International Journal of Advanced Engineering Application
ISSN:3048-6807, Volume No.1 Issue No 3, July 2024

# Design a mobile health system that is both efficient and easily shareable, incorporating division and replication features to improve security

[1]Kumara Swami, [2]Mohan Babu
[1,2]Student, Computer Engineering. SITAM-AP, India.

**Abstract— Wireless wearable sensor devices combined with cloud computing have significantly advanced patient care in modern healthcare. These technologies provide more comprehensive features than traditional healthcare services, enabling more efficient monitoring, data sharing, diagnosis, and remote patient engagement. However, the integration of wearable devices into healthcare introduces several security challenges, including concerns around data privacy and security. The adoption of mobile health (mHealth) systems, which are increasingly patient-driven, has seen substantial growth. Wearable sensors are used to collect real-time patient data, which is then aggregated and encrypted on end-user devices. Healthcare professionals such as doctors, nurses, and researchers store and access this encrypted data in the cloud. One of the primary challenges is the efficient sharing of scalable encrypted data. This paper proposes a Lightweight Sharable and Traceable (LiST) secure mobile health system, where patient data is encrypted end-to-end. The LiST system provides precise keyword searches and secure access control to encrypted data, with support for traitor tracing and user revocation. This system also addresses the issue of traitors who may sell their search keys or steal permissions. The majority of cryptographic computations are handled by the cloud, while end-user devices perform minimal tasks. The LiST system is proven to be secure without relying on a random oracle, and extensive experimentation has shown improvements in system performance. The global expansion of health information technology is evident, with even developing nations adopting smart devices for healthcare. The widespread use of smartphones has driven the demand for mobile applications in healthcare, and both patients and healthcare providers are increasingly comfortable using mobile devices for accessing patient records and diagnosis.**

**Keywords:- Mobile Health, Sharable & Traceable, LiST, Device, Cloud Computing, mHealth, EHR**.

## 1.INTRODUCTION

The integration of wearable sensor devices with cloud computing has transformed modern healthcare, making it more adaptable to the needs of today's patients. Compared to traditional healthcare services, new technologies such as mHealth offer patients more treatment options and advanced care. These technologies enhance the flexibility of monitoring patient records, sharing data, providing diagnoses, and remotely interacting with patients through the cloud. However, the inclusion of wearable devices in healthcare services introduces significant security concerns, particularly regarding the privacy and protection of healthcare data.

The rise of a patient-centered approach has facilitated the development of mobile health systems. These systems enable the aggregation of patient data at end-user devices, securing it while also allowing real-time data collection using wearable sensors. Encrypted data is then distributed and stored in the cloud, where it can be accessed by healthcare professionals, including doctors, nurses, and researchers. However, the efficient sharing of scalable encrypted data remains a significant challenge.

In this project, we propose the development of a secure, portable, scalable, and auditable mobile health system (LiST). The LiST system encrypts patient data end-to-end, providing an efficient mechanism for keyword searches and secure access control for encrypted data. Additionally, the system supports traitor tracing and user revocation, addressing the issue of traitors who might profit from selling search keys or access permissions to colleagues. The bulk of cryptographic computations, which are computationally intensive, is offloaded to the cloud, while end-user devices handle only basic operations. The security of the LiST system is formally established, demonstrating that it is secure even without the use of a random oracle. Extensive testing has been conducted to ensure the system meets performance requirements.

While health information technology is a relatively new field, its applications are expanding rapidly worldwide. Until recently, only countries with decentralized healthcare systems utilized intelligent devices in healthcare. However, developing nations are also making strides in adopting this technology. The increasing availability of mobile networks has led to a growing interest in using mobile phones and the ever-expanding range of applications available on them. This trend has driven the demand for mobile applications in healthcare. Both healthcare providers and patients are becoming more comfortable with the use of mobile devices for diagnostic procedures and managing patient records.

On a global scale, the use of information technology in healthcare is increasing daily. In the past, primarily developed countries utilized computers and associated technologies in healthcare. However, today, even less developed countries are making progress in this area. The widespread coverage of mobile networks in many countries has sparked interest in using mobile phones. Additionally, the number of smartphone users has surged in recent years, leading to a heightened demand for mobile applications. Most desktop applications are now available on mobile devices, enabling end users to access them on their smartphones.

**Mobile Health (mHealth)**

Mobile health technology leverages smartphones, tablets, and other mobile devices to deliver public health and preventive services. This technology enables healthcare practitioners to access electronic health records (EHRs), collaborate with care teams, communicate with patients through portals, monitor patients in real-time, improve disease diagnosis, and track disease progression. Cloud-based telemedicine is another application of this technology, allowing patients to manage their medical information, access their EHRs, and communicate with their doctors. This system facilitates data sharing between patients and healthcare providers when necessary, saving time for both parties. Advances in medical technology over recent decades have made healthcare simpler and more efficient. Both healthcare providers and patients are increasingly comfortable using mobile devices to access medical records and diagnose illnesses, a shift driven largely by technological advancements.

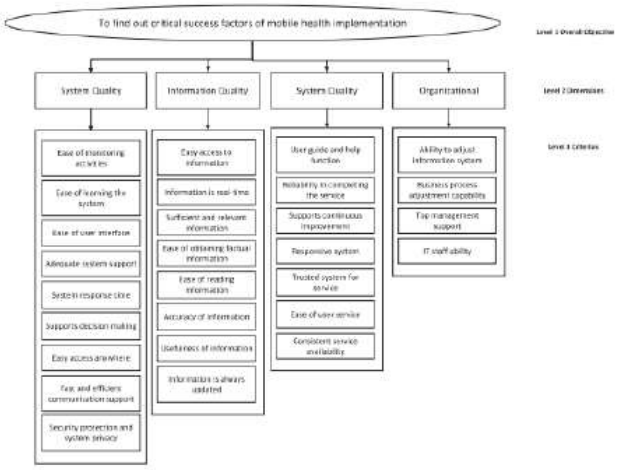


Figure1.1: Critical success factors of m-health implementation

**Distributed Cloud**

A distributed cloud system enhances multitasking by allowing multiple clients to access a single file system simultaneously. Files are fragmented into smaller parts and stored across various machines, which streamlines communication and boosts performance. In the context of digital medical records, this system divides files into smaller chunks before uploading them to the cloud, prioritizing privacy, integrity, and anonymity. This approach accelerates data processing and reduces the time required for operations.

**Health Concerns**

The evolution of e-health has been significantly driven by advancements in cloud computing, mobile technology, satellite systems, and connectivity. E-health enhances healthcare by analyzing large volumes of data, transitioning from traditional paper-based records to Electronic Health Records (EHRs), Electronic Medical Records (EMRs), and Personal Health Records (PHRs). EMRs are used by healthcare providers, while PHRs are maintained by patients to track metrics like blood pressure, glucose levels, and heart rate. The global implementation of EHRs aims to improve the utility of shared medical records and computerized databases. However, issues concerning health data security and privacy have limited their widespread adoption. Data breaches and misuse of sensitive information are serious concerns, with reports such as the Privacy Rights Clearinghouse (2005) noting significant healthcare privacy breaches. To safeguard against these risks, robust security measures are necessary to prevent data loss, manipulation, and unauthorized access. E-health systems need to address these privacy concerns to ensure the safe use of electronic health records.

**Related Work**

Healthcare security encompasses various aspects, including authentication, privacy, data integrity, and tracking. This paper focuses on remote user authentication for healthcare systems, where patients, doctors, and other healthcare providers authenticate to access data via mobile or terminal devices. Traditional user authentication methods, often relying solely on passwords, have proven inadequate. Recent approaches incorporate multi-factor authentication, combining passwords, mobile numbers, and biometric data for enhanced security. These systems typically involve mobile devices, a management server, storage, and a cluster host. The management server stores hashed passwords and biometric data (such as facial and voice recognition) and uses this information to authenticate users against stored credentials. While some systems have improved authentication through encryption and biometric data protection, challenges remain, such as the lack of mutual authentication between user and management servers, and the requirement for high-quality cameras for accurate biometric authentication. Recent proposals include multi-server tele-care systems using smart cards and elliptic curve cryptography to secure patient-doctor communications, addressing issues like password guessing and replay attacks. These systems enhance security with forward secrecy and refined elliptic curve techniques.

**Proposed System**

The proposed system involves embedding a node within the patient's body, which collects signals from wireless sensors and transmits them to a base station. This creates a Wireless Body Sensor Network (WBSN) capable of monitoring vital signs such as heart rate and blood pressure. The system detects abnormalities, triggering alarms and notifying the attending physician via email or text message. Additionally, wireless relay nodes are integrated to forward data from the coordinating node to the base station, enhancing energy efficiency and extending network lifespan. The system improves communication coverage and patient freedom, thereby enhancing the quality of life. It is compared with contemporary multi-hop relay node networks in terms of coverage, energy consumption, and speed, demonstrating superior performance. As mobile health care advances, new security protocols are explored, including those for physiological sensors and channel randomization for physical layer security. Future research should include comprehensive ECG data and assess new protocol security

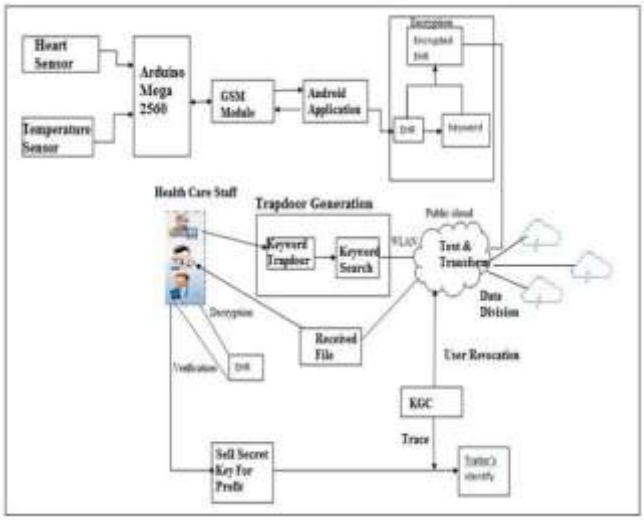


**Figure1.2: Proposed System enhancements.**

**Here's a concise summary of the literature survey you provided:**

Julian Jang-Jaccard et al., 2021

Topic: Security in mobile collaboration tools for rural healthcare.

Summary: The study critiques the ReColl tool's limited security features and the overall lax security in mobile health collaboration tools. It highlights the risks of privacy breaches due to inadequate logging and auditing. Recommendations include improved security practices and system-level security analysis.

### Kalvinder Singh, 2013

- **Topic:** Security in mobile health care systems.

- **Summary:** The thesis discusses the challenges of securing mobile health systems using symmetric key approaches and proposes new protocols for key establishment based on physiological signals. It emphasizes the need for secure and tested protocols to protect health data and validate system security.

### Ebru Celikel Cankaya et al., 2015

- **Topic:** Design and development of Electronic Health Records (EHR) systems.

- **Summary:** This study provides a blueprint for designing EHR systems using software engineering and database development techniques. It emphasizes a formalized approach to design and the inclusion of user-interactive tools in EHR development.

### Sanaz Rahimi Moosavi et al., 2015

- **Topic:** IoT-based healthcare authentication and authorization.

- **Summary:** The study proposes a distributed key management system for IoT-based healthcare that reduces communication overhead and delays. It demonstrates improved security over traditional centralized methods, addressing issues like DoS attacks.

### Fatma Zubaydi et al., 2015

- **Topic:** Security and privacy in mHealth apps.

- **Summary:** This study examines security threats and privacy issues in mHealth apps. It calls for better standards in app development, stronger privacy policies, and more robust security practices to protect sensitive health data.

### Dr. Ajit Singh, 2017

- **Topic:** Cloud computing in healthcare.

- **Summary:** The study explores cloud computing security issues for healthcare, including data security, access control, and malware risks. It emphasizes the need for effective security measures to protect cloud-stored health data and reduce vulnerabilities.

### Brinda Hansraj Sampat & Bala Prabhakar, 2017

- **Topic:** Privacy and security in mHealth apps.

- **Summary:** This research evaluates mHealth apps for privacy and security, identifying issues with privacy policies and app safety. It advocates for stricter app development standards and consumer vigilance to ensure data protection.

### Clemens Scott Kruse et al., 2017

- **Topic:** Security approaches for Electronic Health Records (EHRs).

- **Summary:** The article reviews security measures for EHRs, including administrative, physical, and technical safeguards. It outlines the importance of protecting sensitive health information against various cyber threats.

### M. Kiah et al., 2018

- **Topic:** Security in Android mHealth apps.

- **Summary:** The study proposes the MASF framework to enhance security for Android-based mHealth apps. It includes features like fine-grained access control and data shadowing to protect user privacy with minimal performance overhead.

### Luci Pirmez et al., 2018

- **Topic:** Resource allocation in cloud-based sensor networks.

- **Summary:** Zeus is presented as a resource allocation mechanism for cloud-based sensor networks. It uses a hybrid edge computing approach to optimize resource use and manage delay-sensitive applications efficiently.

### Long Beach et al., 2018

- **Topic:** Security vulnerabilities in mobile health apps.

- **Summary:** The study found significant security weaknesses in mHealth apps, including poor SSL configurations and lack of HIPAA compliance. It recommends improvements in TLS server security, encryption, and compliance with HIPAA standards.

This survey provides a comprehensive view of various security challenges and solutions in mobile and cloud-based health systems, emphasizing the need for robust security measures and standards in these evolving technologies.

**Nureni Ayofe Azeez, Charles Van der Vyver, Egyptian Informatics Journal, ELSEVIER, 2018**

This research analyzed security and privacy in e-Health literature. Some pros and weaknesses of approaches were listed. The literature review discovered over 110 solution models. We compared model publications. Similar models by researchers helped minimize reviewed publications. Define e-Health. Categorizing cloud-based models; HIPAA privacy and security regulations were discussed. Future e-Health security and cloud computing privacy directions were considered. Authors offer secure electronic health architecture to assure efficiency, reliability, and regulated health information access. This design will protect doctors' and patients' privacy.

**Summary**

To improve healthcare, every country must deploy e-Health. Implement security and privacy measures to prevent breaches and vulnerabilities to maximize e-benefits. We analyzed e-Health security and privacy literature and discovered shortcomings. We must use the concepts given to construct an excellent e-Health solution. All countries should establish an e-Health document structure to facilitate uptake. Governments can construct research centers to develop safe e-Health solutions. E-Health services and practices should have specified privacy limits so patients can submit health information safely.

**Karim Abouel mehdi, Abderrahim Beni-Hessane and Hayat Khaloufi, Elsevier, 2018**

Big data changed how companies handle, analyze, and use data. Big data in healthcare is promising. Big healthcare data can improve patient outcomes, predict epidemic outbreaks, get insights, avoid preventable diseases, and minimize healthcare expenditures. Choosing allowed data usage while maintaining patient privacy is hard. Big data can only help medical science and healthcare by addressing security and privacy challenges. Evaluate present solutions' boundaries and upcoming research topics to safeguard massive data. In this paper, we explored big data security and privacy difficulties in healthcare, assessed how they emerge, and offered solutions. We analyzed anonymization and encryption methods and envisioned future study.

**Xiao Chun Yin, Zeng Guang Liu, Bruce Ndibanje, Lewis Nkenyereye, and S. M. Riazul Islam, SensorS, 2019**

Internet-connected devices change healthcare communication. IoT could increase healthcare quality, safety, efficiency, and economic, social, and technical prospects. This link causes credential-stealing malware data breaches. Connected devices can leak patient data. Due to IoT entities and IoT-based healthcare, computer security is crucial today.

In this study, a wireless communication system is used to anonymize IoT health data. The algorithm defines non-dis-closable records to protect internet users' privacy. The proposal encrypts health data securely. Math verified the algorithm's anonymity function. Results suggest anonymization protects the healthcare IoT systems.

**Summary**

Studies offer answers for IoT-based healthcare. Patients, doctors, nurses, and health organizations share data via the network. To avoid difficulties, protect the data owner. This research provided a technique to safeguard IoT data. The suggested algorithm secures user data. When a user uploads his information over a health network, the encrypted data set is anonymize using a key from the key pair. By computing the requirements and anonymizing healthcare data, we showed that our approach provided anonymity. We demonstrated algorithm complexity. The provided technique can secure IoT for wireless health care networks, according to math. Future healthcare will involve sensors. Comparing experiment results to techniques.

**Jordán Pascual Espada, Ronald Yager, Zhiyong Yu, Future Generation Computer Systems, elsevier, 2019**

Many IoT systems use sensors and electronics. This issue focuses on improving device communication and collaboration. Some proposals improve wireless network hardware. Others increase IoT communication and allocation. DNS may be improved for numerous communication contexts. Researchers improved linked device services. IoT devices must interoperate. Some authors suggest frameworks for heterogeneous device communication. Adding more IoT devices could broaden its industrial use. This edition offers fresh perspectives. Privacy and security in communications is another key topic. IoT sensor data and connected devices pose security and privacy challenges.

**Summary**

Recent improvements in embedded device communications, collaborations, and services increase the prospect of establishing new IoT systems and upgrading existing ones. Researchers have presented techniques to improve IoT device communication and collaboration. Many projects improved wireless communications, especially Wi-Fi. Improved communication and allocation; some proposals could improve multi-device network communication

services like DNS. Some authors suggested improving LBS. New software suggestions and frameworks for heterogeneous device communication were given. Some authors incorporate drones into IoT. Privacy and security in communications are also important. IoT device communication and collaboration will increase daily, but not because of one idea or technology. Communication technologies take years to spread. Some suggestions can improve IoT without changing technology.

**Bingqing Shen, Jingzhi Guo and Yilong Yang. Applied sciences, 2019**

IoT monitors health. Laboratories use data. Methods can't change metadata. This study recommends using MedChain to share healthcare data. Blockchain, digest chain, P2P; MedChain allows session-based data sharing. MedChain improves data efficiency and security.

**Summary**

HIE improves patient diagnoses, R&D, and wellness. HIE reduces costs, improves quality, arranges treatment, and monitors disease. MedChain helps patients control their health data. Dual-network design, session-based data sharing, and digest chain structure protect data. Blockchain enhances healthcare efficiency. Improving healthcare data-sharing benefits everyone. Doctors oppose platform changes. Previous project combined inter-organizational data exchange with antiquated systems. Decentralized MedChain scales. Clinicians and researchers use device data. MedChain helps everyone. MedChain isn't perfect. Data first; data sharing slows patient diagnosis. Share hospital data. Physicians keep records. Mobility requires tech and legislation. Manual data access is slow. Emergency care is hindered. Automating data exchange so a doctor's smartphone can start a session is planned. Regulate. MedChain's blockchain directory requires inefficient data streams from providers. Data-collecting mobile and fog devices upload to super-peers. Evaluate it.

**Shivaji M. Sarvade, Sachin M. Pore. Research gate, 2019**

In India, most buildings are reinforced concrete; hence Civil Engineering students study design. Computer programs are needed to investigate and develop structural layouts. Commercial reinforced concrete design methods are expensive and have restricted licensing. Softwares have design assumptions. Most design firms use MS-Excel or other computer programs to create structures. These expensive programs aren't flexible. Python is an easy-to-use programming language. Non-programmers can use Python. This tool teaches concrete structure design. Python allows designers build interactive apps. Executing Python programs; the article discusses Python-based education apps. Python programming in design courses boosts analytical skills and industrial readiness.

**Summary**

Python can teach RCC design. Programming improves debugging skills and analytical thinking. The design industry requires customized, cost-effective structural design; therefore this enhances their career possibilities. Python students can construct structural design applications. Free open-source programming language for PCs with minimum hardware

**A. divya preetha, T.S. Pradeep kumar, International Conference On Recent Trends in Advanced Computing ICRTAC, Science Direct, 2019**

Outsourced PHR exchanges patient health information. Unconstitutional servers could receive medical records, compromising privacy. Medical records can be encrypted. Fine-grained access control is hindered by privacy, scalability, and expert revocation. This book helps honest-but-curious servers manage patient-centric data. Fine-grained, scalable Novel Cipher-text access control. Random-length CP-ABE is used offline. 256-bit AES encrypts CP-ABE data transferred to the cloud over a secure connection (AES-256). Revocation removes leaking keys. Forward and backward secrecy, user revocation, random key length, and collusion attack resistance secure data. MHS-MLPT-computation

**Summary**

Access controls and policy adjustments are needed for record-sharing systems. This paper proposes a multi-layered, traceable mobile health system with data-sharing features. MLPPT-MHS considers device moves frivolous due to restricted resources. Access control and user revocation should be instant. Oracle-free MLPPT-MHS is secure. A subjective study says MLPPT-MHS is superior. MLPPT-app MHS is PC and mobile-friendly.

**Ayman M. Bahaa-Eldin, Mohamed Sobh. The 6th International Workshop on Privacy and Security in HealthCare (PSCare 2019), Science Direct, Elsevier, 2019.**

Expanded to cut costs and improve care. EHR security and privacy must be ensured. We offer a comprehensive hybrid-security protocol to promote privacy and reduce communication costs. It's a secure multifactor remote user protocol that lets patients securely transmit medical

information with doctors via unsecure channels. Three-factor authentication protects user identities (i.e. password, smart device, bio-metrics) Biometrics can't be faked, stolen, or forgotten. Automated formal tool simulates proposed protocol. Biometrics can't be faked, stolen, or forgotten. AVISPA simulates the proposed protocol.

**Summary**

This research presents a multifactor authentication strategy that increases patient security and privacy and reduces communication costs. Using AVISPA, we automated the protocol's formal verification.

1. Summary and Implementation of the Proposed Healthcare App

Objective: Develop a healthcare app that ensures secure, trustworthy communication between patients and doctors, leveraging cloud storage and advanced encryption methods.

Key Technologies and Methodologies:

2. Cloud Storage and Encryption:
    - Ciphertext Policy Attribute-Based Encryption (CP-ABE): Utilized for flexible, granular access control to encrypted health records (EHRs) stored in the cloud.
    - Central Authority (CA) and Attribute Authorities (AAs): A CA is selected from AAs to manage user verification and generate secret keys. AAs handle attribute management separately.
3. System Components:
    - Body Sensor Network (WBSN):
        - Role: Measures vital signs (e.g., heart rate, blood pressure) from patients.
        - Data Transmission: Sends health data to a mobile device via Bluetooth or WLAN.
        - Encryption: Health records are encrypted into ciphertext based on an access policy.
    - Healthcare Workers (Data Users):
        - Role: Access and search encrypted EHRs based on affiliation and type.
        - Trapdoor Generation: Mobile terminals create keyword trapdoors to query encrypted data.
4. Encryption and Decryption Process:
    - Encryption:
        - Cloud-Based: Most ABE encryption calculations are performed by the public cloud.
        - Mobile Device: Only a few operations are needed on the device.
    - Decryption:
        - Cloud-Based: The cloud performs most decryption operations, returning intermediate ciphertext.
        - Mobile Device: Only one exponentiation computation is needed to retrieve and verify EHR data.
5. Revocation and Security:
    - Revocation: A lightweight mechanism ensures quick user revocation without large-scale key updates or ciphertext re-encryption.
    - Traitor Tracking: LiST architecture enables effective tracing of users with exposed keys using minimal operations.

Benefits:

- Efficiency: The app streamlines data collection, storage, and evaluation, reducing reliance on traditional paperwork and improving productivity.
- Security: Extensive testing ensures the app is secure, allowing users to confidently share sensitive information.
- Timely Treatment: Enhanced data handling leads to quicker diagnosis and better patient care.

**Conclusion:** The proposed healthcare app enhances flexibility, effectiveness, and security in managing health data. By integrating advanced encryption techniques and efficient data management practices, the app aims to provide a safe and reliable platform for communication between patients and healthcare providers, ultimately improving patient safety and care.

**References:**

1. Security Analysis of Mobile Applications: A Case Study of a Collaboration Tool in Healthcare, Julian Jang-Jaccard, Jane Li, Surya Nepal, Leila Alem, CSIRO Computational Informatics (CCI)2020
2. Security for Mobile Health Care Systems, Kalvinder Singh, Griffith University, 2013
3. A Secure Healthcare System: From Design to Implementation Ebru Celikel Cankaya, Than Kywe, The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015), Science Direct, Elsevier, 2015
4. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen, 6th International Conference on Ambient Systems, Networks and Technologies (ANT 2015) Science Direct, Elsevier, 2015
5. Security of Mobile Health (mHealth) Systems, Fatma Zubaydi, Ayat Saleh, Fadi Aloul, Assim Sagahyroon Department of Computer Science & Engineering American University of Sharjah, UAE, November 2015
6. A Survey on Security Challenges of Healthcare Analysis Over Cloud, Dr. Ajit Singh Associate Professor, BTKIT, Dwarahat. International Journal of Engineering Research & Technology (IJERT), 04, April-2017
7. Privacy Risks and Security Threats in mHealth apps, Brinda Hansraj Sampat, Bala Prabhakar, Journal of International Technology and Information Management 2017
8. Security Techniques for the Electronic Health Records, Clemens Scott Kruse & Brenna Smith & Hannah Vanderlinden & Alexandra Nealand Education & Training, 2017
9. A security framework for mHealth apps on Android platform, Muzammil Hussain, Ahmed Al-Haiqi, A.A. Zaidan, B.B. Zaidan, M. Kiah, Salman Iqbal, S. Iqbal, Mohamed Abdulnabi. Science Direct, Elsevier, 2018
10. Zeus: a resource allocation algorithm for the cloud of sensors, Igor L. Santos (corresponding author), Luci Pirmez, Flavia C. Delicato, Gabriel M. Oliveira, Claudio M. Farias, Samee U. Khan, Albert Y. Zomaya, Accepted Manuscript, 2018
11. Security Vulnerabilities in Mobile Health Applications, I, the Undersigned Member of the Committee, Have Approved this thesis, California State University, Long Beach Spring 2018
12. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis Nureni Ayofe Azeez, Charles Van der Vyver, Egyptian Informatics Journal, ELSEVIER, 2018
13. Big healthcare data: preserving security and privacy, Karim Abouel mehdi, Abderrahim Beni-Hessane and Hayat Khaloufi, Elsevier, 2018
14. An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks Xiao Chun Yin, Zeng Guang Liu, Bruce Ndibanje, Lewis Nkenyereye, and S. M. Riazul Islam, SensorS,2019
15. Communications, collaborations and services in networks of embedded devices, Jordán Pascual Espada, Ronald Yager, Zhiyong Yu, Future Generation Computer Systems, Elsevier, 2019
16. Med Chain: Efficient Healthcare Data Sharing via Blockchain, Bingqing Shen, Jingzhi Guo and Yilong Yang. Applied sciences, 2019
17. Use of python programming for interactive design of reinforced concrete structures Shivaji M. Sarvade, Sachin M. Pore. Research gate, 2019
18. Mobile Health system, A. divya preetha, T.S. Pradeep kumar, International Conference On Recent Trends In Advanced Computing ICRTAC, Science Direct, 2019.
19. Robust Hybrid-Security Protocol for HealthCare Systems, Ibrahim Albarki, Mohamed Rasslan, Ayman M. Bahaa-Eldin, Mohamed Sobh. The 6th International Workshop on Privacy and Security in HealthCare (PSCare 2019), Science Direct, ELSEVIRE, 2019.