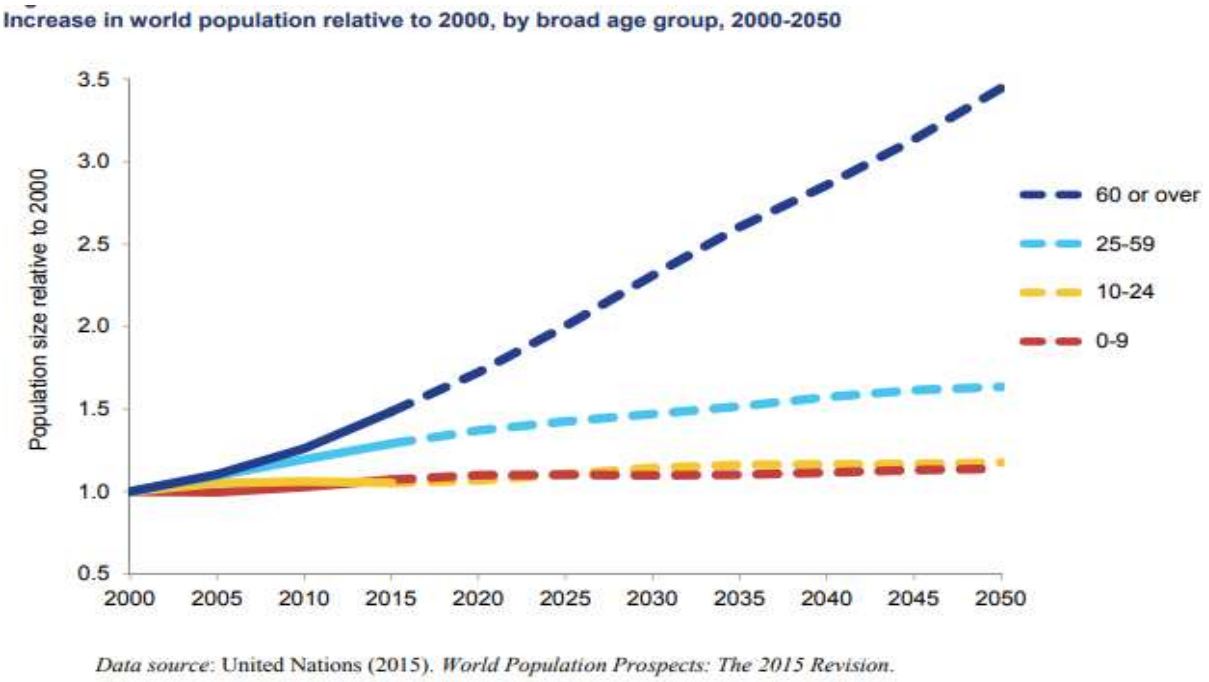
SMART AND SECURE HEALTH CARE SYSTEM FOR ELDERLY AND DISABLED

Dr. V. Srinivasa Naresh
Principal Investigator(PI)
Associate Professor, CSE
Sri Vasavi Engineering College
Tadepalligudem
Andhra Pradesh

Dr. Rama Rao P.V.V.
Co- Investigator(CI)
Professor, EEE
Sri Vasavi Engineering College
Tadepalligudem
Andhra Pradesh

Project Significance

Increased life expectancy results in a large aging population in the next two decades coupled with Inability of Elderly and disabled people to Afford Medication emphasizes the need for **smart, secure , reliable and cost effective health care systems.**



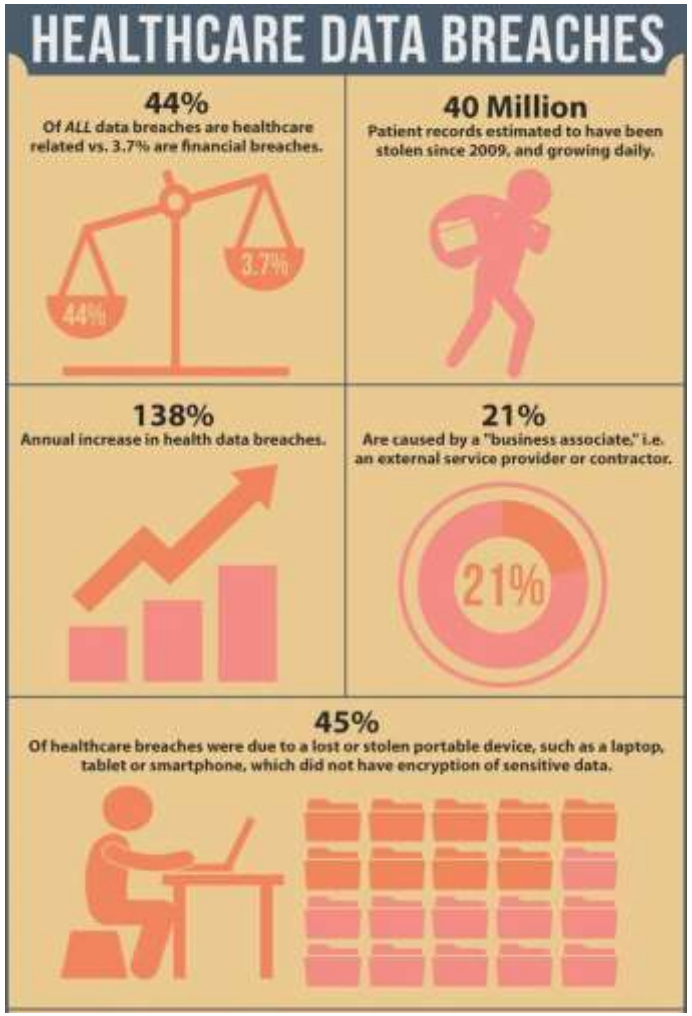
Data source: United Nations (2015). *World Population Prospects: The 2015 Revision.*

Project Significance

✓Increase in Healthcare data breaches with the existing centralized systems emphasize a **blockchain integrated decentralized secure and smart health care system** while ensuring reliability, privacy, security and trust.

✓Ensuring trust in medical community, iscientist and in pharmaceutical is essential to improve the quality of healthcare.

✓With blockchain we can save Massive loss of time, money and eventually life.



How the project is unique from Existing Solutions

Existing Solution	Proposed Solution
We need to trust intermediary [third party] to store our health records	Third parties can be eliminated by establishing a distributed ledger which has built in trust mechanism [blockchain]
Cost per transaction is very high as lot of intermediaries are involved.	Reduces transaction costs due to disintermediation, as well as near-real time processing.
No standard method for Patient identity	Uses Private and public keys identifiers which creates a singular, more secure method of protecting patient identity
No health data interoperability between systems	Shared data enables real-time updates across the network to all parties
Limited Access to health data	Distributed, secure access to patient health data across the distributed ledger
Inconsistent rules and permissions	Smart contracts creates a rule-based method for accessing patient data that can be permissioned to selected organizations

Objectives

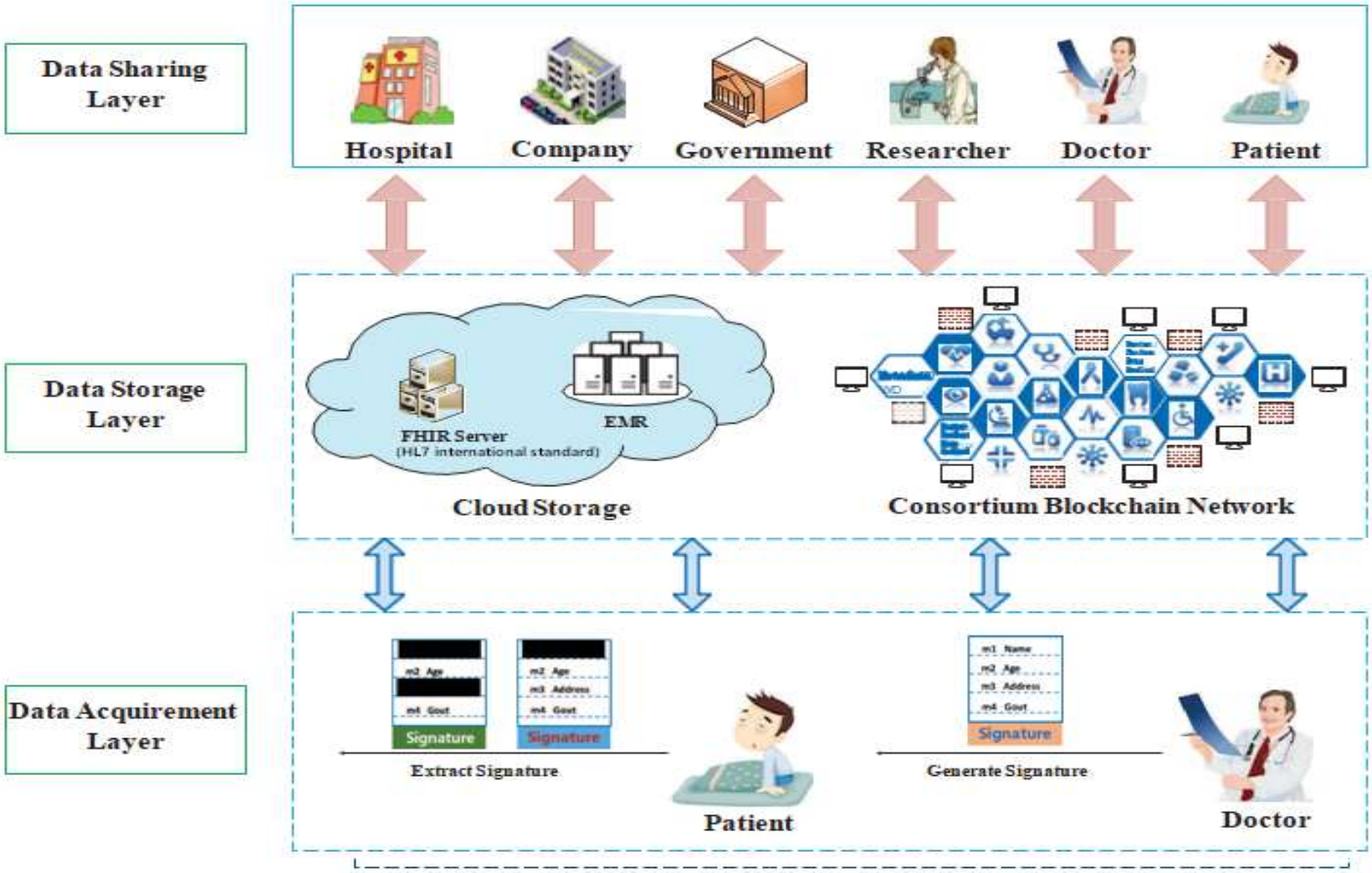
- ✓ To build a **BLOCKCHAIN INTEGRATED SMART AND SECURE HEALTH CARE SYSTEM** while ensuring system **reliability, security and privacy**, **Interoperability** of the data.
- ✓ To provide **enhanced security** for storage and Privacy-Preserving DataSharing using **Blockchain** .
- ✓ To collaborate with doctors from hospitals engaged in studying and validating the results on their patients for taking preventive measure for any abnormalities.

METHODOLOGY

Sensor Data Includes:

1. Pulse
2. Oxygen in blood (SPO2)
3. Airflow (breathing)
4. Body temperature
5. Electrocardiogram (ECG)
6. Glucometer
7. Galvanic skin response (GSR - sweating)
8. Blood pressure (sphygmomanometer)
9. Patient position (accelerometer)
10. Muscle/electromyography sensor (EMG)

BLOCKCHAIN BASED PRIVACY-PRESERVING DATA SHARING(BDPS) FOR Electronic Medical Records(EMR)



BDPS System Architecture

The function of each layer is described as follows.

Data Acquirement Layer

In this layer, EMRs are created by data providers such as doctors. Doctors sign patients' EMRs using their private key and send them to the patients. Patients are the owners of EMRs and can completely control them. In order to avoid privacy information is leaked in the process of data sharing, patients can remove sensitive information of EMRs and generate valid extraction signatures.

Data Storage Layer

The function of this layer is to store the original EMRs and its indexes. Components of data storage layer include:

Fast Healthcare Interoperability Resources (FHIR): The standard was created and is managed by the Health Level Seven International (HL7) healthcare standards organization.

Cloud Storage. The cloud stores patients' encrypted EMRs and the extraction signature, meanwhile, outputs storage location url and a timestamp.

Consortium Blockchain Network. We use consortium blockchain to reserve indexes of EMRs and achieve data sharing. The patient predefined access permissions in the smart contracts to ensure data sharing securely.

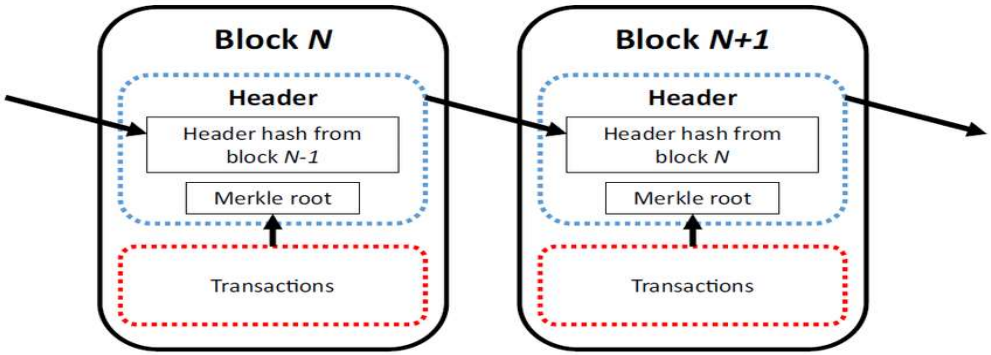
Data Sharing Layer

In this layer, the authorized patients, medical workers and healthcare institutions can request patients' EMRs and utilize them for making personal health plans, getting better clinic treatment or carrying out medical research.

SECURITY ANALYSIS

A. Immutability (Tamper Proof)

- Every transaction is hashed using SHA256 algorithms
- Each Block is also hashed and linked to previous block
- All the transactions are again grouped and a Merkle Root of the transactions are calculated and stored in the block.
- As Merkle root is created which contains all the transaction hashes it is highly impossible to tamper / modify any transaction which ensure Immutability / Data integrity



B. Privacy Preservation

In BPDS, the privacy property is ensured with the following features:

-- Anonymity. Each participant generates a unique account with *a **random public key***. Therefore, each transaction on the blockchain is anonymous.

-- Cloud Storage. The original EMRs are **encrypted** and stored in the cloud storage. ***limited storage capacity of blockcahin*** is solved, but also the risk of the original medical data leakage is greatly reduced.

-- Content Extraction Signature(CES) scheme when the doctors sign the EMRs. The patients can remove any sensitive portions in the original data to obtain the valid extraction signatures with minimal risk of data privacy leakage. Moreover, any entities cannot forge extraction signatures without the signer's private key.

-- Improved DPoS. BPDS uses the improved DPoS consensus to realize the trust between a certain number of preselected nodes in the consortium blockchain. In the improved DPoS, the selected medical organizations are reputable and reliable, which guarantees the reliability of data sharing.

C. Data Secure Storing and Sharing

The security of data storing and sharing is an important feature of BPDS. In this scheme, patients can have complete control over their own EMRs. The processes from data acquiring to data sharing are all secure.

-- Data Acquiring. The use of symmetric encryption technology guarantees the confidentiality and integrity of EMRs generated by doctors.

-- Data Storing. The patient encrypts the original EMRs and stores them in the cloud. The use of the distributed storage and CP-ABE-based access control scheme in cloud ensures the security of the medical data.

-- Data Release. First, the indexes of EMRs are reserved in a tamper-proof block chain, which cannot be modified arbitrarily. Second, blockchain is a distributed database without single-point-of-failure and each node has a copy of transaction records. Besides, the digital signature provides authentication, integrity, and non-repudiation for each transaction.

-- Data Sharing. In BPDS, the data access permissions are preset in the smart contracts. Only authorized users or institutions can use the EMRs. The executed access records are stored in the blockchain to trace the behaviours of data. Once someone violates the access rules or permissions, the data owner has the right to revoke his/her access permission

Smart Contracts

- Smart contracts are event-driven computer programs running on the public ledger. It can handle and transfer assets of considerable value.
- Specifically, smart contracts are some scripts or codes that are deployed in blockchain. Once the predefined conditions are activated, the scripts on the contract content could be executed without the help of an external trusted authority.
- The entire process is automated and the executed transactions are recorded in the public ledge for auditing. The asset owner has the right to revoke the access permissions to the user who violates the contract.
- In this system patients are allowed to predefine access permissions and duration in the smart contracts to finely control the data sharing of EMRs.

Expertise available with the proposed investigating group/institution in the subject of the project.

- We have expertise in Block chain technologies, light weight cryptography and AI/ML.
- We established AI/ ML Research Centre in collaboration with Bennet University leadingindia.ai. and an IOT Centre of Excellence is also available in the college.
- The principal investigator and CO PI successfully completed sponsored one UGC and Two DST projects in the area of security and cognitive computing.
- The principal investigator is having five SCI papers in the area of Security

Indicative techno-economic viability/cost benefits analysis of the project/product developed

Techno Viability:

- As part of techno viability there is no blockchain integrated smart and secure Health Care systems using light weight cryptography. So in this project we will adopt various new viable technologies as follows:
- In this project we will be using the state of the art sensors which are noninvasive and collect data using Arduino Gateway and data is stored in Block-chain for immutable and transparency of patient data store in a distributed manner . We will be implementing Light Weight Cryptography for transmitting data from sensor to Block-chain for secure transmission and to analyze patient data we implement machine learning algorithms.

Economic Viability

- In Health Care Systems for optimal economic viability we are using block chain technology which is an open source. Further Reduces transaction costs due to disintermediation, as well as near-real time processing.
- we are using light weight cryptography and machine learning algorithms for predictive analysis. So we can build a proto type within the economic viability.
- It is planned to develop a blockchain integrated smart health care system while ensuring system reliability, data security, robustness of processing and prediction algorithms, with minimal transmission delay, energy-efficiency and low setup and maintenance.

Cost benefits analysis:

- **Within optimal cost this system can provide the following benefits:**
- For people who are unable to express their health abnormalities and unable to move from the place, This system will help them to monitor the health condition.
- Medical assistance provisions in short span to save a life.

Budget

Sl. No.	Items	Budget (in Rs.)			
		1st Year	2nd year	3rd year	Total
A.	Recurring				
1.	Manpower (2 Nos)	25,000+ (10%)×12×2= 6,54,000	25,000+ (10%)×12×2= 6,54,000	28,000+ (10%)×12×2= 7,39,200	20,47,200
2.	Consumables	100000	100000	Rs.100000	3,00,000
3.	Travel	50,000	50,000	50,000	1,50,000
4.	Training Programme	-	50000	50000	1,00,000
4.	Contingency	50,000	50,000	50,000	150,000
5.	Overheads	100000	100000	100000	3,00,000
	Total (A)	9,54,000	10,04,000	10,89,200	30,47,200
B.	*Non Recurring*				
1.	Equipment	15,00,000	---	---	
2.	Fabrication Costs	1,00,000	---	--	
	Total (B)	16,00,000			
	Grand Total (A+B)	25,54,000	Rs. 10,04,000	Rs.10,89,200	Rs. 46,47,200

Equipment

Sl. No.	Generic name of the Equipment along with make & model	Imported/Indigenous	Estimated Costs
1	Six –High Configuration Desktops Systems which supports GPU	Indigenous	12,00,000
2	High Configuration Routers	Indigenous	50,000
3	Arduino Uno with Sensor Shield v2.0 and accessories	Indigenous	20,000
4	Sensors	Indigenous	30,000
5	Two-High Configuration Laptop Systems	Indigenous	2,00,000
		Total	15,00,000

Justification:

We need six (6) systems with good configuration which supports GPU to establish a 6 node blockchain private network and also for running machine learning algorithms. Minimum configuration is Core i7 with 16 GB RAM , 1 TB HDD and Nvidia 1080 Ti graphics card for processing health sensor data for analysis. Further Arduino Uno with Sensor Shield v2.0 and accessories, various sensors, two high-end laptops to carry the work to remote places and for presentations and High Configuration Routers etc..

Pert Diagram indicating project life

Sl.no.	Task	%age of Work to be completed	6 m	12 m	18 m	24 m	30 m	36 m
1	Data Collection	10						
2	Data Analysis and problem Identification	40						
3	Training, Algorithm Development, Prototype Design with hardware software integration and Mobile launch of the same.	90						
4	Full online testing of the prototype on site	100						

m* - months

THANK YOU