A Future Solution for Block chain Based Distributed Electronic Health Record Data with Confidentiality and Security using Blake2b

Majji Vikram Raj Kumar, Duvvada Rajeswara Rao

Abstract**: A blockchain is a shared, public register, storing business transactions and outlining assets, and of which immutable in nature. Globally Electronic Health Record (EHR) market is swiftly rising. Due to this swift growth of the EHR market worth is predictable to be $50 billion in 2025. Blockchain will revolutionize in the medical field, to store medical historical records in a tamper proof, secure, and more reliable in the effective diagnosis and treatment in the real-time medical data. Health care data it can be twisted copied and modified faster than ever before and if the data is the critical thing behind more efficient care block chain may be the medium to get us there, currently the medical organizations are being ruined because of poor data integration. Our project consists of Drug description, Data Security, Huge Data, cloud. Once the data is entered the data goes to the block and links to the chain. We are using blake2b, because blake2b is much faster and has less rounds compared with the blake. Blake2b is about 30 percent faster than the blake. The data is finally transferred to the Json file to compact and easy to transfer in nature. We similarly converse the privileges of blockchain, along with the tests tackled and future viewpoints. Execution measurements in blockchain systems, for example, latency, throughput, Round Trip Time (RTT), has been advanced for achieving upgraded results. Contrasted with customary EHR frameworks, which use customer server design, the proposed framework utilizes blockchain for improving proficiency and security.

***Keywords** : blockchain, healthcare, EHR, medical data, distributed ledger.*

I. INTRODUCTION

Blockchain is possibly best known for trust cryptocurrency transactions in a protected way. The usage of blockchain for health archives is pacific in its initial stages, but then again here are vibrant safety paybacks that could advantage to cut healthcare data cracks while creation it far easier for data to be collected among benefactors and saved by patients. Currently, the way health information's are kept and shared leaves much to be anticipated. The system is not well-organized, there are many barriers that avoid the distribution of information and patients' health information is not permanently stored by a sole organizations provider instead patient`s full health records are scrapped and blowout across numerous provider`s systems. Blockchain proposes is a chain of information chunks of blocks, which hold particulars of business transactions, separately encrypted to guarantee secrecy. Putting away the information in a sole site, blockchain data in an programmed record, which is circled across synchronized, reproduced records. Each one is associated with the previous block by a one of a kind open key with access to information deliberately controlled. As has been uncovered with the monstrous information breaks, single units can't be trusted to hold tremendous degrees of information and keep it ensured in a provincial framework. Stacking data in a circulated framework could be a pragmatic other option. On the off chance that blockchain is reused for wellbeing data, instead of various medicinal services associations are putting away their individual duplicates of a patient's information, the patient would permit independently access to their data and give them safely.

II. RELATED WORK

In this paper, the works involving the effort supported out by many authors on blockchain based distributed Electronic health record data methods are discussed.

Li, Hongyu, et al. [1] proposed a shared approach in how the medical information is preserved in the blockchain system. They able to provide a reliable storage resolution to guarantee the primitive and verification of stored information while protective confidentiality for users. They executed a sample of DPS (data preservation system) built on real world blockchain based like Ethereum. In order to confirm our scheme, thorough researches and assessments remained.

Concluding the most shared conditions, Griggs, Kristen N., et al. [2] provides a archetype smart gadget that triggers smart contracts that inscribes the records of all actions on the blockchain. This smart contract arrangement would sustenance real-time patient monitoring and medicinal involvements by distribution of announcements to patients and medicinal specialists, while also upholding a secure record of who has originated these activities. This would resolve numerous security vulnerabilities related with distant patient check, control and automate the distribution of notifications to all complicated parties.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Majji Vikram Raj Kumar*, Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India. Email: vikramrocky1996@gmail.com

Dr. D. Rajeswara Rao, Computer Science and Engineering HOD, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India. Email: hodcse@vrsiddhartha.ac.in

Retrieval Number: F8033038620/2020©BEIESP
DOI:10.35940/ijrte.F8033.038620

Zhang, Aiqing [3] proposed two sorts of the blockchains, that are private blockchain and consortium blockchain, are developed by formulating their information structures, and accord components.

The private blockchain is liable for putting away the PHI (personal health information) while the consortium blockchain tracks the protected records of the PHI. So as to accomplish information security, get to control, protection conservation and secure hunt, every one of the information including the PHI, catchphrases and the patients' character are open key scrambled with watchword search. Besides, the square generators are vital to give confirmation of conformance to adding new squares to the blockchains, which ensures the framework accessibility. Security investigation shows that the proposed convention can meet with the security purposes.

Guo, Rui, et al. [4] suggested that to ensure the legitimacy of EHRs typified in blockchain, we present a trait-based mark plot with various specialists, in which a patient supports a message as indicated by the characteristic while uncovering no data other than the proof that they has witness to it. Besides, there are numerous experts deprived of disclosed in single or central one to generate and separate exposed isolated keys of the patient, which stays away from the escrow matter and fits into with which the technique of appropriated information storing in the blockchain. By distribution of the anonymous pseudorandom work seeds between specialists, this convention competes with conspiracy assault.

Sun, You, et al. [5] proposed the requirement of protection safeguarding and checking of administrators with dual capabilities. On one hand, the clients need to check the validness of EHR information just as the personality of the endorser. Then again, the patient needs to keep his genuine personality private to such an extent that others can't follow and derive his character data. In any case, run of the mill blockchain frameworks that utilization pen names open keys, for example, Bitcoin's blockchain, can't bolster such protection safeguarding check. In such frameworks, it is difficult to check the legitimacy of underwriter's personality, and foes or inquisitive gatherings can figure the genuine character from the arrangement of proclamations and moves made with a particular pen name derivation assaults, for example, by exchange diagram examination. Right now, propose a decentralized trait-based mark plot for human services blockchain, which gives proficient protection safeguarding check of validness of EHR information and underwriter's personality. The investigation and trials show that our plan is successful and deployable.

III. SCOPE

The extension of blockchain technology in healthcare is enormous. Scope for an enhanced technology-integrated patient trails through integration with blockchain technology for benefit monitoring and allows securely connect with the remote linking with providers.

IV. BLAKE2B ALGORITHM

Blake2 is impressively speedier than blake, because of its smaller number of revolutions. blake2b sorts out 12 rounds, and blake2s calculation composes 10 rounds, contrasted with 16 and 14 correspondingly for blake. On long messages, the blake2b what's more with the blake2s types are required to be generally 25% and 29% quicker. Equal hashing likewise helps from cutting edge CPU advancements, as recently surveyed. Intel processor Sandy Bridge, blake2b is 72.99% faster than blake-512, and blake2s is 40.16% more rapidly than blake -256, • On intel i3 cpu, blake 2b is 30.15% quicker than blake -512, and blake2s is 43.78% more rapid processing than blake -256.

V. METHODOLOGY

First the central admin will login into the blockchain system. If patient want to register, they will check according to policies and procedures of the hospital. Name, date of birth, gender, address, name of guardian (in case the patient is a minor), contact number, email address (optional) are the details collected from the patient to input into the blockchain records. If in case an unidentified patient is brought to the hospital, (the patient is unconscious) and patient to be registered first we will register as anonymous and take minimal registering details from the person who brought to the hospital. The complete information is registered into the blockchain network. The process for the classification task of solution for blockchain based distributed Electronic health record data methods as shown in figure.

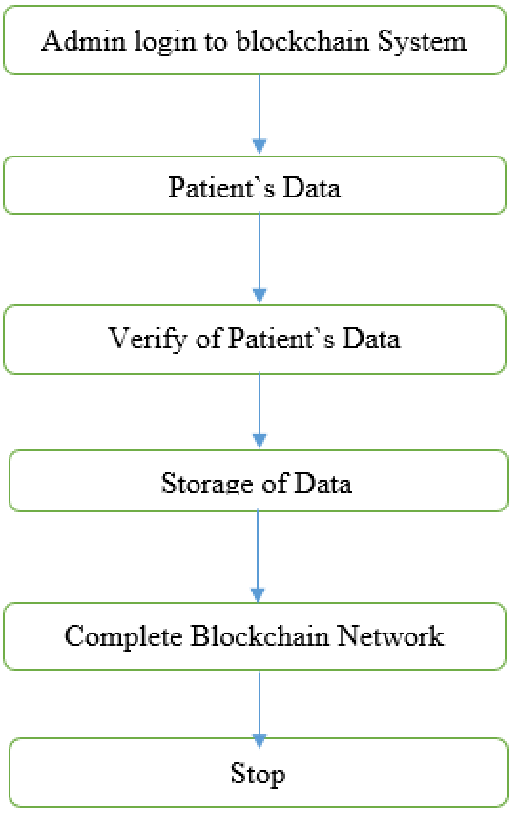


Fig. 1. Overview of Proposed process

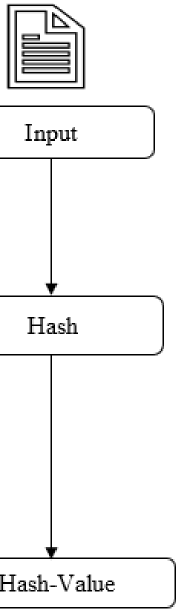


Fig. 2. Overview of Methodology

Algorithm:

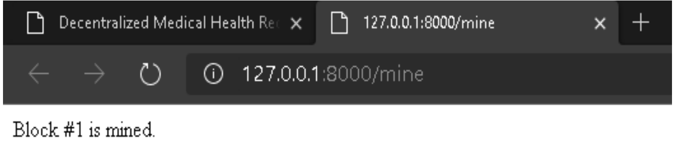
```
Step1: Input of medical data into system (patientId, Prescriptions)
Step2: verification of the patient data
Step3: Apply blake2b algorithm
Step4: if (id==0):
          bid="GENESIS BLOCK"
          prevhash="none"
      else:
          bid=self.id
          lastblock=self.x[-1]
          prevhash=lastblock["hash"]
Step5: Stop
```

VI. EXPERIMENTAL SETUP

In our project python is used as a language to implement blockchain technology. We used Amd A9 processor with 3.00 GHz, 4 GB RAM 3200 MHz, 128 GB SSD, 20 Mb/s internet connection. We had used Flask micro web framework written in Python language. It is pronounced as a microframework because it does not need specific tools or libraries and easy to install in nature we had used flask framework.

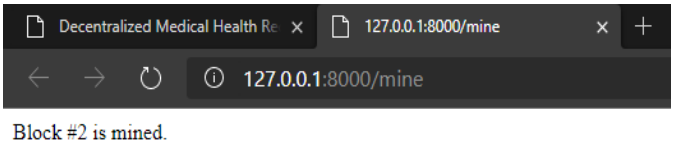
VII. RESULTS

In this, when we can observer the data in medical blockchain is inserted, data mining, block formation, block mining and the complete project user interface design.



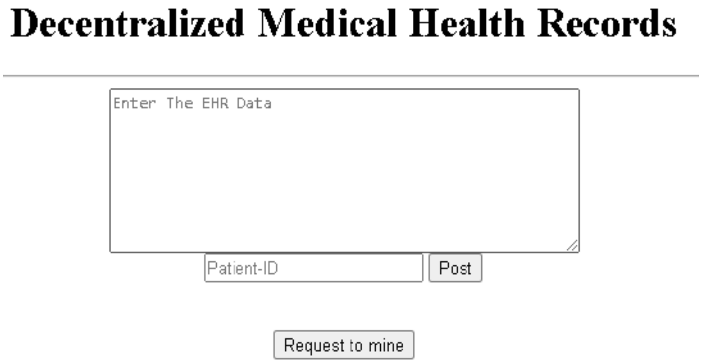
Block #1 is mined.

Fig.3. Block #1 mining



Block #2 is mined.

Fig.4. Block #2 mining



Decentralized Medical Health Records

Fig.6. Application User interface

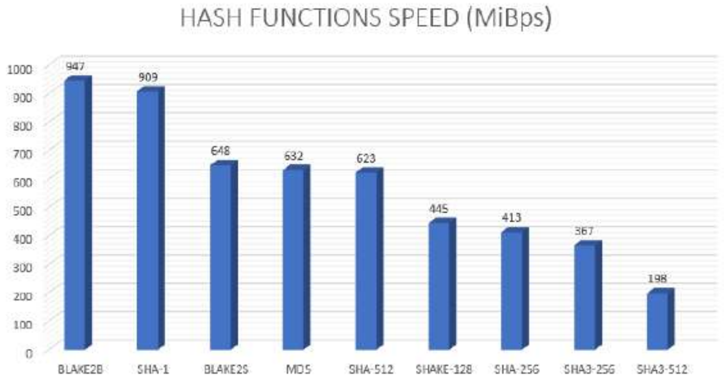
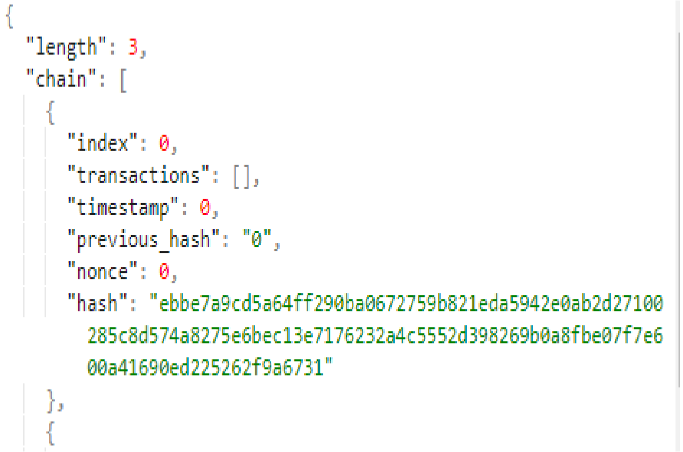
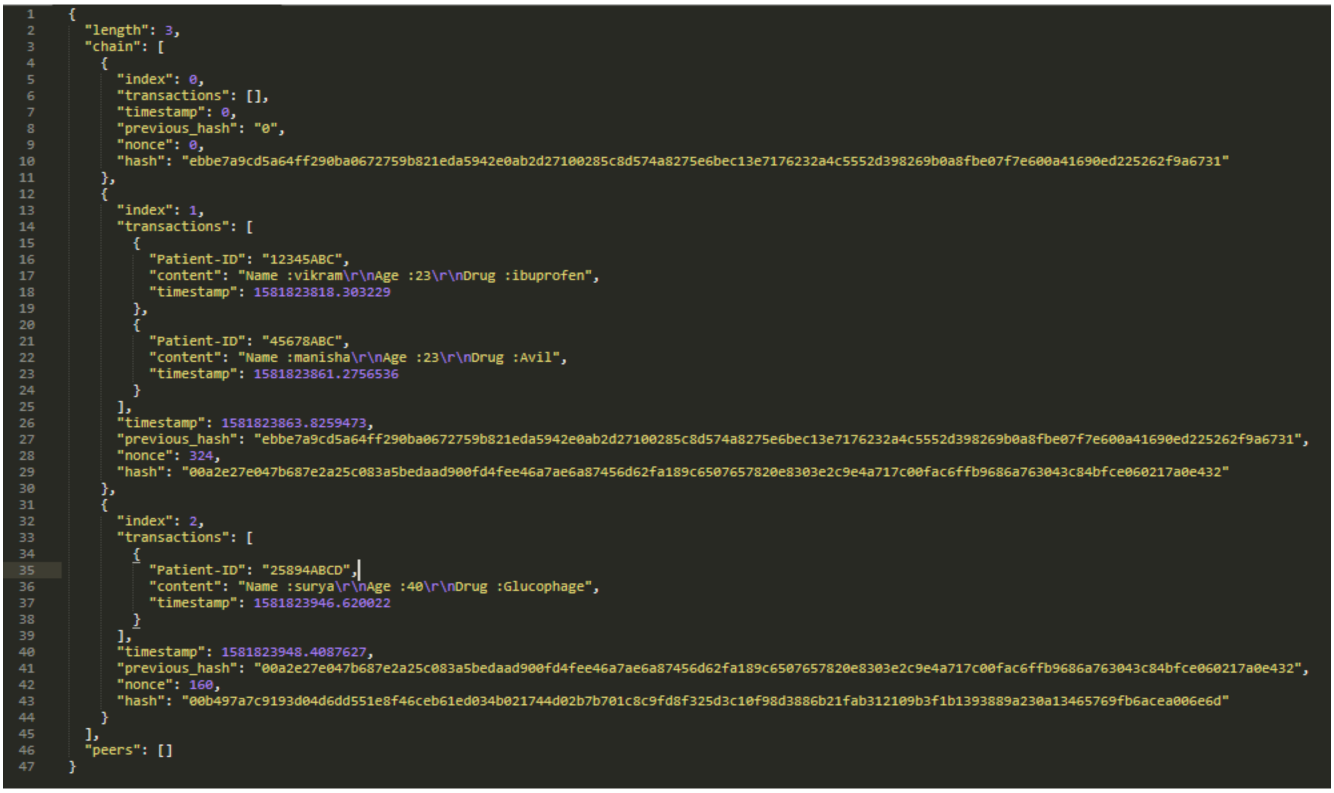


Fig.7. Hash Function Speed (MiBps)



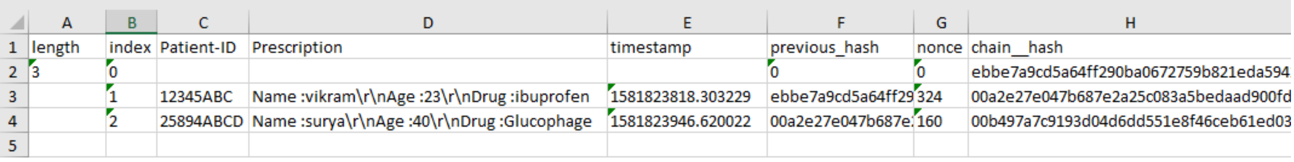
```
{
  "length": 3,
  "chain": [
    {
      "index": 0,
      "transactions": [],
      "timestamp": 0,
      "previous_hash": "0",
      "nonce": 0,
      "hash": "ebbe7a9cd5a64ff290ba0672759b821eda5942e0ab2d27100
        285c8d574a8275e6bec13e7176232a4c5552d398269b0a8fbe07f7e6
        00a41690ed225262f9a6731"
    },
    {
```

Fig.8. Genesis block



```
{
  "length": 3,
  "chain": [
    {
      "index": 0,
      "transactions": [],
      "timestamp": 0,
      "previous_hash": "0",
      "nonce": 0,
      "hash": "ebbe7a9cd5a64ff290ba0672759b821eda5942e0ab2d27100285c8d574a8275e6bec13e7176232a4c5552d398269b0a8fbe07f7e600a41690ed225262f9a6731"
    },
    {
      "index": 1,
      "transactions": [
        {
          "Patient-ID": "12345ABC",
          "content": "Name :vikram\r\nAge :23\r\nDrug :ibuprofen",
          "timestamp": 1581823818.303229
        },
        {
          "Patient-ID": "45678ABC",
          "content": "Name :manisha\r\nAge :23\r\nDrug :Avil",
          "timestamp": 1581823861.2756536
        }
      ],
      "timestamp": 1581823863.8259473,
      "previous_hash": "ebbe7a9cd5a64ff290ba0672759b821eda5942e0ab2d27100285c8d574a8275e6bec13e7176232a4c5552d398269b0a8fbe07f7e600a41690ed225262f9a6731",
      "nonce": 324,
      "hash": "00a2e27e047b687e2a25c083a5bedaad900fd4fee46a7ae6a87456d62fa189c6507657820e8303e2c9e4a717c00fac6ffb9686a763043c84bfce060217a0e432"
    },
    {
      "index": 2,
      "transactions": [
        {
          "Patient-ID": "25894ABCD",
          "content": "Name :surya\r\nAge :40\r\nDrug :Glucophage",
          "timestamp": 1581823946.620022
        }
      ],
      "timestamp": 1581823948.4087627,
      "previous_hash": "00a2e27e047b687e2a25c083a5bedaad900fd4fee46a7ae6a87456d62fa189c6507657820e8303e2c9e4a717c00fac6ffb9686a763043c84bfce060217a0e432",
      "nonce": 160,
      "hash": "00b497a7c9193d04d6dd551e8f46ceb61ed034b021744d02b7b701c8c9fd8f325d3c10f98d3886b21fab312109b3f1b1393889a230a13465769fb6acea006e6d"
    }
  ],
  "peers": []
}
```

Fig.9. JSON view sublime text editor



	A	B	C	D	E	F	G	H
1	length	index	Patient-ID	Prescription	timestamp	previous_hash	nonce	chain__hash
2	3	0				0	0	ebbe7a9cd5a64ff290ba0672759b821eda594
3		1	12345ABC	Name :vikram\r\nAge :23\r\nDrug :ibuprofen	1581823818.303229	ebbe7a9cd5a64ff29	324	00a2e27e047b687e2a25c083a5bedaad900fd
4		2	25894ABCD	Name :surya\r\nAge :40\r\nDrug :Glucophage	1581823946.620022	00a2e27e047b687e:	160	00b497a7c9193d04d6dd551e8f46ceb61ed03
5								

Fig.10. JSON view excel

VIII. CONCLUSION

In this paper real structure of sharing connecting medical records using blockchain innovation framework is designed. Each part of therapeutic records is examined quickly. The attributes of blockchain are clarified on its edge. Huge information expository consumes its distinct capacities and is clarified quickly in presentation. Medicinal records sharing framework's respectability, cancellation and cleanse, record sharing, stockpiling, design transformation, information relocation, understanding and institutionalization are inspected. Various ways to deal with defeat all human related difficulties are proposed right now certainty. The utilization of blockchain is significant. Nonetheless, different advancements, large information examination and tokenization, are especially expected to enhance the first plan. Albeit genuine execution isn't placed into creation, the methodologies ought to be down to earth enough.

Every recommendation gives a few subtleties and explanations for the specialized heading. Expectation that this will invigorate further innovative work to support patients just as general medicinal network. I had used Blake2b as blockchain formation algorithm there is Blake3 which is more advanced than the blake2b. Concerning about resources available we had developed on blake2b.

REFERENCES

1. Li, Hongyu, et al. Blockchain-based data preservation system for medical data. Journal of medical systems 42..8 (2018):141.
2. Griggs, Kristen N., et al. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems 42.7 (2019): 130.
3. Zhang, Aiqing, and Xiaodong Lin. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems 42.8 (2018): 140.
4. Guo, Rui, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE access 6 (2018): 11676-11686.
5. Sun, You, et al. A decentralizing attribute-based signature for healthcare blockchain. 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2018.
6. Boulos, Maged N. Kamel, James T. Wilson, and Kevin A. Clauson. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. (2018): 25.
7. Dagher, Gaby G., et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society 39 (2018): 283-297.
8. Ji, Yaxian, et al.BMPLS: blockchain-based multi-level privacy preserving location sharing scheme for telecare medical information systems. Journal of medical systems 42.8 (2018): 147.
9. Gatteschi, Valentina, et al. "Blockchain and smart contracts for insurance: Is the technology mature enough?." Future Internet 10.2 (2018): 20.
   (EMR). 2018 IEEE International Conference on Communications (ICC). IEEE, 2018.

AUTHORS PROFILE

Majji Vikram Raj Kumar, Studying Master of Technology, Department of Computer Science and Engineering, V R Siddhartha Engineering College, Vijayawada. I come from a humble family and this pushed him to carve out his own destiny. I am working as freelancer in web development and digital marketing in Vijayawada. I had worked with more than 40 websites designs and 6 digital marketing campaigns. Interested in Blockchain technology and cryptocurrency mining. I am an enthusiast of blockchain technology and the disruptive value of decentralized applications. I am currently holding Bitcoin, Ethereum, XRP (Rippe), Bitcoin cash, Cardano, Tron, Stellar, Dogecoin, Ubiq, Decred, Bitcoin gold, Bittorrent, Bitmax token, Smart cash, Vite, Bittube, Expanse, Musicoin, Pirl, Lite gold.

Dr. Duvvada Rajeswara Rao, Head of Department of Computer Science and Engineering (CSE), HOD, Velagapudi Ramakrishna Siddhartha Engineering College, vijayawada. he is qualified in Ph.D. in Computer Science & Engineering. He has 25 years of teaching experience and she published more than 62 journal papers and 5 international conference papers.