International Journal of Research (IJR)

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

An Integrated Approach Of Blockchain And For Securing Hospital Data

Pelluri Venkat Chandu[1], Jakkula Siddarth[2], Kamatam Venkata Rohan[3], Shaik Zulfeqhar Ahmed[4], Dr.Mohammad Riyaz Belgaum[5], Mrs.M.Srilakshmi[6]

[1,2,3,4] U.G. Scholar, [5]Guide, Associate Professor, [6]Head of the Department

[1,2,3,4,5,6] G.Pullaiah College of Engineering and Technology

Email:- [1]venkatchandupvc1@gmail.com, [2]siddu.j.2k@gmail.com, [3]k.v.rohan359@gmail.com, [4]shaikzulfikar786@gmail.com, [5]riyazbmd@gmail.com

ABSTRACT

Data is the enter for diverse computing (AI) algorithms to mine vital characteristics, however, statistics at the internet is shipped anywhere and managed with the aid of using more than one stakeholders who do not accept as true with one some other, making statistics utilization tough to authorize or validate in complex our on-line world. As a result, setting up actual-time statistics sharing in our on-line world, moreover as a actual-time effective AI, is particularly tough. By integrating 3 vital components, we advise the SecNet, an structure in order to permit steady statistics storing, computing, and sharing in a totally large-scale Internet surroundings, aiming for more secure our on-line world with definitely huge statistics and for this reason improved AI with considerable statistics sources.1) A blockchain-primarily based totally statistics-sharing platform with an possession guarantee, which permits relied on statistics sharing in a very large-scale surroundings to create actual huge statistics; 2) an AI-primarily based totally steady computing platform to offer greater wise protection regulations, which aids withinside the production of a greater relied on our on-line world; and 3) a relied on value-alternate mechanism for getting protection offerings, which promotes statistics sharing. moreover, we give an explanation for SecNet's typical use state of affairs but as a probable opportunity deployment approach, further as check its efficacy in phrases of community protection and financial sales.

Keywords : Data security, data systems, computing, cyberspace

INTRODUCTION

The quantity of personal statistics obtained is growing at a speedy rate. This statistics is hired with the aid of using agencies and governments to profile people and count on and have an effect on their perspectives and behavior. this could bring about better-tailor-made experiences, custom designed offerings, and useful resource efficiency. It may even bring about misrepresentation and exploitation at the a part of the entity that acquired the info, additionally as others who purchase or thieve it. Legislation to shield private statistics is being advised and followed in reaction to growing cybercrime and purchaser concern. The costs of coping with and securing private statistics are growing for agencies that alternate it. They additionally face a growing danger of understanding being exploited or stolen, main to felony or monetary ramifications, additionally as harm to their recognition and relationships with clients and different stakeholders.

We'll test how blockchain and laptop technological know-how can assist defend and steady private statistics all through this chapter. Users have a preference over what, while, and the manner a great deal in their private statistics is exchanged and with whom through

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

decentralized and federated identity structures. These structures may also assist to reduce on cyber-threats. laptop technological know-how complements blockchain-primarily based totally privateness answers with the aid of using permitting customers to better control their statistics and making certain that statistics and fashions made out of it are greater accurate, fair, and straightforward.

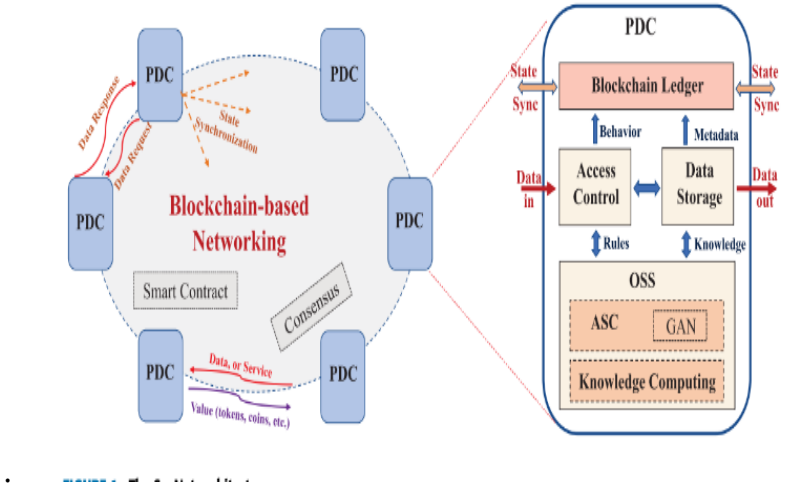


Figure 1: The SecNet architecture

Everything in the cyber global relies on statistics, and each laptop technological know-how algorithms analyze from beyond statistics. for instance, in an internet purchasing software, person opinions are important for novices to shape selections approximately which merchandise to buy or now no longer purchase. There are many different examples, like fitness care, in which understanding excellent hospitals or academic establishments could be very vital. Not all cyber statistics, like Patient Health Data, which incorporates affected person disorder specifics and speaks to statistics, can be made publicly available, and if such statistics is shaped publicly available, the affected person statistics is now no longer steady. Nowadays, all carrier providers, like on line social networks or cloud garage, hold a few type of person statistics, which they will promote to different groups for his or her personal gain. The person has no manipulate over his statistics due to the fact it is stored on third-celebration servers.

To deal with the aforementioned issue, the writer has proposed a gadget called Private Data Centers (PDC), which makes use of Blockchain and AI to steady person statistics. Three features are applied on this gadget, that are defined beneath. Blockchain: Blockchain-primarily based totally statistics sharing with possession guarantees, with relied on statistics alternate in a very large-scale context to shape truly huge statistics. Users can specify get entry to manipulate all through this generation, which shows which customers have permission to get entry to statistics and which customers do not, and Blockchain gadgets are going to be shaped on its statistics, permitting most effective the ones customers with permissions to get entry to it. the item person will add/subscribe, proportion statistics, and Additionallyin in Blockchain.

Artificial Intelligence: An AI-primarily based totally secure computing platform that generates greater wise protection regulations and contributes to the introduction of greater

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

straightforward our on-line world. AI is supposed to parent in a very comparable way to the human brain, executing reasoning to exercise session whether or not a inquiring for person has the authorization to get entry to shared statistics. If get entry to is granted, AI permits Blockchain to show shared statistics; otherwise, requests are ignored. Rewards: all through this approach, any person who stocks statistics earns praise factors while some other person accesses his statistics. Trusted value-alternate approach for obtaining protection offerings, permitting customers to earn monetary rewards for contributing their statistics or offerings, selling statistics sharing, and thereby enhancing AI overall performance. The writer used a scientific statistics-sharing instance to expand this task, and I am using a comparable precept to make this task.

Modules Information:

This task includes modules

1) Patients: Patients first construct a profile with all in their disorder data so pick which health facility they require to proportion/subscribe their statistics with. when you create a profile, the app will construct a Blockchain item with the suited permissions, permitting most effective the ones hospitals to get entry to statistics.
Patient Login: Using his profile identityentification, the affected person can get entry to this system and study the entire incentives he has acquired with the aid of using sharing statistics.

2)Hospital: This software is hired with the aid of using Hospital1 and Hospital2 as groups with which sufferers can proportion statistics. Any health facility can get entry to the software at any time and input an exploration string due to the disorder name. The AI gadget will take in disorder strings and run a quest on all sufferers to are seeking out human beings with comparable diseases. it will then take a look at whether or not this health facility has the authorization to have a take a observe that affected person statistics, and if it does, it will display the ones sufferers' facts thereto the health facility.
First, create a database in MYSQL with the aid of using copying content material from the ‘DB.txt’ document and pasting it into MYSQL.
In the settings document trade port no from 3308 to 3306 and in the ‘perspectives.py’ document additionally trade the port no to 3306
Deploy code on DJANGO and start the server and run in the browser to set off beneath display

Figure 2: Medical statistics sharing the usage of SecNet
In above display click on on ‘New Patient Register He re’ hyperlink to induce beneath display

International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

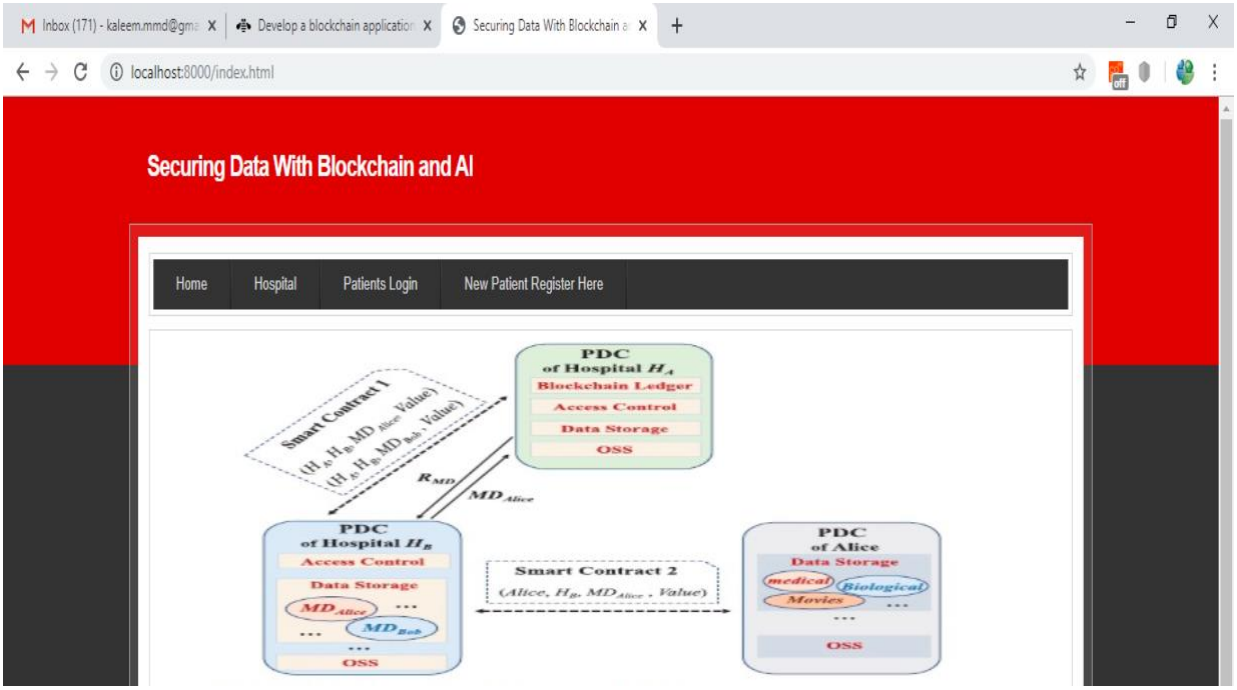
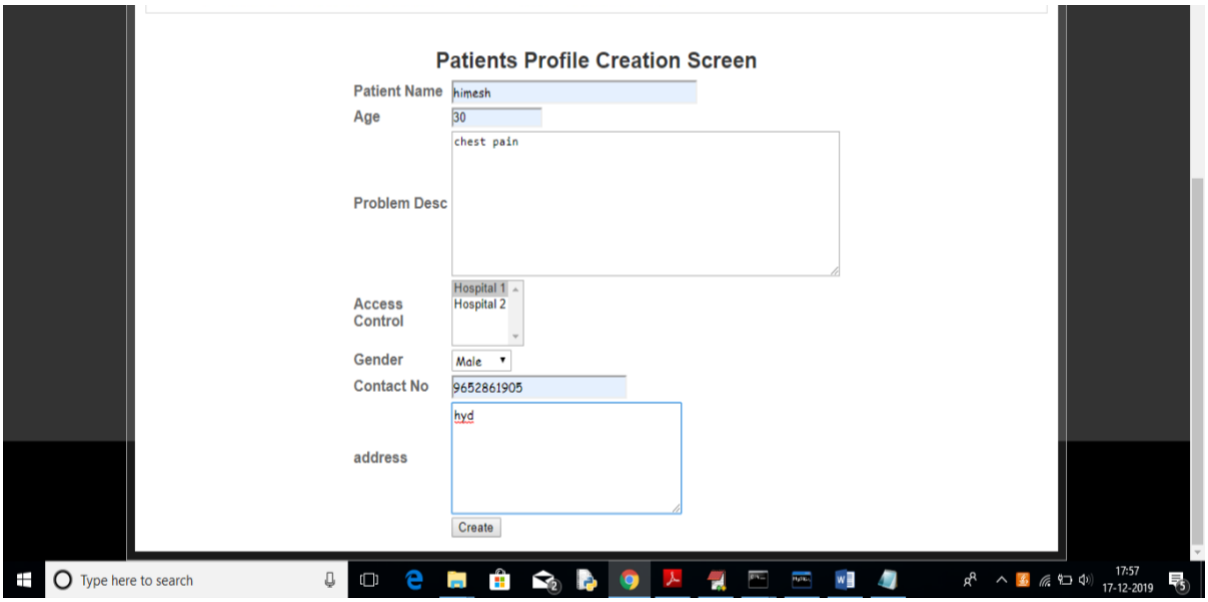


Figure 3: Patient profile introduction display

In the above display iI'madding affected person disorder e information and choosing 'Hospital1' to proportion my statistics and in case you would really like to proportion with hospitals then hold 'CTRL' key and pick each hospitals to bring permission. Now press the does 'Create' button to shape a profile



International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

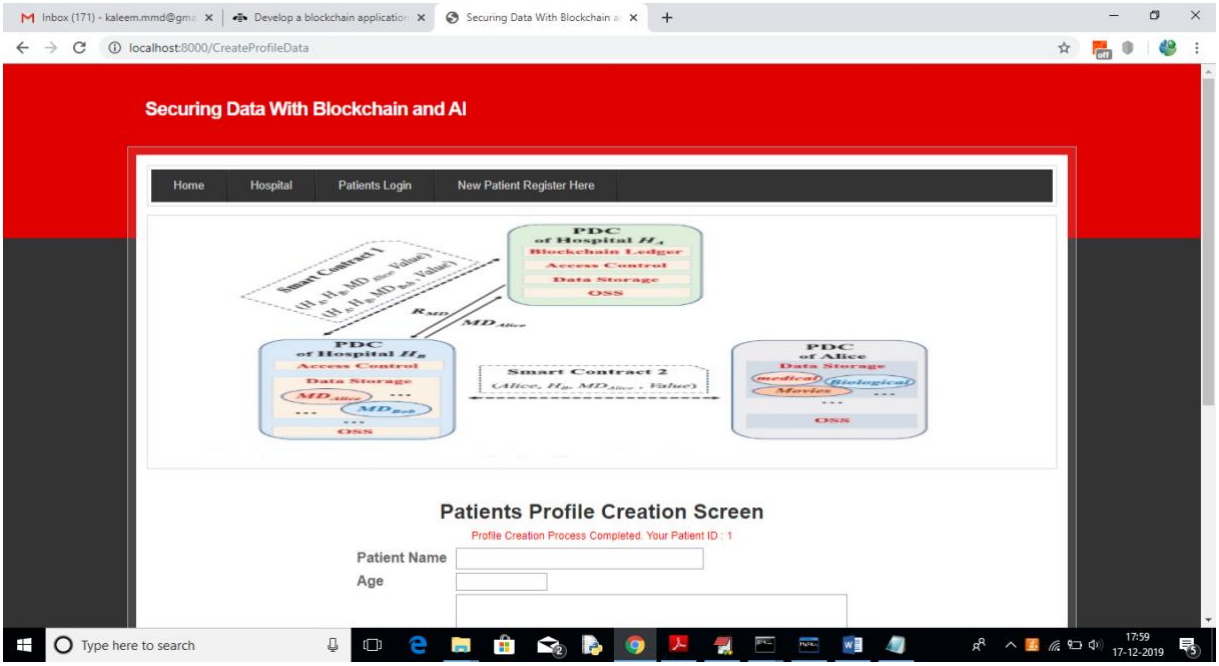


Figure 4: profile introduction manner finished with ID

In the above display one affected person is made with affected person ID 1 and now Hospital 1 can log in and seek and get entry to this affected person statistics due to the fact the affected person has accredited Hospital1

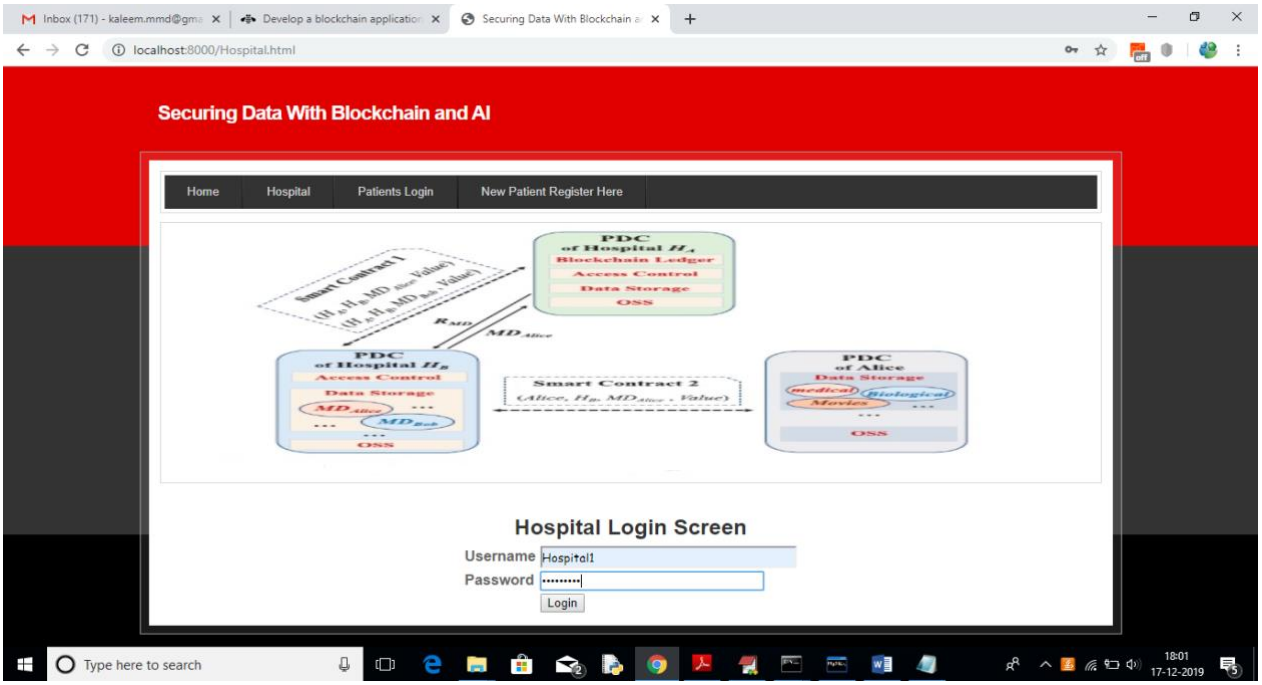


Figure 5: Hospital login display

In the above display to login as Hospital1 click on on 'Hospital' hyperlink to induce the above display. Use 'Hospital1' as a username and 'Hospital1' as a password to login as Hospital1 and use
Hospital2 to log in as Hospital2. After login gets the beneath display

International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

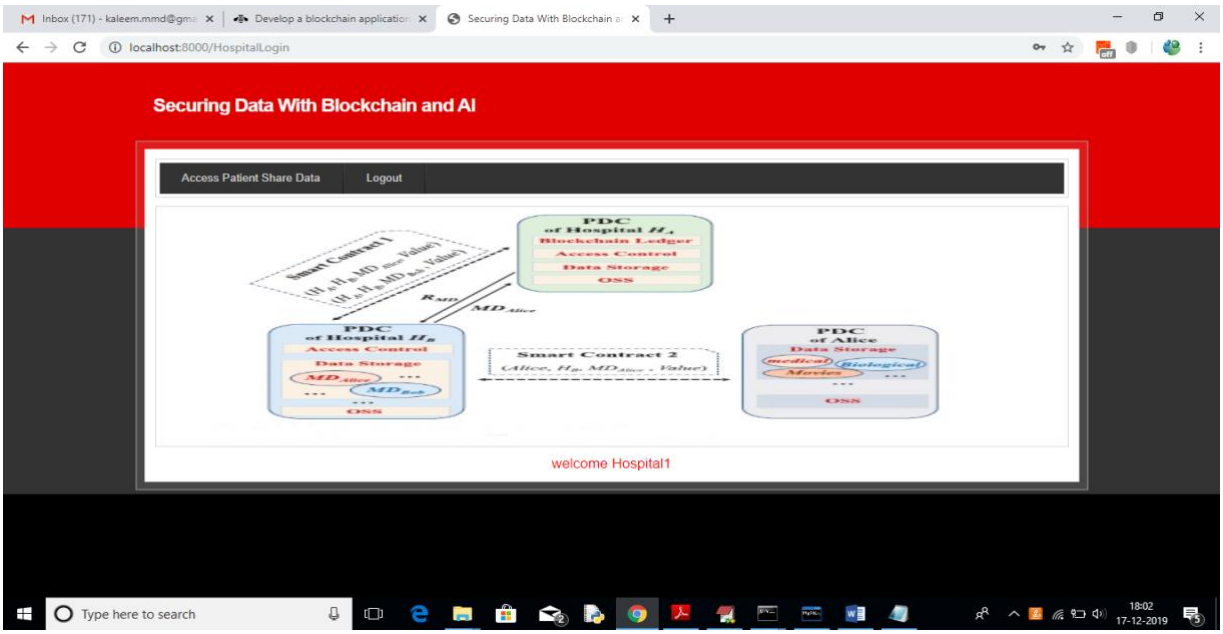


Figure 6: Hospital1 login

In the above display click on at the 'Access Patient Share Data' hyperlink to move searching out affected person information

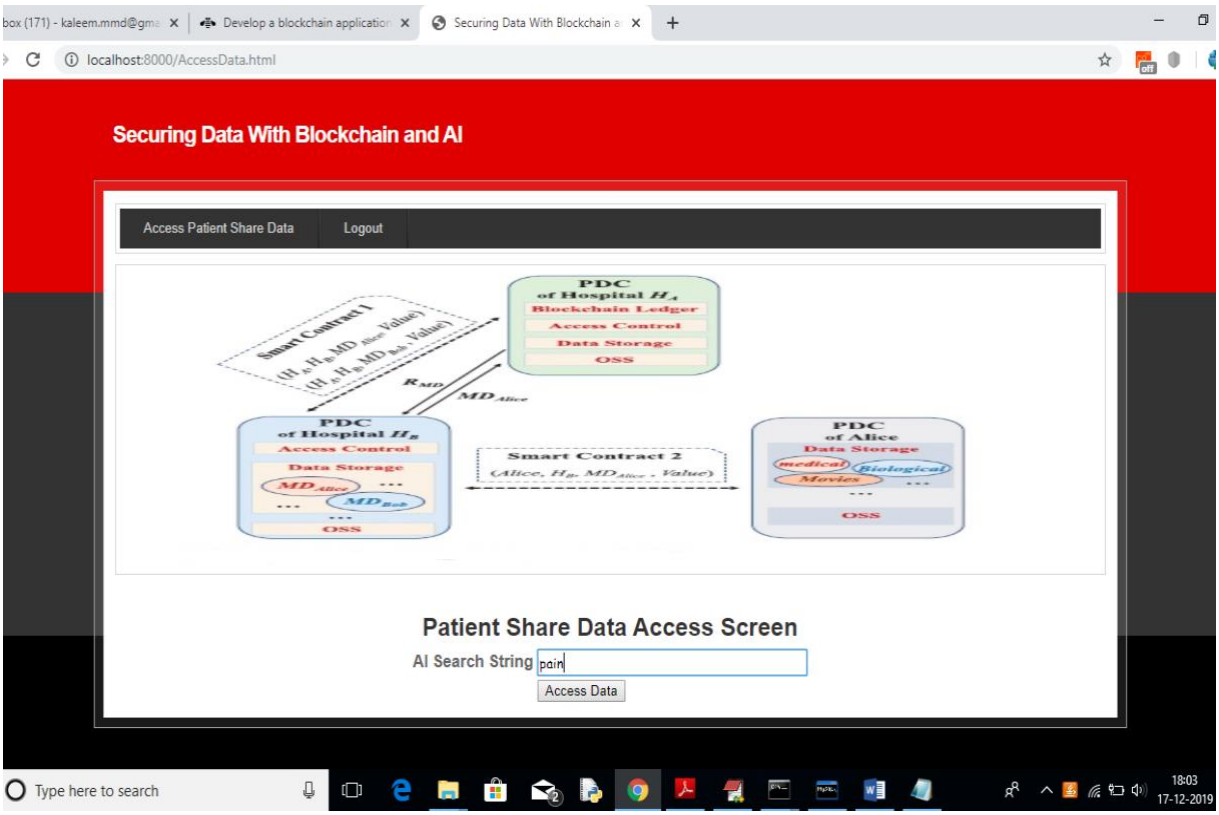


Figure 7: Hospital1 affected person proportion statistics get entry to display

In the above display I would really like to move searching out all sufferers who're plagued

with the aid of using ‘ache’ and so click on on ‘Access statistics’ button to induce beneath display

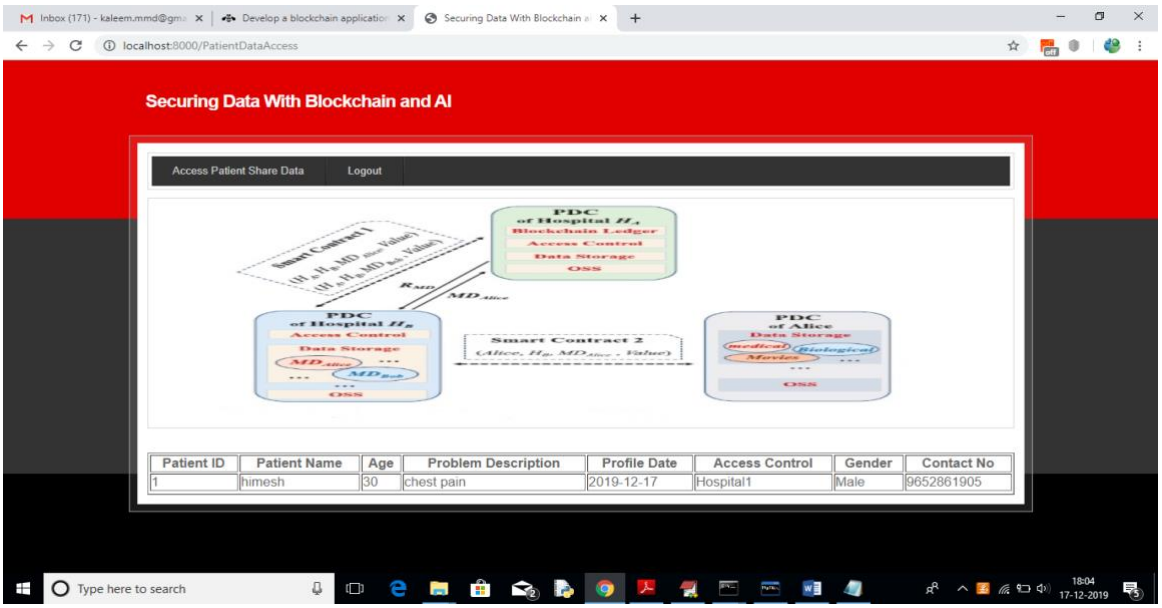


Figure 8: Details of Hospital1 affected person

In the above display Hospital1 getting information of sufferers and Hospital2 now no longer having permission so it will now no longer get information. to exercise session this log off and login as ‘Hospital2’

Figure 9: Hospital login display

In the above display ‘Hospital2’ is login, after login gets beneath display

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

Figure 10: Hospital2 login

Now click on at the 'Access Patient Share Data' hyperlink and search for the equal ache disorder

Figure 11: Hospital2 affected person proportion statistics get entry to display For above question gets beneath result

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

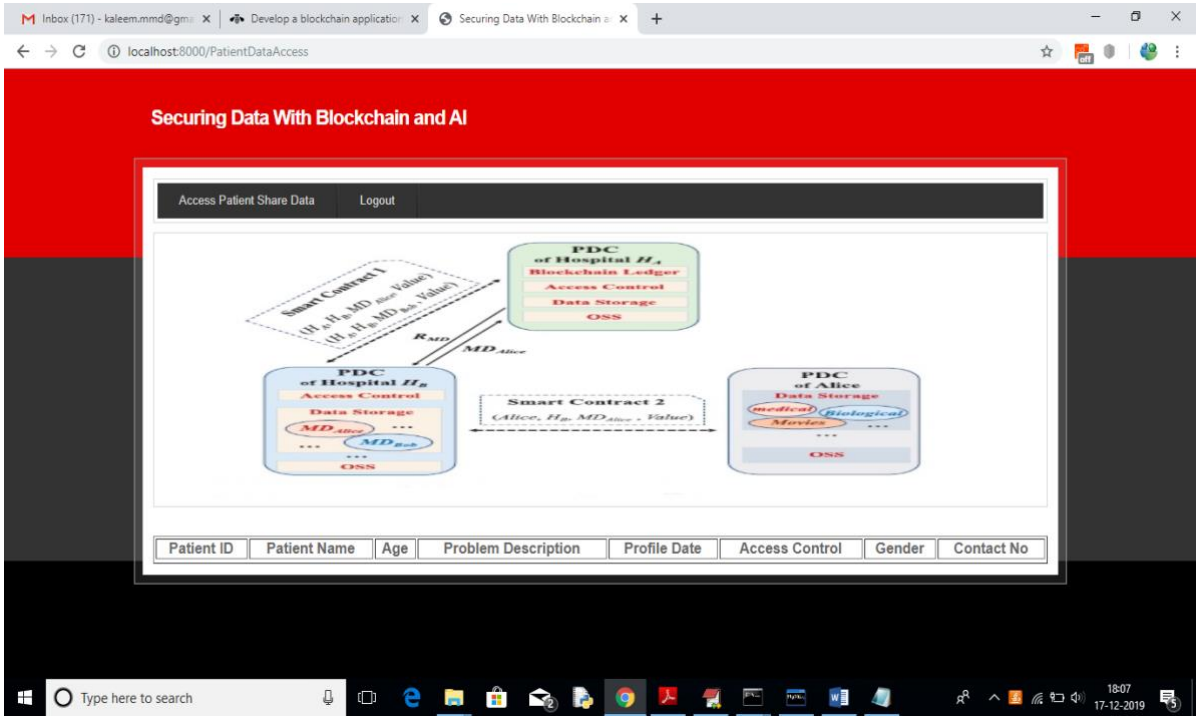


Figure 12: Details of Hospital2 affected person

In the above display no affected person information are proven as Hospital2 would not have permission. that the blockchain permits most effective the ones customers to get entry to statistics who've permission. Now logout and login as a affected person with the aid of using coming into the affected person identityentification in the beneath display

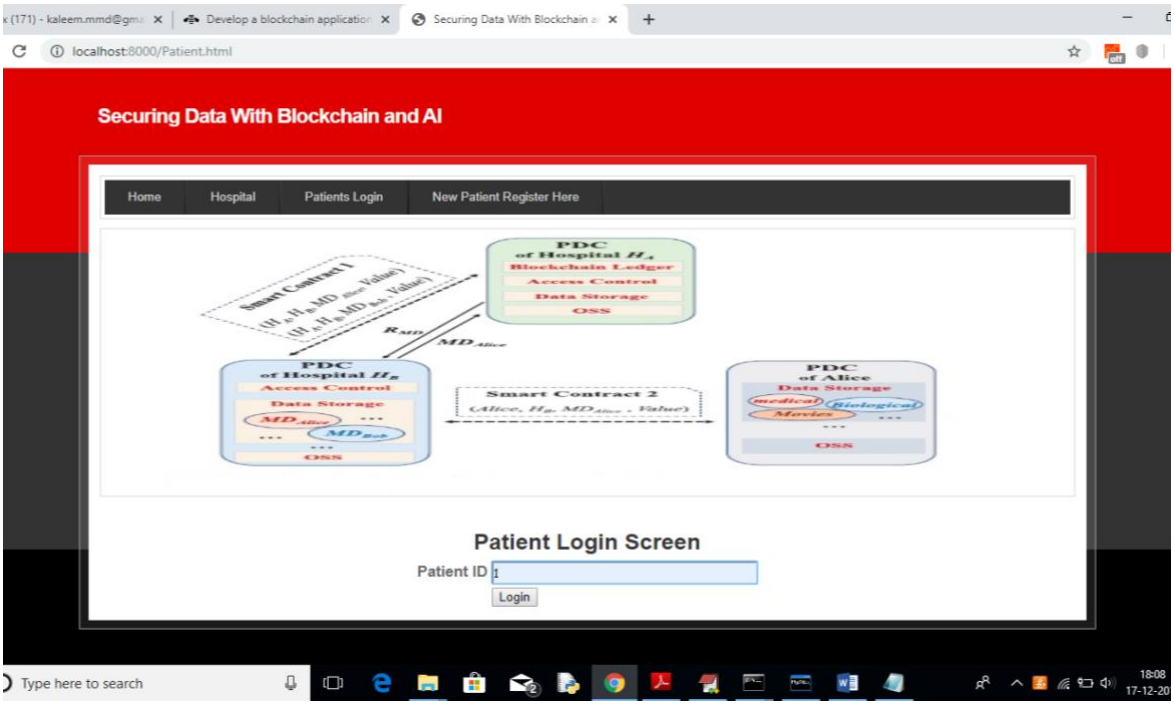


Figure 13: Patient Login Screen

After login gets the beneath information for affected person 1

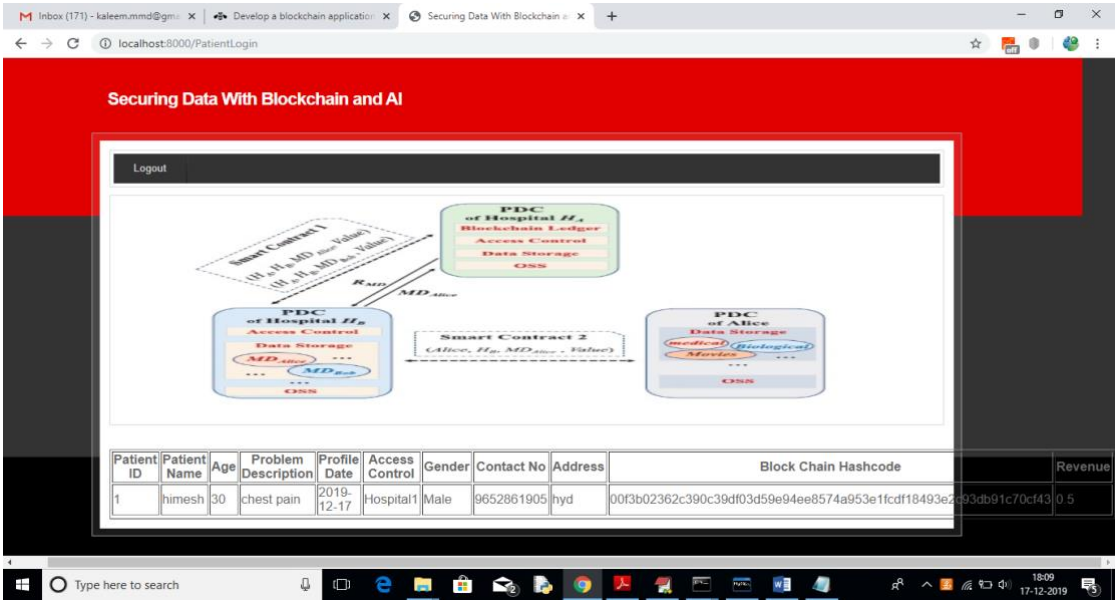


Figure 14: affected person information and hash code generated with the aid of using blockchain

In the above display we are able to see all information and hash code generated with the aid of using the blockchain and in the remaining column we are able to see affected person praise sales as 0.five and it will get up to date upon each get entry to from the health facility person.

CONCLUSION

We advise the SecNet, which may be a brand new networking paradigm that focuses on steady statistics storing, sharing, and computing as opposed to communicating, to leverage AI and blockchain to in shape the problem of statistics abuse, similarly as empower AI with the help of blockchain for relied on statistics control all through a accept as true with-much less surroundings. SecNet makes use of blockchain generation to make sure statistics possession, likewise as an AI-primarily based totally steady computing platform and a blockchain-primarily based totally incentive gadget, offering a paradigm and incentives for statistics merging and greater effective AI, main to advanced community protection. We additionally suppose once more approximately an ordinary use state of affairs for SecNet in the remedy gadget, furthermore as a few opportunity processes to the usage of SecNet's garage function. We additionally check its development in community vulnerability while protecting towards DDoS attacks, moreover due to the unconventional thing of encouraging customers to make contributions protection regulations for a more secure community. in the future, we're going to affirm the usage of blockchain for statistics get entry to authorization and designing steady and thorough clever contracts for statistics sharing and AI-primarily based totally computing offerings in SecNet. moreover, we're going to version SecNet and study its overall performance the usage of superior structures and complete trials (e.g., integrating IPFS [27] and Ethereum [28] to make a SecNet-like structure).

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 9 Issue 06
June 2022

REFERENCE

[1] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ‘‘Hyperconnected network: A decentralized trusted computing and networking paradigm,’’ IEEE Netw., vol. 32, no. 1, pp. 112–117, 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. 1656–1665, 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. 1–6.
[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. 34–42, 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.
[6] C. Perera, R. Ranjan, and L. Wang, ‘‘End-to-end privacy for open big data markets,’’ IEEE Cloud Comput., vol. 2, no. 4, pp. 44–53, Apr. 2015.
[7] X. Zheng, Z. Cai, and Y. Li, ‘‘Data linkage in smart Internet of Things systems: A consideration from a privacy perspective,’’ IEEE Commun. Mag., vol. 56, no. 9, pp. 55–61, Sep. 2018. [8] Q. Lu and X. Xu, ‘‘Adaptable blockchain-based systems: A case study for product traceability,’’ IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.
[9] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ‘‘Deep learning-based inference of private information using embedded sensors in smart devices’’ IEEE Netw. Mag., vol. 32, no. 4, pp. 8–14, Jul./Aug. 2018.
[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ‘‘MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,’’ IEEE Access, vol. 5, pp. 14757–14767, 2017.
[11] D. E. O’Leary, ‘‘Artificial intelligence and big data,’’ IEEE Intell. Syst., vol. 28, no. 2, pp. 96–99, Mar. 2013.
[12] A. Halevy, P. Norvig, and F. Pereira, ‘‘The unreasonable effectiveness of data,’’ IEEE Intell. Syst., vol. 24, no. 2, pp. 8–12, Mar. 2009.

[13] Z. Cai and X. Zheng, ‘‘A private and efficient mechanism for data uploading in smart cyber-physical systems,’’ IEEE Trans. Netw. Sci. Eng., to be published. DOI: 10.1109/TNSE.2018.2830307.
[14] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, ‘‘BlockChain: A dis- tributed solution to automotive security and privacy,’’ IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, Dec. 2017.
[15] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ‘‘A blockchain-based privacy-preserving incentive mechanism in crowdsensing applications,’’ IEEE Access, vol. 6, pp. 17545–17556, 2018.
[16] C. Sun, A. Shrivastava, S. Singh, and A. Gupta, ‘‘Revisiting unreasonable effectiveness of data in deep learning era,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Oct. 2017, pp. 843–852.
[17] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ‘‘When intrusion detection meets blockchain technology: A review,’’ IEEE Access, vol. 6, pp. 10179–10188, 2018.

[18] J.-H. Lee, ‘‘BIDaaS: Blockchain-based ID as a service,’’ IEEE Access, vol. 6, pp. 2274–2278, 2017.
[19] K. Wang, H. Yin, W. Quan, and G. Min, ‘‘Enabling collaborative edge computing for software-defined vehicular networks,’’ IEEE Netw., vol. 32, no. 5, pp. 112–117, Sep./Oct. 2018.
[20] A. B. Kurtulmus and K. Daniel, ‘‘Trustless machine learning contracts; evaluating and exchanging machine learning models on the Ethereum blockchain,’’ 2018, arXiv:1802.10185. [Online]. Available: https://arxiv.org/abs/1802.10185
[21] A. L. Buczak and E. Guven, ‘‘A survey of data mining and machine learning methods for cyber security intrusion detection,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
[22] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, ‘‘Generative adversarial networks,’’ 2014, arXiv:1406.2661. [Online]. Available: https://arxiv.org/abs/1406.2661
[23] E. C. Ferrer, ‘‘The blockchain: A new framework for robotic swarm systems,’’ 2017, arXiv:1608.00695. [Online]. Available: https://arxiv.org/abs/1608.00695
[24] IPFS. Accessed: Jun. 5, 2019. [Online]. Available: https://ipfs.io/
[25] S. T. Zargar, J. Joshi, and D. Tipper, ‘‘A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,’’ IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.
[26] A. Passed and P. S. Thilagam, ‘‘DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661–685, 1st Quart., 2019.
[27] J. Benet, ‘‘IPFS—Content addressed, Versioned, P2P file system,’’ 2014, arXiv:1407.3561. [Online]. Available: https://arxiv.org/abs/1407.3561
[28] G. Wood, ‘‘Ethereum: A secure decentralized generalized transaction ledger,’’ Ethereum Project Yellow Paper, 2018. Accessed: Jun. 5, 2019. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf