. Conf. HumanCentered Comput. Environments, pp. 236–237, 2012.
36. P. V. Gorp and M. Comuzzi, “MyPHRMachines: Lifelong personal health records in the cloud,” in Proc. 25th Int. Symp. Comput.-Based Med. Syst., pp. 1–6, Jun. 2012.
37. P. V. Gorp, M. Comuzzi, A. Fialho, and U. Kaymak, “Addressing health information privacy with a novel cloud-based PHR system architecture,” in Proc. IEEE Int. Conf. Syst., Man, Cybern., pp. 1841– 1846, Oct. 2012.
38. “HL7 Implementation Guide for CDA Release 2: Personal healthcare monitoring report, DSTU release 1.1,” Health Level Seven, Jan. 2013.
39. PatientGeneratedDocumentInformativeDocument.(2013)[Online].Available:http://wiki.hl7.org/index.php?title¼ Patient_Generated_Document_Informative_Document
40. R.Colomo-Palacios, V. Stantchev, and A. Rodr ıguez-Gonz alez, “Special issue on exploiting semantic technologies with particularization on linked data over grid and cloud architectures,” Future Generation Comput. Syst., vol. 32, pp. 260–262, Mar. 2014.
41. V. Stantchev, T. Schulz, T. Dang, I. Ratchinski, “Optimizing Clinical Processes with Position Sensing,” IT Professional, vol. 10, no. 2, pp. 31–37, Feb/Mar. 2008.
42. A. Rosenthal, P. Mork, M. Li, J. Stanford, D. Koester, and P. Reynolds, “Cloud computing: A new business paradigm for biomedical information sharing,” J. Biomed. Informat., vol. 43, no. 2, pp. 342–353, 2010.
43. H. A. J. Narayanan and M. H. Giine, “Ensuring access control in cloud provisioned healthcare systems,” in Proc. IEEE Consumer Commun. Netw. Conf., pp. 247–251, Jan. 2011.
44. (2013). NIST CDA guideline validation. [Online]. Available: http://cdavalidation.nist.gov/cda-validation/validation.html