iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35243

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Securing Hospital Data with Blockchain and AI

M. Shailaja[1], B. Rajesh[2], P. SaiPrakash[3], Mrs. V. Sandya[4], Mr. B. Ramji[5]
[1, 2,3] *B. Tech Student,* [4] *Assistant Professor,* [5]*Assistant Professor, Dept of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad, Telangana, India*

Abstract: ***In cyber world everything is dependent on data and all Artificial Intelligence algorithms discover knowledge from past data only, With the development of information technologies, the trend of integrating cyber, physical and social (CPS) systems to a highly unified information society, rather than just a digital Internet, is becoming increasing obvious. An increasing amount of personal data, including location information, web-searching behaviour, user calls, user preference, is being silently collected by the built-in sensors inside the products from those big companies, which brings in huge risk on privacy leakage of data owners. In this paper, we aim at securing data by combining blockchain and AI together, and design a Secure Networking architecture (termed as SecNet) to significantly improve the security of data sharing, and then the security of the whole network. In SecNet, to protect data, one of the biggest challenges is where and how to store data, because users have to give their data to service providers if they want to use certain services or applications.***

I. INTRODUCTION

This project is titled as “Securing Data With Block chain and AI”. This software provides facility to secure data storing, sharing and computing instead of communicating. This project uses block chain technologies, and AI-based secure computing platform as well as block chain-based incentive mechanism, offering paradigm and incentives for data merging and more powerful AI to nally achieve better network security. Moreover, we discuss the typical use scenario of SecNet in medical care system, and gives alternative ways for employing the storage function of SecNet. Furthermore, we evaluate its improvement on network vulnerability when countering DDoS attacks, and analyze the inventive aspect on encouraging users to share security rules for a more secure network. In this project, we aim at securing data by combining block chain and AI together, and design a Secure Networking architecture (termed as SecNet) to significantly improve the security of data sharing, and then the security of the whole network, even the whole CPS(Cyber, Physical and Social) Systems. In SecNet, to protect data, one of the biggest challenges is where and how to store data, because users have to give their data to service providers if they want to use certain services or applications. This is caused by the inherent coupling of user data and application in current service mechanisms, which significantly hinders the development of data protection and application innovation. The main features of this project is securing data by combining block chain and AI together, and design a Secure Networking architecture (termed as SecNet) to significantly improve the security of data sharing, and then the security of the whole network. In addition, swarm intelligence can be used in SecNet to further improve the data security, by collecting different security knowledge from huge amount of intelligent agents scattered everywhere in the CPS, with the help of trusted exchange mechanisms for incentive tokens.

II. LITERATURE SURVEY

In this proposed system we introduce the secure network architecture to providing the security for hospital data and provides the secure sharing. By using AI there is we can search for particular patient details. In past, researchers have used data from different sources .The past researches are Hyper connected network: A decentralized trusted computing and networking paradigm , Lightweight RFID protocol for medical privacy protection in IoT, Enhancing selectivity in big data, Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective, Adaptable blockchain-based systems: A case study for product traceability:A case study for product traceability. Tracing the origin of products across complex supply chains requires a transparent, tamper-proof metadata infrastructure that is not only trusted by all the involved parties but also adaptable to changing environments and regulations. Can such advanced infrastructure be implemented in a decentralized way? Qinghua Lu and Xiwei Xu share their story of developing the origin Chain system, which leverages emerging blockchain technology to do so.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

III. PROPOSED SYSTEM AND ARCHITECTURE

In this paper, we propose the SecNet, which is a new networking paradigm focusing on secure data storing, sharing and computing instead of communicating. SecNet provides data ownership guaranteeing with the help of block chain technologies, and AI-based secure computing platform as well as block chain-based incentive mechanism, offering paradigm and incentives for data merging and more powerful AI to nally achieve better network security. Moreover, we discuss the typical use scenario of SecNet in medical care system, and gives alternative ways for employing the storage function of SecNet. Furthermore, we evaluate its improvement on network vulnerability when countering DDoS attacks, and analyze the inventive aspect on encouraging users to share security rules for a more secure network

The system is very simple in design and to implement. The system requires very low system resources and the system will work in almost all configurations. It has got following features:

A. Secure data Storage and Processing.
B. Safe data transfer.
C. Increased customer trust.
D. Security is more.
E. Accuracy is more.

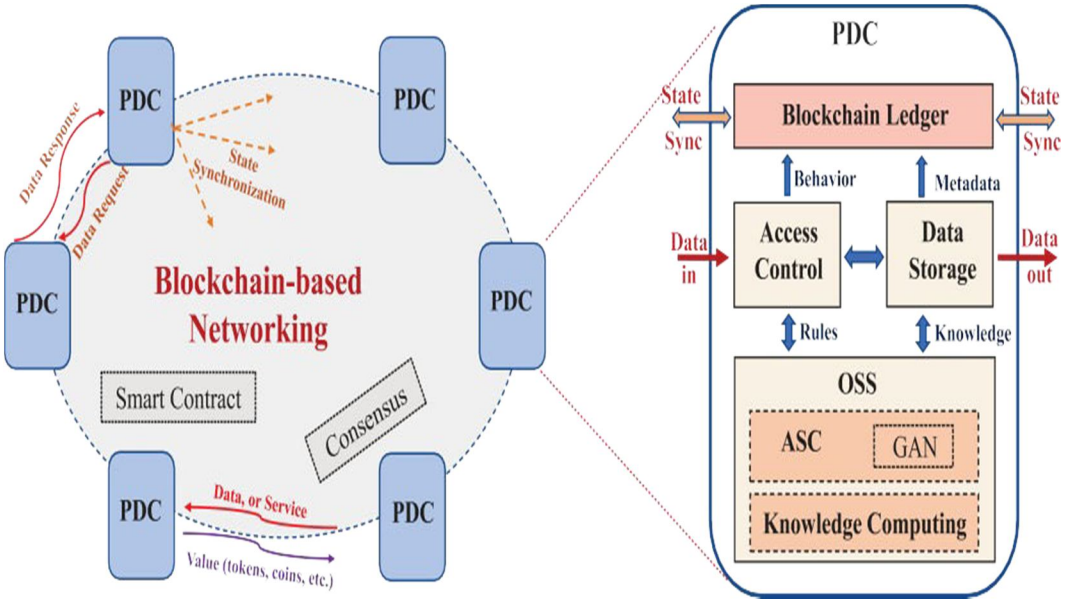


Fig. 1 System Architecture

A system architecture is very important to understand the flow of the project. It describes the step-by-step procedure of the complete project. In this the overall architecture is connected to the Blockchain based network.The overall architecture is tells about the secure network. SecNet are connected with data storage module and access control module for data security. SecNet is build as an architecture for a more secure cyberspace, by integrating three key components:

1) Block chain-based data sharing with ownership guarantee
2) AI-based secure computing platform based on big data to produce intelligent and dynamic security rules
3) Trust value exchange mechanism for purchasing security services.

In this Private Data Center (PDC'S) are provides more secure and intelligent data storage system via physical entities instead of software-based algorithms as in open Personal Data Store (PDS). Every PDC connected with each other and provide Blockchain based protection. Every PDC cooperate through the execution of smart contract in order to reach consensus. Each PDC/node contain Blockchain ledger to synchronize state with other nodes. Blockchain ledger contains Operating Secure System(OSS), which enables the AI based Secure Computing (ASC)f for generating knowledge and Securing the data

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

IV. IMPLEMENTATION

A. *Module and its Description*

1) *Patient Register:* In this Module Patients first create his profile with all details like Name, Age, Problem Description and then select desired hospital with whom they wishes to share/subscribe data. While creating profile application will create Blockchain object with allowable permission and it will allow only those hospitals to access data. After clicking on create they will get a Patient Id. The Patient Id is different for every new registered patient.
2) *Hospital Login:* In this Module Hospital is login with entering details like Hospital Name and password, then they have to click on login button. After clicking on login they will get one screen that contains Access Patient Data and Logout links. Here Hospital1 and Hospital2 are using in this application as two organizations with whom patient can share data. At a time any hospital can login to application and then enter search string as disease name.
3) *Access Patients Data:* In this module if the Hospital wants to access the patient details, then they have to click on Access Patient Data, then they will get the patient details in new screen if there is patients are registered with that particular Hospital. After getting patients information click on logout. AI algorithm will take input disease string and then perform search operation on all patients to get similar disease patients and then check whether this hospital has permission to access that patient data or not, if hospital has access permission then it will display those patients records to that hospital.
4) *Patient Login:* In this Module the Patient can login to application with his Patient id and check total rewards he earned from sharing data. In this technique all users who is sharing the data will earn rewards point upon any user access his data. trusted value-exchange mechanism for purchasing security service, providing a way for participants to gain economic rewards when giving out their data or service, which promotes the data sharing and thus achieves better performance of AI.
5) *View Block chain Hash code:* In this Module after login the patient they will get a Blockchain object. The Blockchain object is generated for every registered patients. The Blockchain object is different from one patient to another patient. Blockchain object will be generate on that access data and allow only those users to access data which has permissions. In Blockchain object user will add/subscribe share data and give permission.

V. RESULTS AND ANALYSIS

In this project when we runs the code in Django server, output gives the home page of the Securing data with Blockchain and AI. By using the Home page patient has rights to create their profile and Hospitals has rights to login to the system and Hospitals access the data who are registered with the respected hospitals.

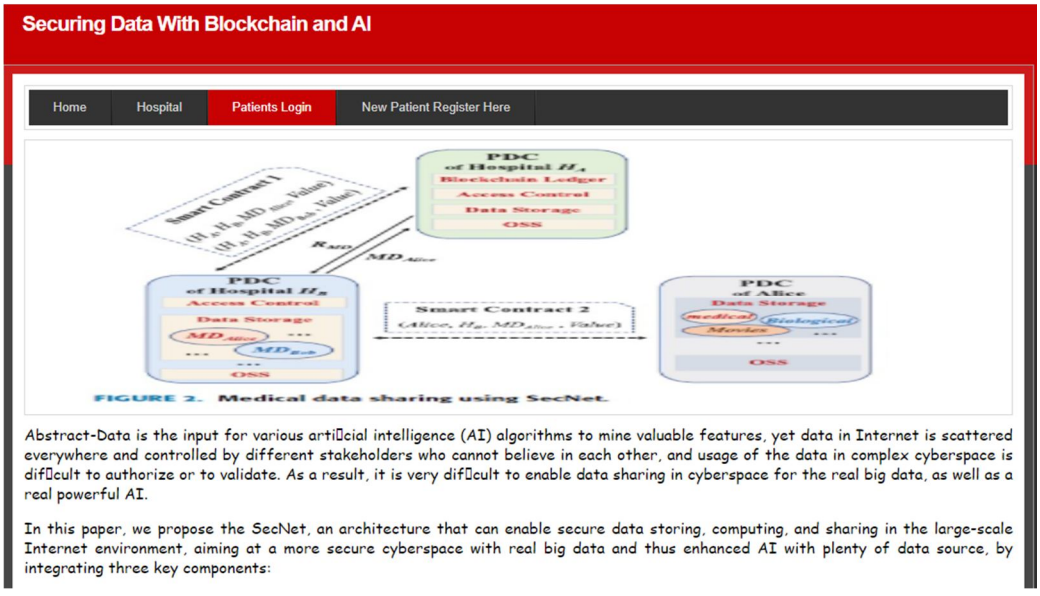


Fig 1:Home page

In above screen click on 'New Patient Register Here' link to get below screen. In below screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile.

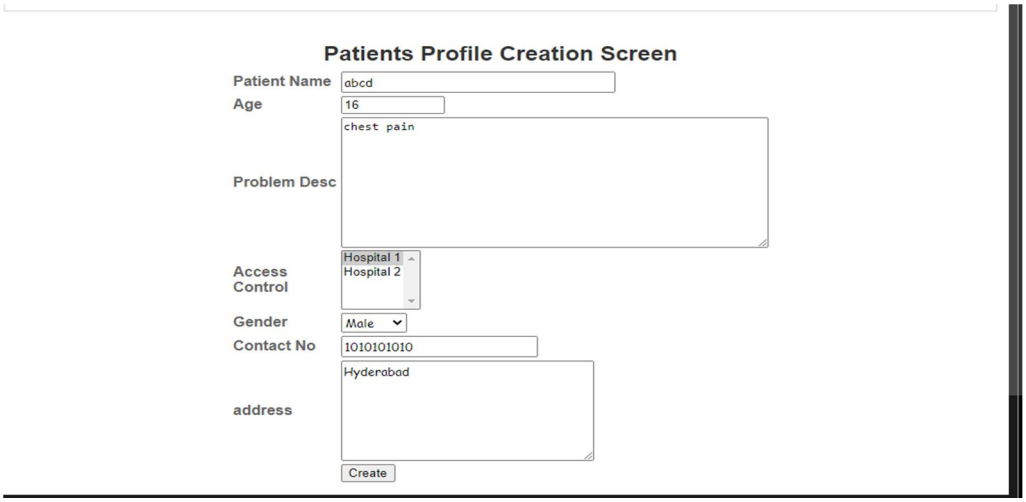


Fig 2: Patient Profile Login

In home page if we want to login as Hospital1 click on 'Hospital' link to get below screen. Use 'Hospital1' as username and 'Hospital1' as password then click on login.

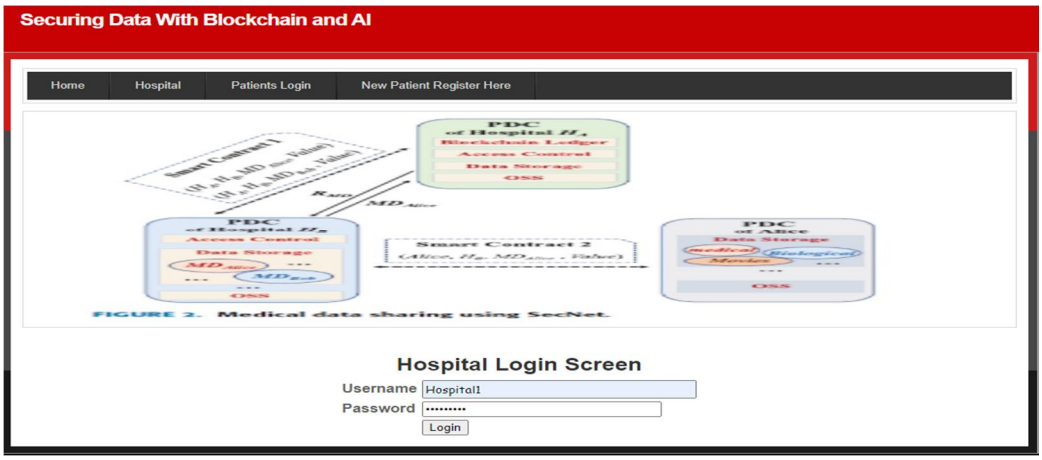


Fig 3: Hospital Login

In new screen click on 'Access Patient Share Data' link to search for patient details. Then we get the below screen. In below screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get next screen.

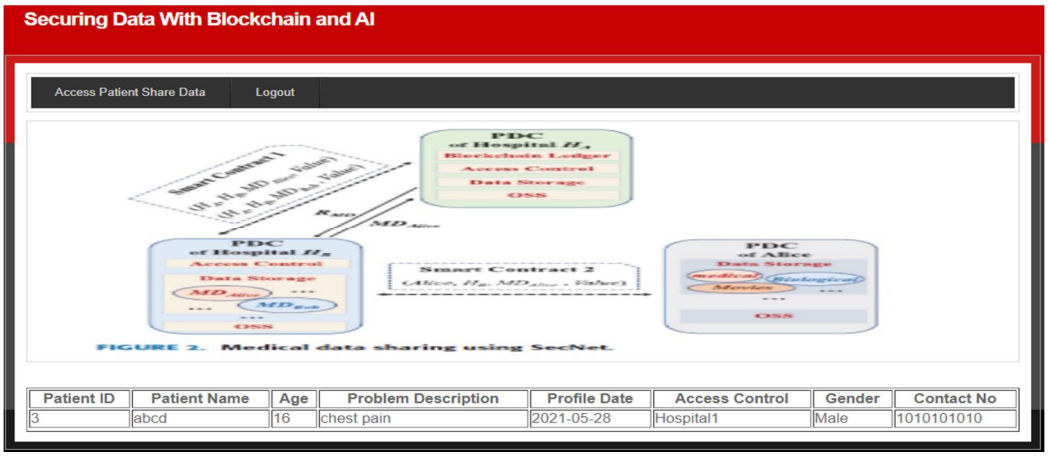


Fig 4:Accessing the patient data

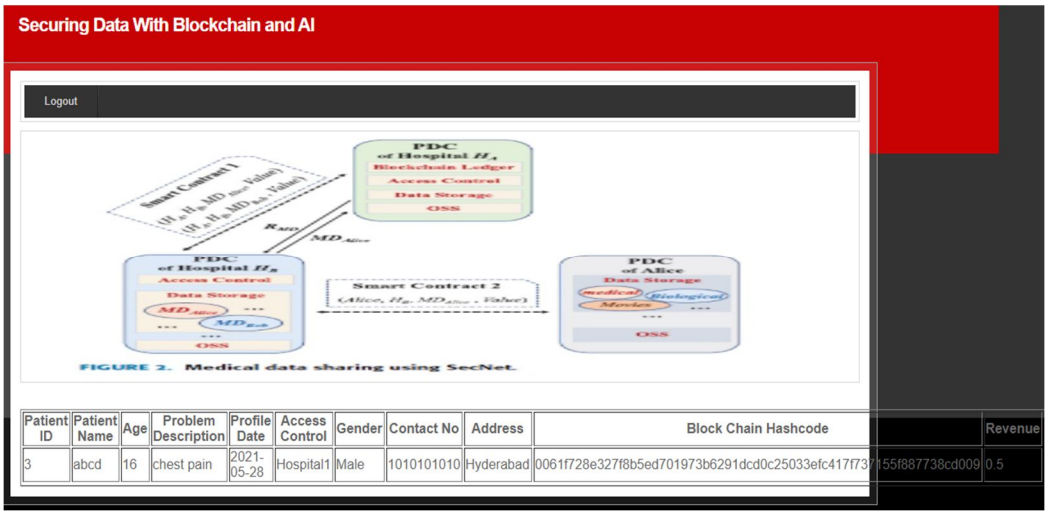


Fig 5:Viewing Blockchain Hashcode

In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

VI. CONCLUSION

In this paper there have been some related works that have utilized the Public health record database and techniques to achieve various different approaches and to identify their flaws and shortcomings. There have been various methodologies that have been proposed by a plethora of authors each offering a unique technique to Public Health Record management. This has influenced our approach drastically and helped and enabled us to propose a secure and efficient Public Health Record management system that uses the Blockchain Paradigm. The Blockchain is used due to its inherent nature of being resilient to changes and tampering, this is utilized to provide an effective Access control Mechanism that can help restrict the leakage of valuable sensitive data of the patients in the Public Health Records. The methodology discussed will be implemented in the upcoming researches.

VII. FUTURE ENHANCEMENTS

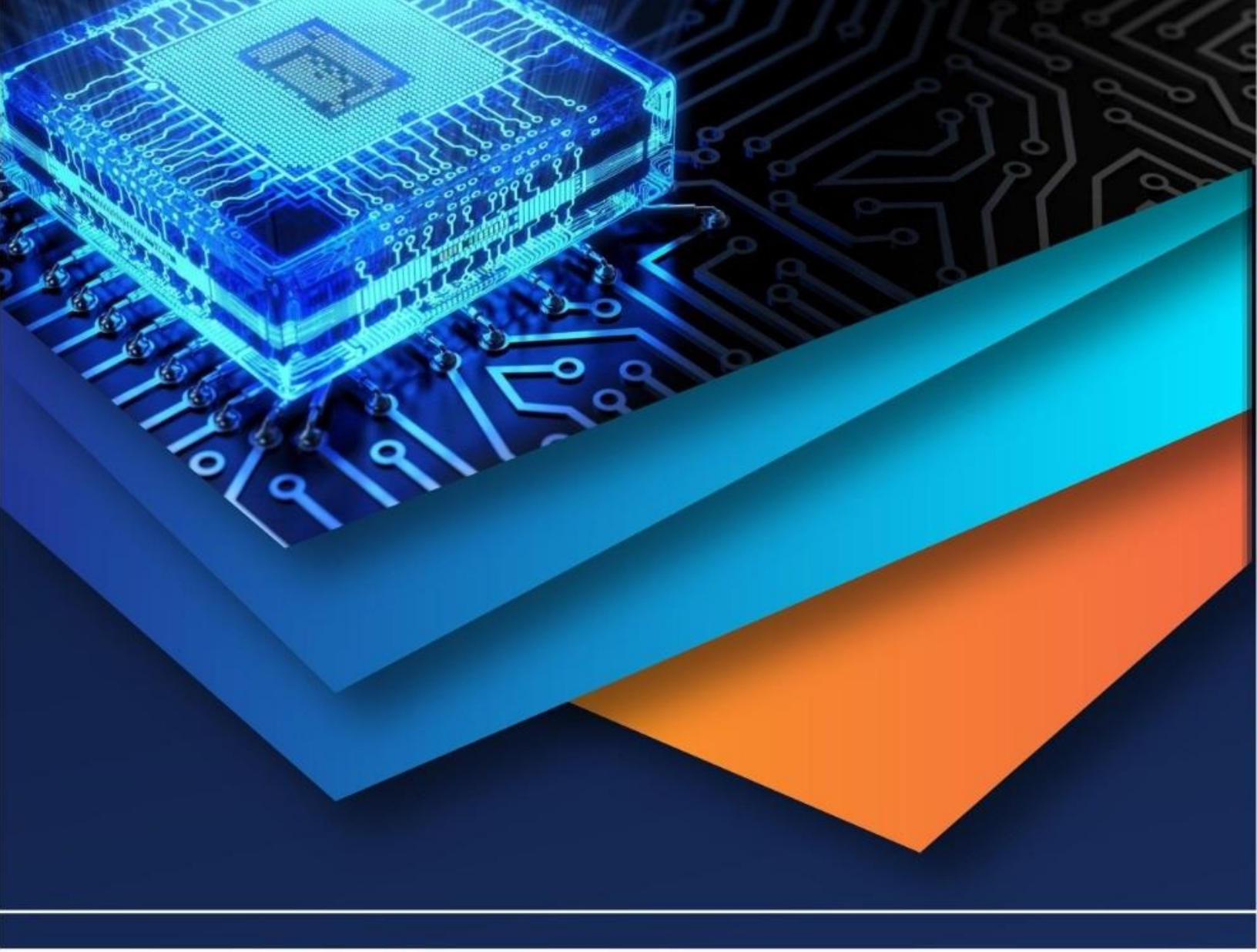
In future work, we will explore how to leverage blockchain for the access authorization on data requests, and design secure and detailed smart contracts for data sharing and AI-based computing service in SecNet. In addition, we will model SecNet and analyze its performance through extensive experiments based on advanced platforms (e.g., integrating IPFS and Ethereum [28] to form a SecNet-like architecture). The other direction will include advances in AI that when combined with blockchain can substantially improve its value. These advance can provide both increased cyber security and more ethical use of data.

VIII. ACKNOWLEDGEMENT

We take this opportunity to express our gratitude to PRC Coordinator Mr. B. Ramji, and Mrs. V.Sandya, Department of CSE, CMR Technical Campus, for their guidance and support at every stage of the project. We would like to extend our gratitude to HOD Dr. K. Srujan Raju, Department of CSE, CMR Technical Campus for his support. We also take this opportunity to thank Dr. A. Raji Reddy, Director CMR Technical Campus, for providing us with all the facility that was required.

REFERENCES

[1] H. Yin, D. Guo, K.Wang, Z. Jiang, Y. Lyu, and J. Xing, ``Hyper connected network: A decentralized trusted computing and networking paradigm," IEEE Netw., vol. 32, no. 1, pp. 112117, Jan./Feb. 2018.
[2] K. Fan, W. Jiang, H. Li, and Y. Yang, ``Lightweight RFID protocol for medical privacy protection in IoT," IEEE Trans Ind. Informat., vol. 14, no. 4, pp. 16561665, Apr. 2018.
[3] T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ``Amber: Decoupling user data from Web applications," in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 16.
[4] M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang, and S. Sen, ``Enhancing selectivity in big data," IEEE Security Privacy, vol. 16, no. 1, pp. 3442, Jan./Feb. 2018.
[5] Y.-A. de Montjoye, E. Shmueli, S. S.Wang, and A. S. Pentland, ``openPDS: Protecting the privacy of metadata through SafeAnswers," PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY