Tracking of Prenatal and Postnatal for Fetus Condition System

Rekha.C[1], Deepa.B[2], Jegatha.R[3]

[1,2,3]Assistant Professor
Sri Sai Ram Institute of Technology

***Abstract*: The broad acknowledgment of cloud based administrations in the medicinal services area has brought about financially savvy and helpful trade of Personal Health Records (PHRs) among a few taking an interest elements of the e-Health frameworks. By the by, putting away the secret wellbeing data to cloud servers is helpless to disclosure or robbery and requires the improvement of philosophies that guarantee the protection of the PHRs. Along these lines, we propose a system called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR plot guarantees understanding driven control on the PHRs and jam the secrecy of the PHRs. The patients store the scrambled PHRs on the un-confided in cloud servers and specifically concede access to various sorts of clients on various bits of the PHRs. A semi-confided in intermediary called Setup and Re-encryption Server (SRS) is acquainted with set up people in general/private key combines and to create the re-encryption keys. Besides, the technique is secure against insider dangers and furthermore implements a forward and in reverse access control. Besides, we formally dissect and confirm the working of SeSPHR philosophy through the High Level Petri Nets (HLPN). Execution assessment with respect to time utilization shows that the SeSPHR approach can possibly be utilized for safely sharing the PHRs in the cloud.**

***Keywords*: Cloud computing, PHR, SRS,SeS, PHR**

INTRODUCTION:

Advancements in medicine, quality of education and technological growth have been massive over the past few years. Starting from smart phones to 3D technologies and robotic surgery to Nano medicine, the world has grown to a whole new level. Sadly, these advancements are not easily accessible by all. Remote or underdeveloped regions of the world are still suffering without the aid of advanced medicine and technology. India, being a diverse nation has its population widely spread into two areas, rural and urban. Urban areas are developed and have access to all the latest developments. The inadequate development of rural areas has had even less impact on key issues such as unemployment and health issues.

The broad acknowledgment of cloud based administrations in the medicinal services area has brought about financially savvy and helpful trade of Personal Health Records (PHRs) among a few taking an interest elements of the e-Health frameworks. By the by, putting away the secret wellbeing data to cloud servers is helpless to disclosure or robbery and requires the improvement of philosophies that guarantee the protection of the PHRs. Along these lines, we propose a system called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR plot guarantees understanding driven control on the PHRs and jam the secrecy of the PHRs. The patients store the scrambled PHRs on the un-confided in cloud servers and specifically concede access to various sorts of clients on various bits of the PHRs. A semi-confided in intermediary called Setup and Re-encryption Server (SRS) is acquainted with set up people in general/private key combines and to create the re-encryption keys. Besides, the technique is secure against insider dangers and furthermore implements a forward and in reverse access control. Besides, we formally dissect and confirm the working of SeSPHR philosophy through the High Level Petri Nets (HLPN). Execution assessment with respect to time utilization shows that the SeSPHR approach can possibly be utilized for safely sharing the PHRs in the cloud.

EXISTING SYSTEM:

The cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service provider. Therefore, the integration of aforementioned entities results in the evolution of a cost effective and collaborative health ecosystem where the patients can easily create and manage their Personal Health Records (PHRs). Generally, the PHRs contain information, such as demographic information, patients' medical history including the diagnosis, allergies, past surgeries, and treatments, laboratory reports, data about health insurance claims, and private notes of the patients about certain important observed health conditions.

DISADVANTAGE:

1.Storing the private health information to cloud servers managed by third-parties is susceptible to unauthorized access.
2.In particular, privacy of the PHRs stored in public clouds that are managed by commercial service providers is extremely at risk.
3.The privacy of the PHRs can be at risk in several ways, for example theft, loss, and leakage.

Literature:

Existing systems for patients data storage are not scalable enough for the increasing number of patients and applications. Cloud computing promises low cost, high scalability, availability and disaster recoverability which can be a natural solution for some of the problems faced in storing and analysing patients' medical records. This paper examines the impact of cloud computing on improving healthcare services. More specifically, this research details the architectural design for a personal health record system called ‖MedCloud‖ that utilizes and integrates services from Hadoop's ecosystem in conjunction with HIPAA privacy and security rules. A scalable platform is proposed for developers to use in application development and Restlet, a web portal, is presented to users, to access the MedCloud system. Later on, the development of the MedCloud model is illustrated through issues analysis followed by an in- depth performance evaluation. Healthcare is always a major concern for the community. ―Towards smarter IT‖ is the main slogan for a successful healthcare institution. There is a great need for new strategies to reduce healthcare costs and improve the quality of service. Moreover, IT has positively affected the healthcare sector, it provides more accurate and timely information regarding patient SURVEY

Author Name: Jun Zhou ; Xiaodong Lin ; Xiaolei Dong ; Zhenfu CaoDistributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Finally, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.

AuthorName:Majdi Rawashdeh ; MuhammadAl-Qurishi ; Mabrook_Al-Rakhami_; Maged S Al-Quraishi significant issue over the world. Obesity has various negative consequences that might impact not only the health but also the social and the economic issues. Current studies reveal the lack of patients' commitment to the doctors' instructions. In this paper, we propose a new cloud-based model with ultimate aim to monitor obese patients' health condition and behavior constantly under a real-time vision of the caregiver. The proposed model provides a technical method to record, disseminates, and share knowledge and awareness among patients and caregivers. This model utilizes wireless body sensor network devices to measure heart rate; mobile web-service as a middle ware to process the data from/to cloud knowledge- base and a caregiver backend/dashboard for the real-time monitor. A live test demo of the model experimented on 55 subjects to check its applicability and cost-effectiveness. The results were promised and prove its ability to help overcoming this disease.Obesity phenomenon has become a significant over the world. Obesity has various negative consequences that might impact not only the health but also the social and the economic issues. Various medical studies were conducted to prevent this chronic disease. Researchers revealed the main causes of the disease. Recent studies show the lack of patients' commitment to the doctors' instructions. However, there is no single research, which monitored the patient's eating, and drinking attitude and behavior by using computer technology. Therefore, the ultimate aim of this research is to provide supportive software to monitor patients' health condition and behavior. This should encourage further technological research and motivate developers to invent new solutions, which might assist to get rid of this illness.

Author Name: Majdi Rawashdeh ; MuhammadAl-Qurishi ; Mabrook_Al-Rakhami_; Maged S Al-Quraishi Obesity phenomenon has become a significant issue over the world. Obesity has various negative consequences that might impact not only the health but also the social and the economic issues. Current studies reveal the lack of patients' commitment to the doctors' instructions. In this paper, we propose a new cloud-based model with ultimate aim to monitor obese patients' health condition and behavior constantly under a real-time vision of the caregiver. The proposed model provides a technical method to record, disseminates, and share knowledge and awareness among patients and caregivers. This model utilizes wireless body sensor network devices to measure heart rate; mobile web-service as a middle ware to process the data from/to cloud knowledge- base and a caregiver backend/dashboard for the real-time monitor. A live test demo of the model experimented on 55 subjects to check its applicability and cost-effectiveness. The results were promised and prove its ability to help overcoming this disease.Obesity phenomenon has become a significant over the world. Obesity has various negative consequences that might impact not only the health but also the social and the economic issues. Various medical studies were conducted to prevent this chronic disease. Researchers revealed the main causes of the disease. Recent studies show the lack of patients' commitment to the doctors' instructions. However, there is no single research, which monitored the patient's eating, and drinking attitude and behavior by using computer technology. Therefore, the ultimate aim of this research is to provide supportive software to monitor patients' health condition and behavior. This should encourage further technological research and motivate developers to invent new solutions, which might assist to get rid of this illness.

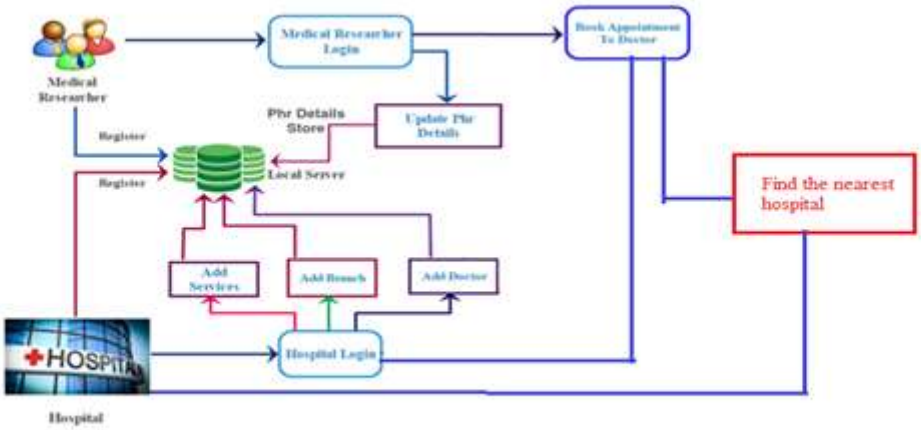
Author Name: Adam Pawlak ; Krzysztof Horoba ; Janusz Jezewski ; Janusz Wrobel ; Adam Matonia
While maternal, infant and under-five child mortality rates in developing countries have declined significantly in the past two to three decades, newborn mortality rates have reduced much more slowly. While it is recognized that almost half of the newborn deaths can be prevented by scaling up evidence-based available interventions such as tetanus toxoid immunization to mothers; clean

and skilled care at delivery; newborn resuscitation; exclusive breastfeeding; clean umbilical cord care; management of infections in newborns, many require facility based and outreach services. It has also been stated that a significant proportion of these mortalities and morbidities could also be potentially addressed by developing community-based packages interventions which should also be supplemented by developing and strengthening linkages with the local health systems. Some of the recent community-based studies of interventions targeting women of reproductive age have shown variable impacts on maternal outcomes and hence it is uncertain if these strategies have consistent benefit across the continuum of maternal and newborn care.

Author Name:Shella Arrum Wardhani ; Richard Karel Willem Mengko ; Agung Wahyu Setiawan
Multiple-micronutrient (MMN) deficiencies often coexist among women of reproductive age in low-to middle-income countries. They are exacerbated in pregnancy due to the increased demands, leading to potentially adverse effects on the mother and developing fetus. Though supplementation with MMNs has been recommended earlier because of the evidence of impact on pregnancy outcomes, a consensus is yet to be reached regarding the replacement of iron and folic acid supplementation with MMNs

PROPOSED S YSTEM:

We propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High Level Petri Nets (HLPN). Performance evaluation regarding time consumption indicates that the SeSPHR methodology has potential to be employed for securely sharing the PHRs in the cloud.



INPUT DESIGN:
The major inputs for Web Based Accommodation can be categorized module-wise. Basically all the information is managed by the software and in order to access the information one has to produce one's identity by entering the user-id and password. Every user has their own domain of access beyond which the access is dynamically refrained rather denied.

ADVANTAGE:
1.We present a methodology called SeSPHRthat permits patients to administer the sharing of their own PHRs in the cloud.
2.The SeSPHR methodology employs the El-Gamal encryption and proxy re-encryption to ensure the PHR confidentiality.
3.The forward and backward access control is also implemented in the proposed methodology.
4.Formal analysis and verification of the proposed methodology is performed to validate its working according to the specifications.

OUTPUT DESIGN:

The major outputs of the system are tables and reports. Tables are created dynamically to meet the requirements on demand. Reports, as it is obvious, carry the gist of the whole information that flows across the institution. This application must be able to produce output at different modules for different inputs.

CONCLUSION:
The government has proposed many plans for the welfare and development of rural areas. Yet, the reduction of mortality rate has not been efficient. Thus a need for a better system prevails. Our system would meet the requirements as it monitors the health of

the mother and child in all angles and would be able to address the criticality of any situation. Our system also helps easy access by urban doctors through cloud computing to provide better knowledge and conclusion on the patient's condition. This intensive tracking at both prenatal and postnatal conditions will contribute to the decrease in child mortality rate in rural areas

REFERENCES:

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era*, *Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.
[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.
[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms forwireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.
[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.
[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Modelfor Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, pp. 1290–1302, 2002.
[6] S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptiveclustering hierarchy protocol for wireless sensor networks," *Comput.Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.
[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput.Applications*, vol. 47, no. 11, pp. 23–28, 2012.
[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.
[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc.IEEE NCA*, 2007, pp. 145–152.
[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,"
[11] M. Blanton, M. M. J. Atallah, K. B. K. Frikken, and Q. Malluhi, "Secure and Efficient Outsourcing of Sequence Comparisons," Comput. Secur. 2012, pp. 505–522, 2012.
[12] M. Franklin, M. Gondree, and P. Mohassel, "Communication-efficient private protocols for longest common subsequence," in Topics in Cryptology--CT-RSA 2009, Springer, 2009, pp. 265– 278.
[13] M. Gondree and P. Mohassel, "Longest common subsequence as private search," in Proceedings of the 8th ACM workshop on Privacy in the electronic society, 2009, pp. 81–90.
[14] D. Szajda, M. Pohl, J. Owen, B. Lawson, and V. Richmond, "Toward a practical data privacy scheme for a distributed implementation of the SmithWaterman genome sequence comparison algorithm," in Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS 06), 2006.
[15] M. Blanton and M. Aliasgari, "Secure outsourcing of DNA searching via finite automata," in Data and Applications Security and Privacy XXIV, Springer, 2010, pp. 49–64.
[16] J. R. Troncoso-Pastoriza, S. Katzenbeisser, and M. Celik, "Privacy preserving error resilient dna searching through oblivious automata," in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 519–528.
[17] K. B. Frikken, "Practical private DNA string searching and matching through efficient oblivious automata evaluation," in Data and Applications Security XXIII, Springer, 2009, pp. 81–94.