Securing Data Over Network with Blockchain and AI

Dr.Arun Kumar Kandru[1], Kolusu Venkata Sai Pavan Babu[2]

[1]Associate Professor, Department of CSE, Malla Reddy Engineering College, Hyderabad, Telangana, India , kandruarun002@gmail.com

[2]PG Student, Department of CSE, Malla Reddy Engineering College, Hyderabad, Telangana, India ,pavanbabukolusu@gmail.com

doi: 10.48047/ecb/2023.12.si4.1003

ABSTRACT

The research proposes a framework called SecNet for ensuring the safety of data over its lifecycle via the Internet at scale. The widespread dispersion of data across digital spaces has rendered authentication and authorization of its usage difficult. The proposed architecture is comprised of three primary elements: In order to generate authentic big data, blockchain-based data exchange with ownership guarantee is necessary. Blockchain technology makes it possible to verify the authenticity of the data and trace it back to its original creator. Data encryption enabled by artificial intelligence: This system has the potential to create a more secure and trustworthy digital ecosystem by developing more nuanced security rules. When used to cyber security, AI has the potential to discover new vulnerabilities and flaws in the system. The effectiveness of AI may be improved if individuals were incentivized to share their data via the establishment of a trustworthy system for exchanging monies in exchange for the supply of a security service. This article compares and contrasts the typical SecNet implementation with some of its alternatives. We also analyze the repercussions on network security and revenue generation. Overcoming the challenges of allowing data interchange through the internet is central to the proposed architecture, which aims to boost AI performance utilizing real-world huge data.

INTRODUCTION

With the advancement of information technology comes a greater emphasis on the integration of cyber, physical, and social (CPS) systems in the direction of a fully integrated information society rather than a digital Internet [1]. In today's digital era, the individual should have full control over the use of their data. Actually, the opposite is true. The importance of data in the modern information culture has motivated big firms to collect as much of it as they can [4, 5]. Multinational companies are gathering an increasing amount of personal data on their customers, including their online behavior, contacts, preferences, and movements, through sensors embedded in their devices (references 6 and 7). Since there is no

failsafe method to monitor data access, data owners have no control over who may see their data. This means that there are inadequate systems in place to track down and penalize those responsible for data theft [8]. When data risks are poorly managed, they may be difficult to deal with [9]. For instance, when a large organization buys individuals' personal data, it loses part of their capacity to appreciate and control the risks involved. More possibility for wrongdoing exists when records cannot be changed.

Artificial intelligence (AI) can manage vast amounts of data, including extensive information, if there is a dependable and efficient method for gathering and consolidating data scattered throughout the entire CPS to create genuine big data, According to reference [11], AI advancements provide significant advantages, including enhanced data security, and enable superior performance in various fields compared to humans. As per [12], research indicates that basic AI systems, such as the perceptron from the 1950s, can outperform modern state-of-the-art technologies. when presented with huge volumes of data on an orders-of-magnitude scale. The issue is communicating securely [13]. Perhaps the blockchain, which employs network-wide consensus mechanisms to provide immutable data exchange and monetary incentives [14, 15], might be beneficial in this regard. As a result, AI might benefit from the secure data exchange provided by blockchain [16].[18]. Data throughput and safety might be improved with the help of AI.

LITERATURE SURVEY

In this piece, we believe that blockchain and AI can work together to build a SecNet Secure Networking architecture that would make networks like the CPS safer for exchanging data and accessing information. Since users must give their data to service providers in order to get access to particular services or apps in the SecNet ecosystem, data storage has emerged as one of the most pressing issues [1, 3]. Since current service systems tightly couple user data with application, this hampers data security and application innovation. The PDS architectures of HyperNet [1] and openPDS [5] served as inspiration. SecNet eventually phased out PDS in favor of PDC, a hardware-based data storage system that offers superior security and intelligence. Users may have faith that SecNet PDCs will keep their data secure. PDC allows users in SecNet to fine-tune how and when their data is shared, as well as get context into how their data is being used. SecNet information storage options extend beyond PDC.

Due to the absence of trust among data stakeholders, the accessibility of data for utilization in AI training and analysis is reduced, hindering the transfer of Internet data. Even if trust is hard to come by in today's environment, Distributing trustworthy information via blockchain technology is efficient, low-cost, and easy. Because of the exposure to fresh Internet sources, this may help AI make better decisions. To prevent unauthorized access to user information and ensure the safe movement of data in trustless environments, SecNet employs blockchain

technology. Multi-model collaboration in edge computing may increase the effectiveness of edge network systems [19]. Blockchain's unchangeable data structure suggests it might be used for reliable financial dealings.

So, in order for SecNet to provide blockchain-based data sharing with ownership guarantees, every piece of shareable content must first be registered in the DRB(Data Recording Blockchain). Access by anybody other than the data owner must be logged and validated using this chain. When it comes to data, only DRB can provide assurances of precision and thoroughness. SecNet enables automated and tamper-proof value exchange via the use of smart contracts embedded in data, providing financial incentives for enterprises to share data or offer security services. SecNet encrypts private data and facilitates CPS exchange.

In order to be successful, AI algorithms need be well-connected and integrated with one another [11]. Businesses that have potential conflicts of interest might benefit from sharing data with one another. Artificial Intelligence(AI) can efficiently analyze vast amounts of data using secure data sharing through blockchain-based smart contracts [20]. This can lead to time-saving, risk reduction, and more accurate forecast and decision-making assistance for security policies that a PDC should adopt, provided there is enough data available. Artificial Intelligence(AI) can continually learn patterns from either real-world data or simulated data created by GAN [22] thanks to the incorporation of Machine Learning [21]. SecNet is considering integrating state-of-the-art AI technologies like these into its Operation Support System in order to detect anomalous behavior involving data that has so far eluded detection. (OSS). SecNet may leverage swarm intelligence to improve data security by linking several intelligent agents across the CPS with trustworthy token exchange methods.

The built-in sensors of devices controlled by large corporations are discreetly collecting various personal information including location data, web browsing behavior, user interactions, and preferences. Since there is no failsafe method to monitor data access, data owners have no control over who may see their data. This means that there are inadequate systems in place to track down and penalize those responsible for data theft [8]. As a result, it is difficult to manage data risks without adequate data management expertise.

Data is the lifeblood of every AI system. New users of shopping applications often rely on the feedback of established users. When applying to schools, use your background in medicine to your advantage. Once shared, a patient's medical records, which may contain their contact information and health history, are no longer confidential.

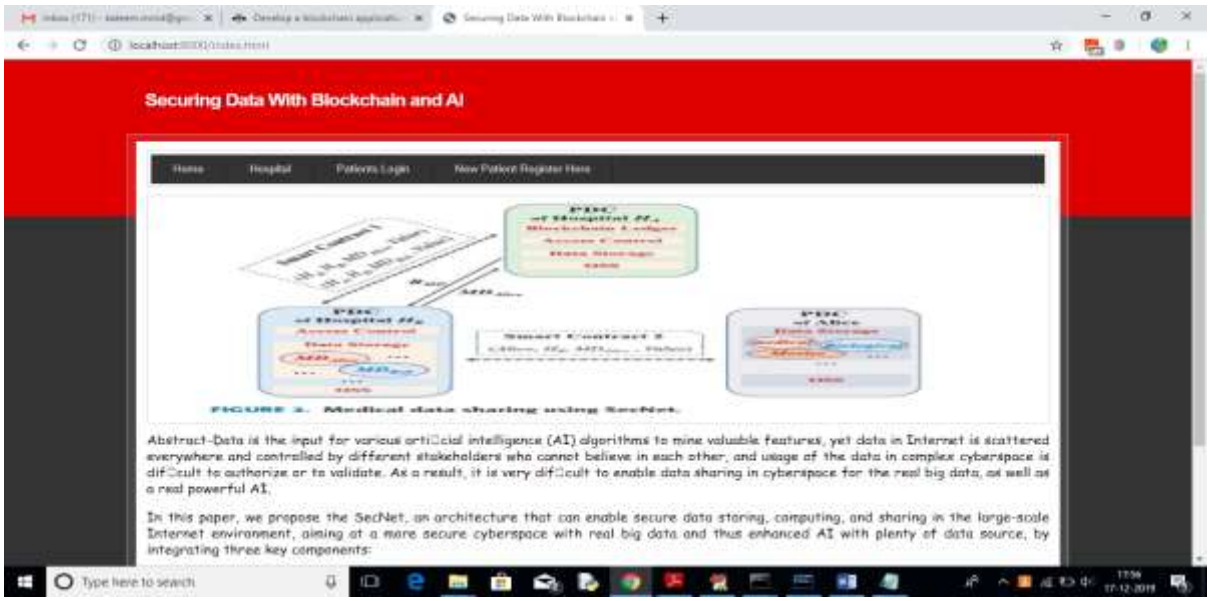
Users don't have much control over their data since it's usually stored on third-party servers and then sold to marketers and advertising. The author suggests a private data center (PDC) that uses Blockchain and AI to ensure user privacy. This strategy makes use of the following three skills.

True big data is only conceivable thanks to blockchain-based DLT, which guarantees data ownership and allows secure data transmission at scale. Users may design Blockchain objects with permissions that allow access only to the appropriate parties. Blockchain enables people to add/subscribe to items in order to expedite data distribution and authorization.

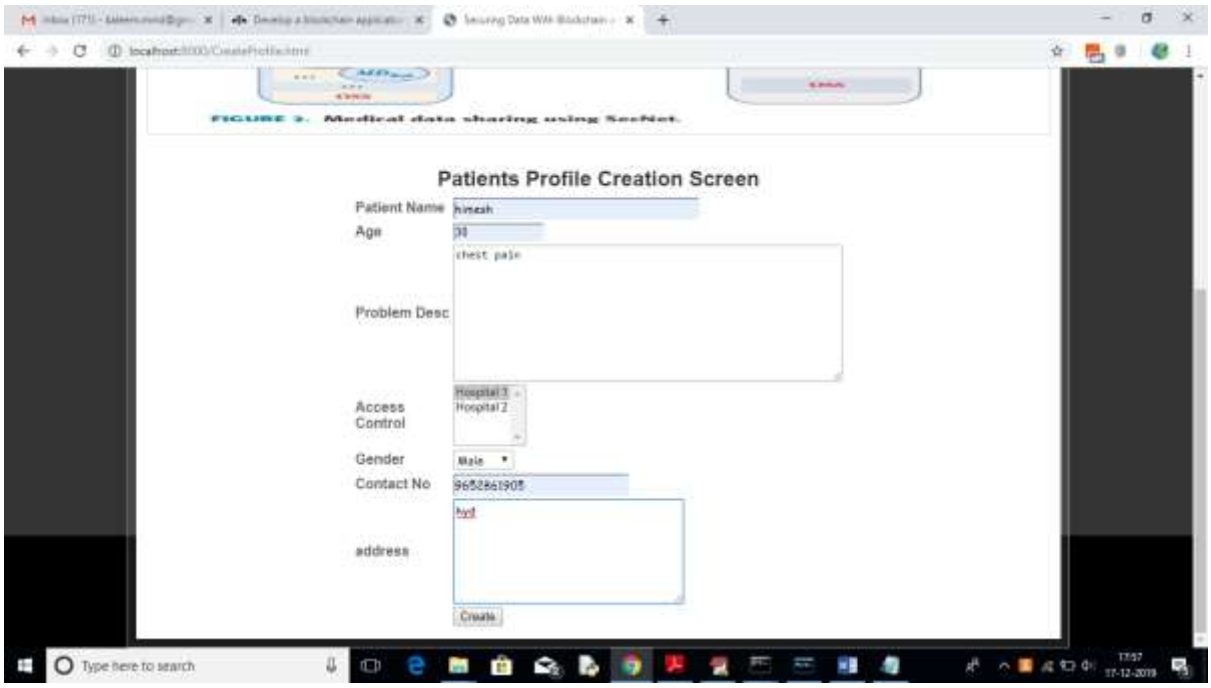
Secure computing solutions powered by AI might help improve users' faith in cyberspace. Artificial intelligence, like the human brain, uses reasoning to affirm a user's request with the barest minimum of information. If the data is available, the AI will add it to the Blockchain; otherwise, it will be disregarded.The system guarantees that individuals who offer their data are remunerated whenever it is utilized by third parties. An impenetrable value exchange for safe services that not only pays people for their data but also makes AI more effective.

Private data centers, the blockchain, and artificial intelligence all work together to keep customer data secure. It's a hat trick! 1) Blockchain, an immutable distributed ledger. By granting each user access to his data, the user decides who may see what. The blockchain object will produce features like one user giving another user read-only access. 2) AI: an AI-based secure computing platform that refines existing security concepts to provide a safer and more trustworthy online environment. The cognitive processes of AI will resemble that of humans. Data access is restricted until authorized users request it. Access to private information requires authentication. At long last, users get paid for letting other parties access their data. The act of teaching others is rewarded. The efficiency of AI is enhanced when data is shared across systems. Strengthens security for user data. The data is within the user's control, but is invisible to anybody else.

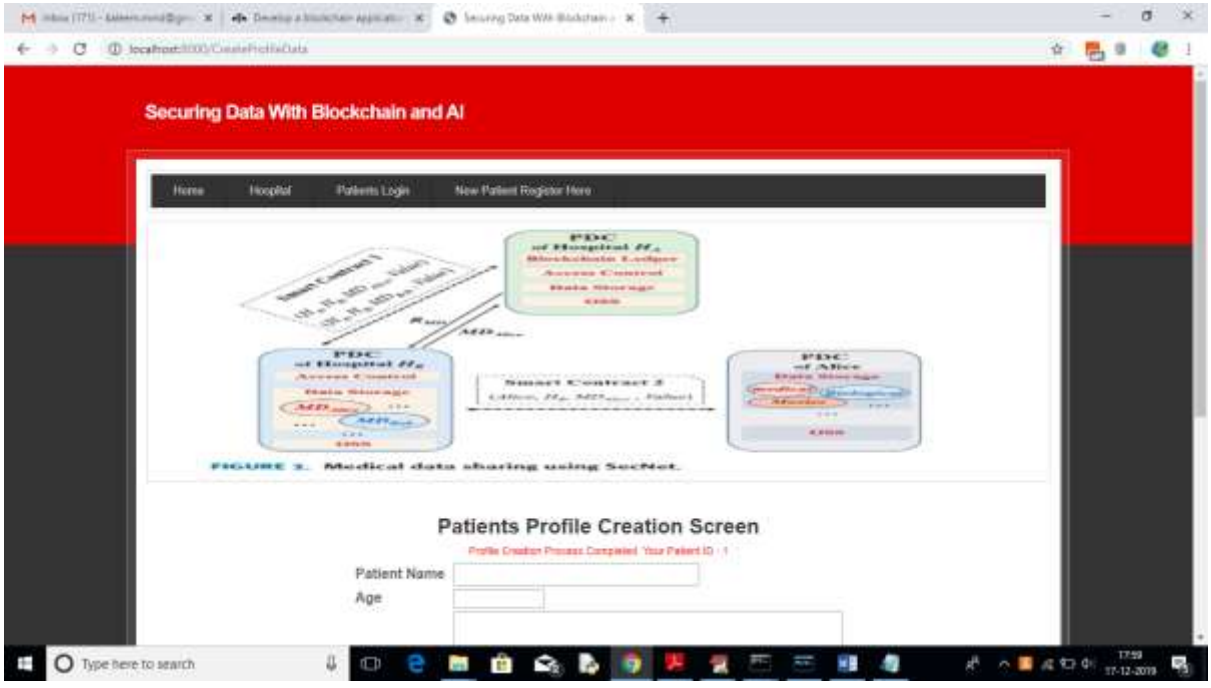
PROPOSED SYSTEM



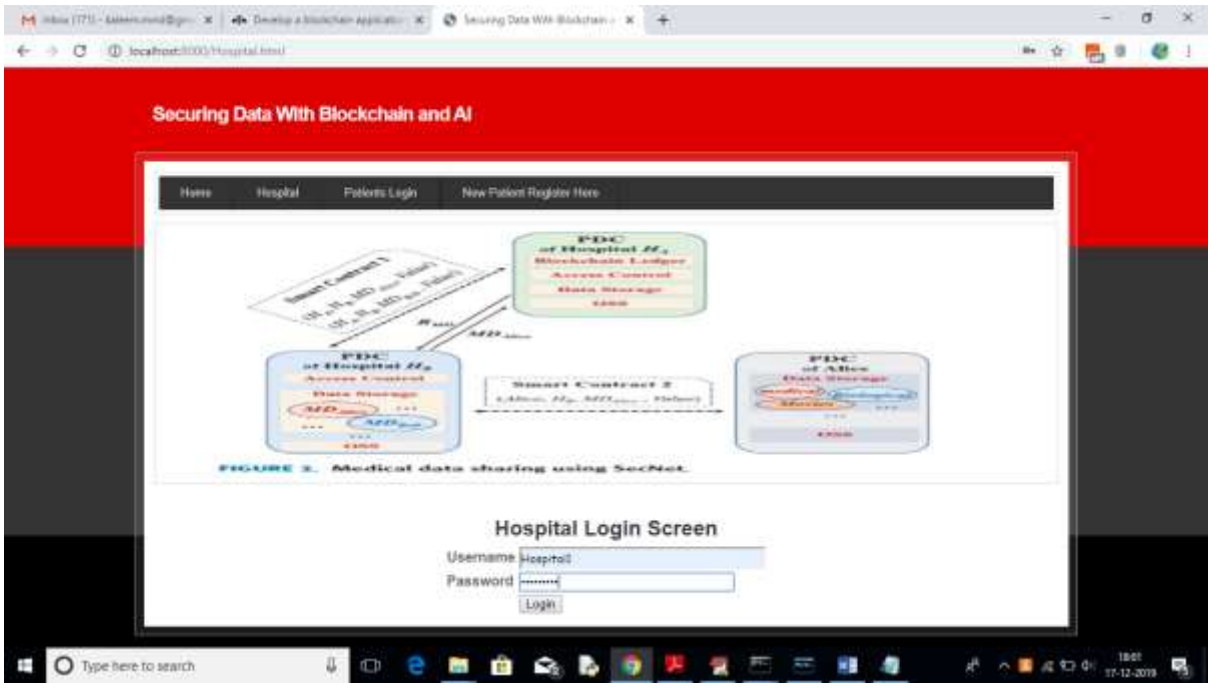
To access the screen displayed below, please click on the 'New Patient Register Here' hyperlink located on the previously mentioned screen.



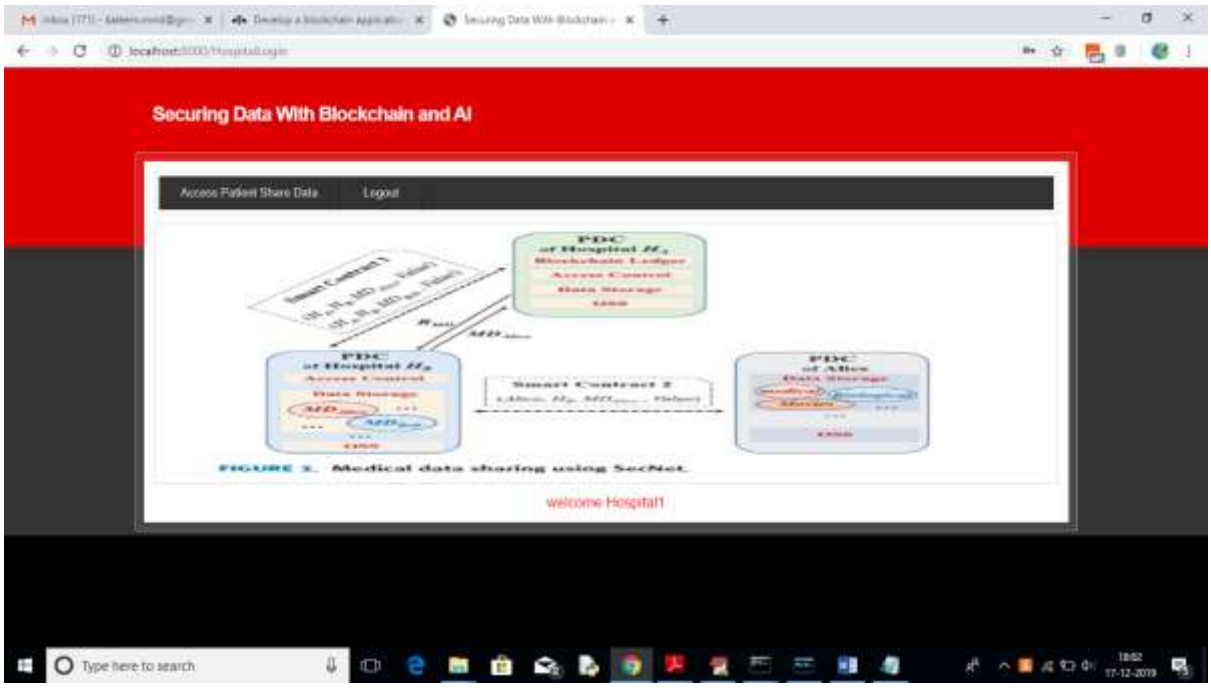
I've decided to have "Hospital1" be the final destination and will fill in the patient's illness specifics on the subsequent page. To provide permission to two separate hospitals, press and hold CTRL while clicking their names. To create a new account, click the "Create" button.



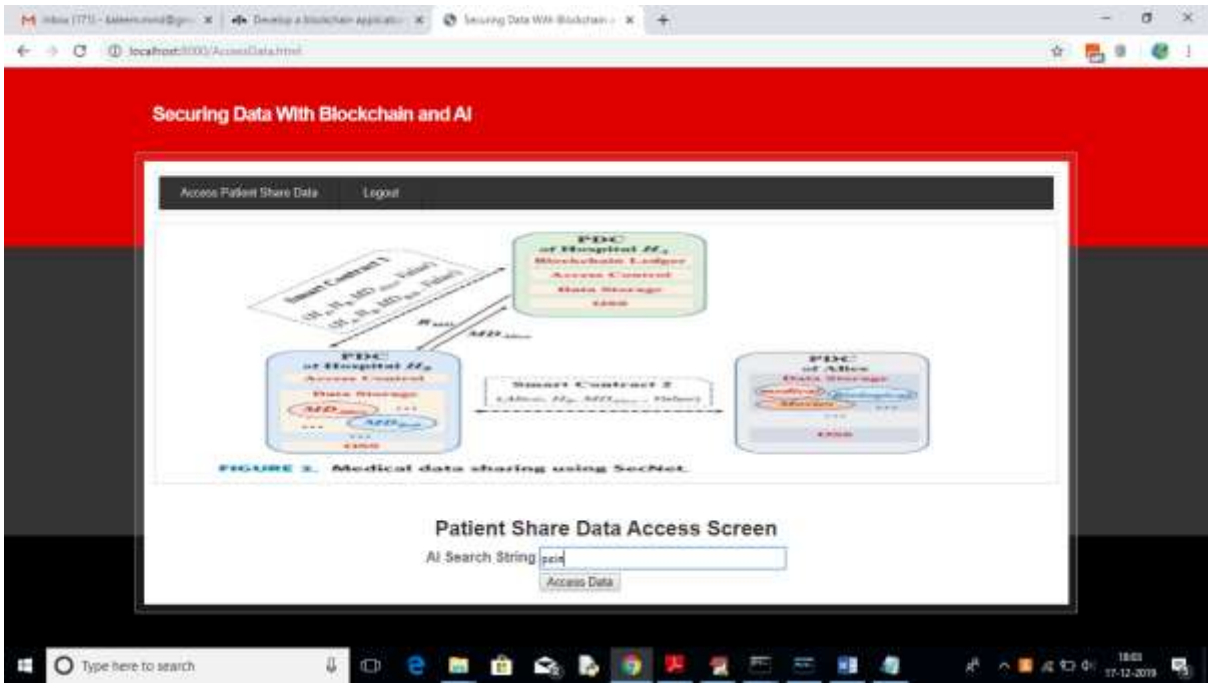
On the page before this one, a single patient with the patient ID 1 is generated. Because the patient consented, Hospital 1 is allowed to log in, look for, and investigate the data associated with this patient.



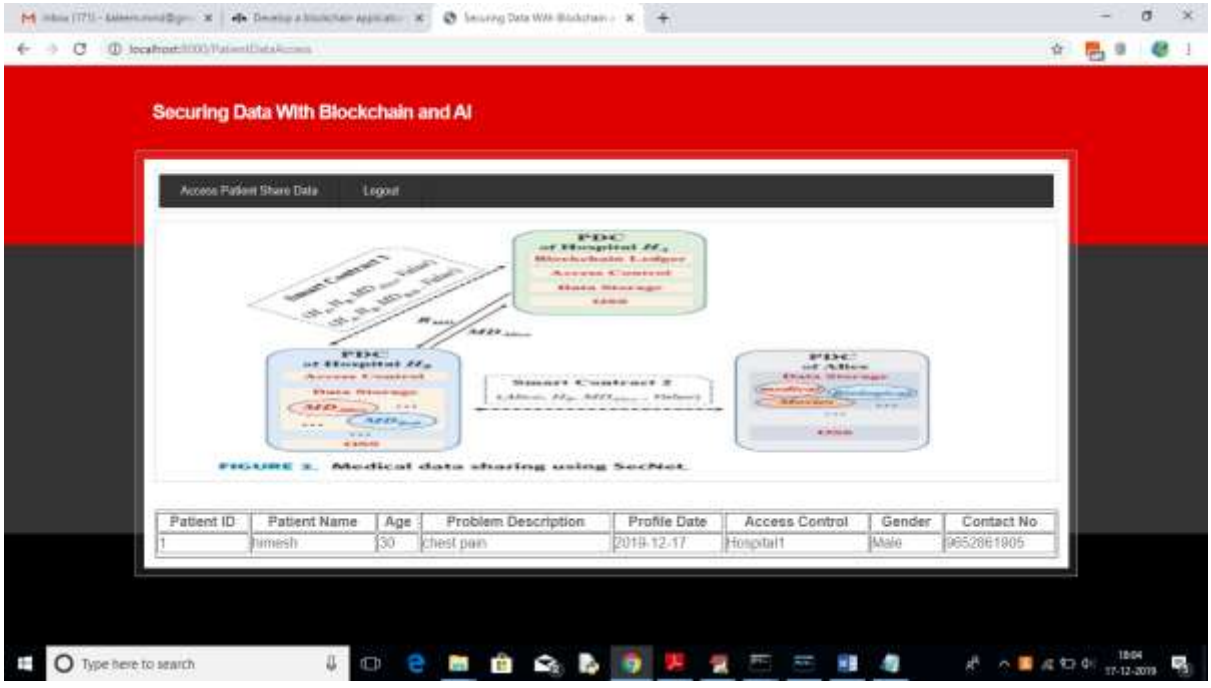
To return to the previous screen as Hospital1, choose the 'Hospital' link on the one that is now shown. You may log in as Hospital1 with the login "Hospital1" and password "Hospital1," and as Hospital2 with the username "Hospital2." You'll see the screen below after signing in.



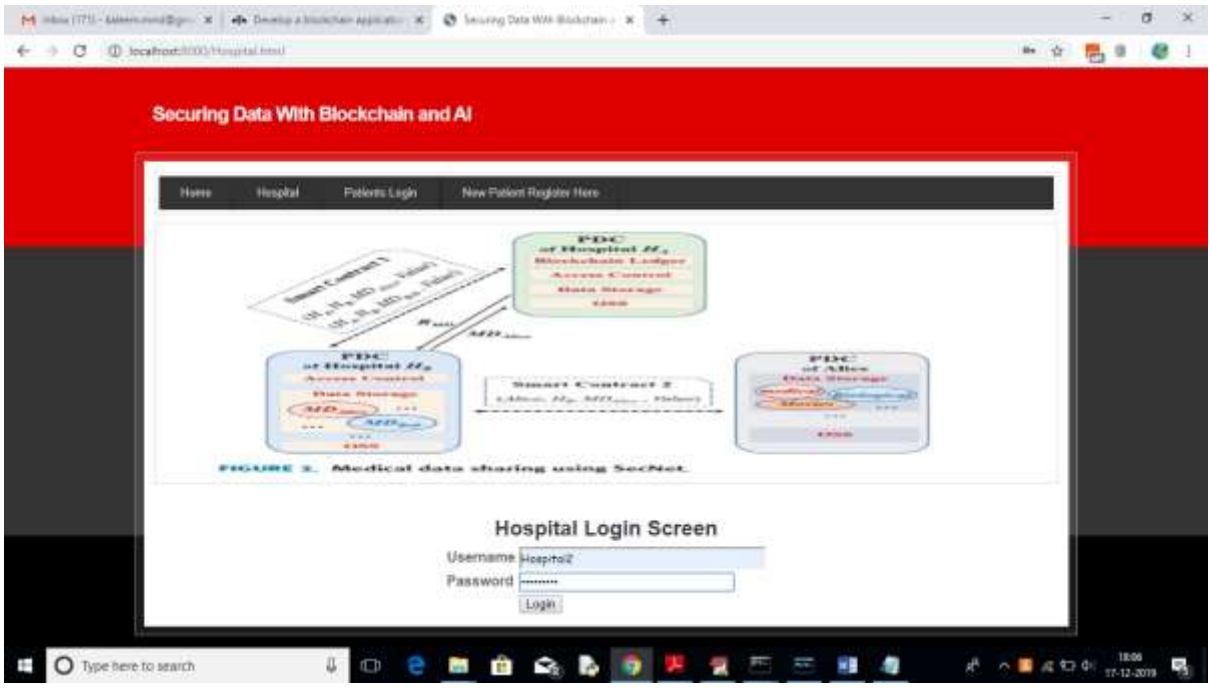
To search for patient details, click on the link labeled 'Access Patient Share Data' on the screen above.



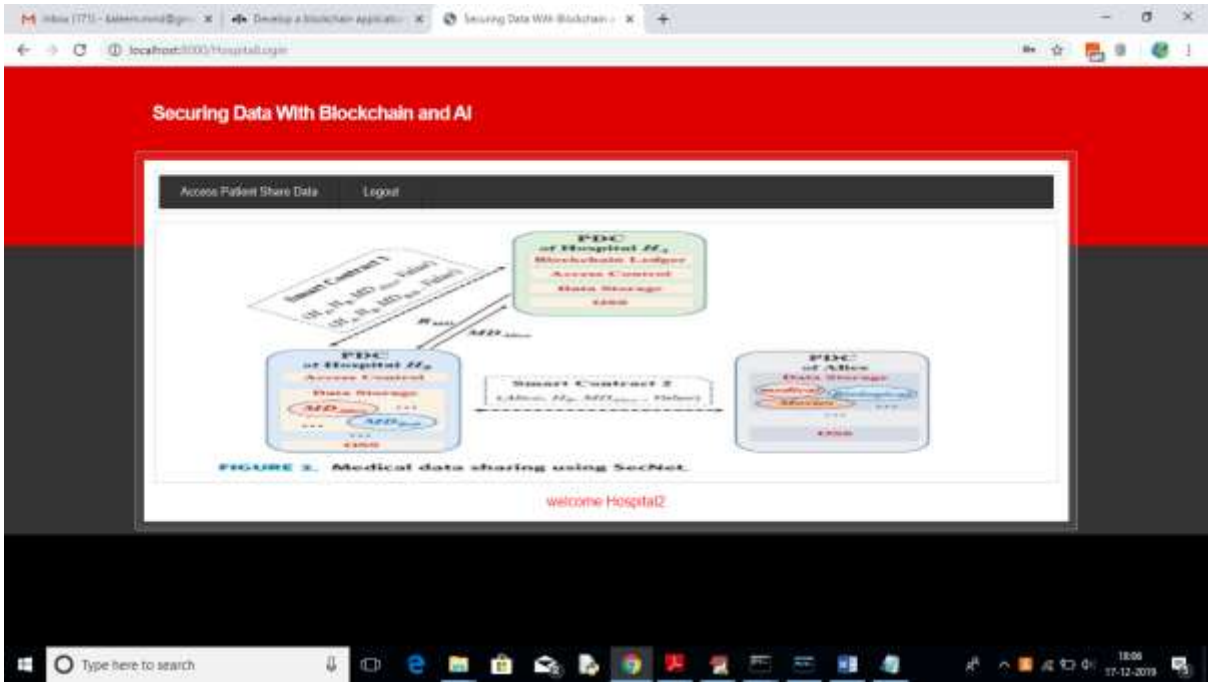
I aim to conduct a search on the screen above to retrieve information regarding patients experiencing 'pain'. Subsequently, I intend to select the 'Access data' button to view the screen below.



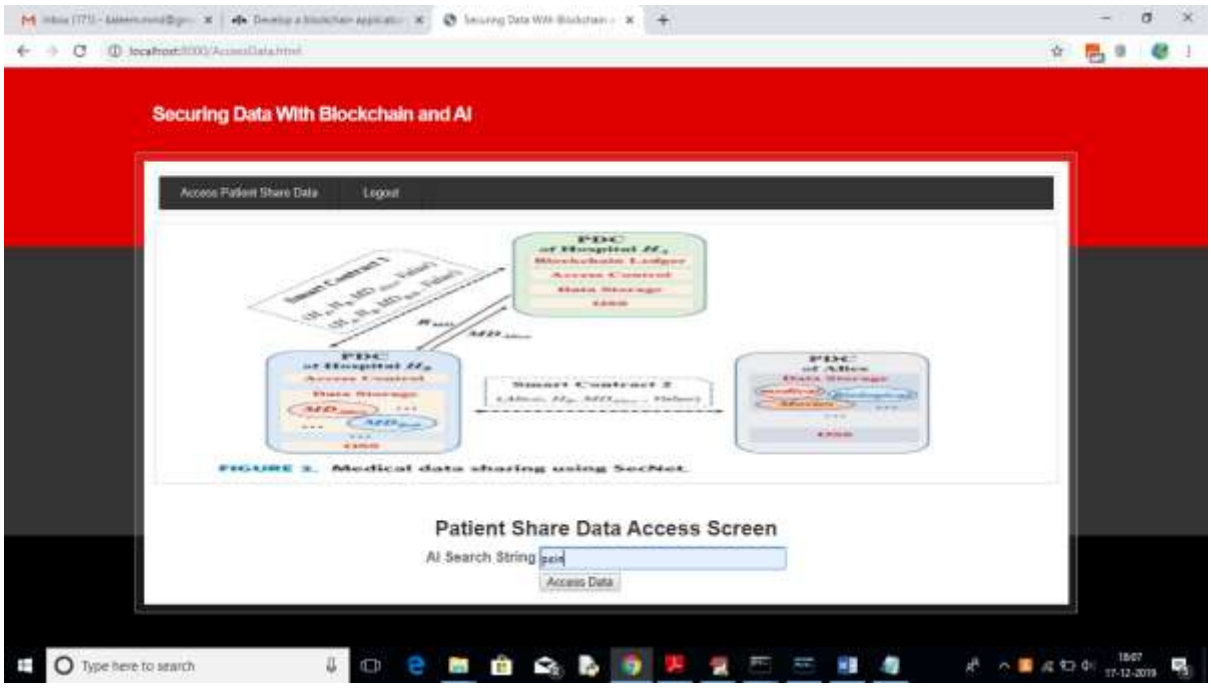
The hospital named "Hospital1" is able to access patient details on the screen while "Hospital2" does not have the necessary permissions to view the information. To verify this, kindly log out and log back in as "Hospital2".



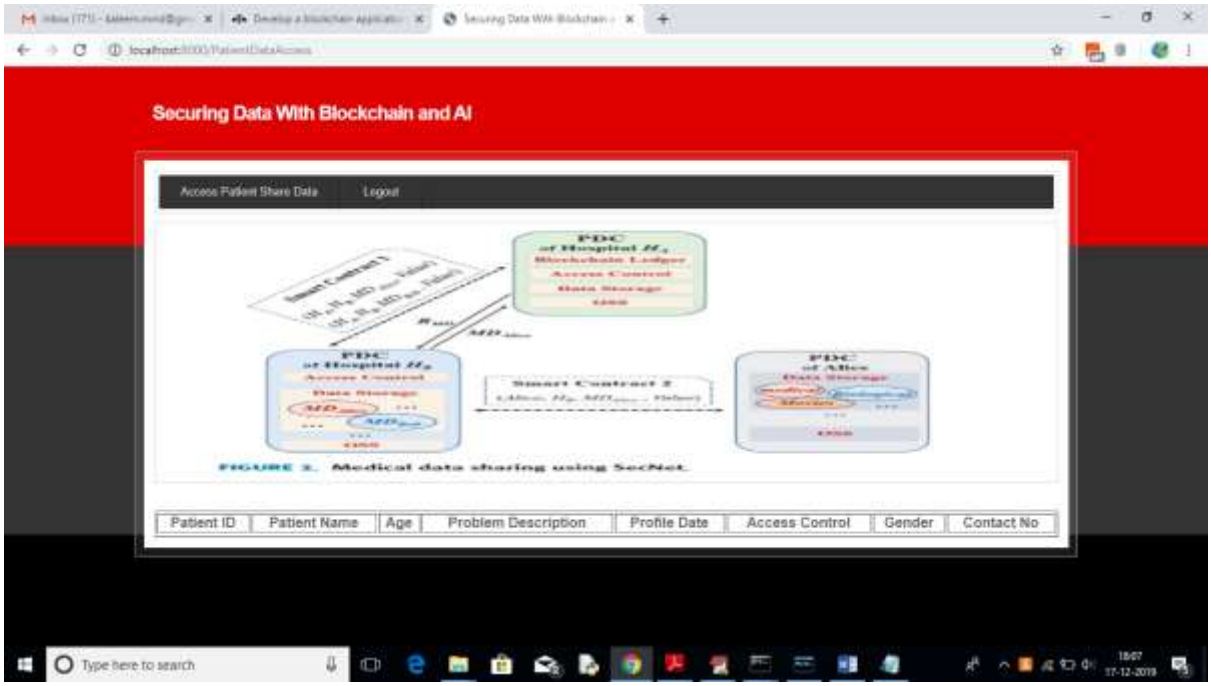
In above screen 'Hospital2' is login, after login will get below screen



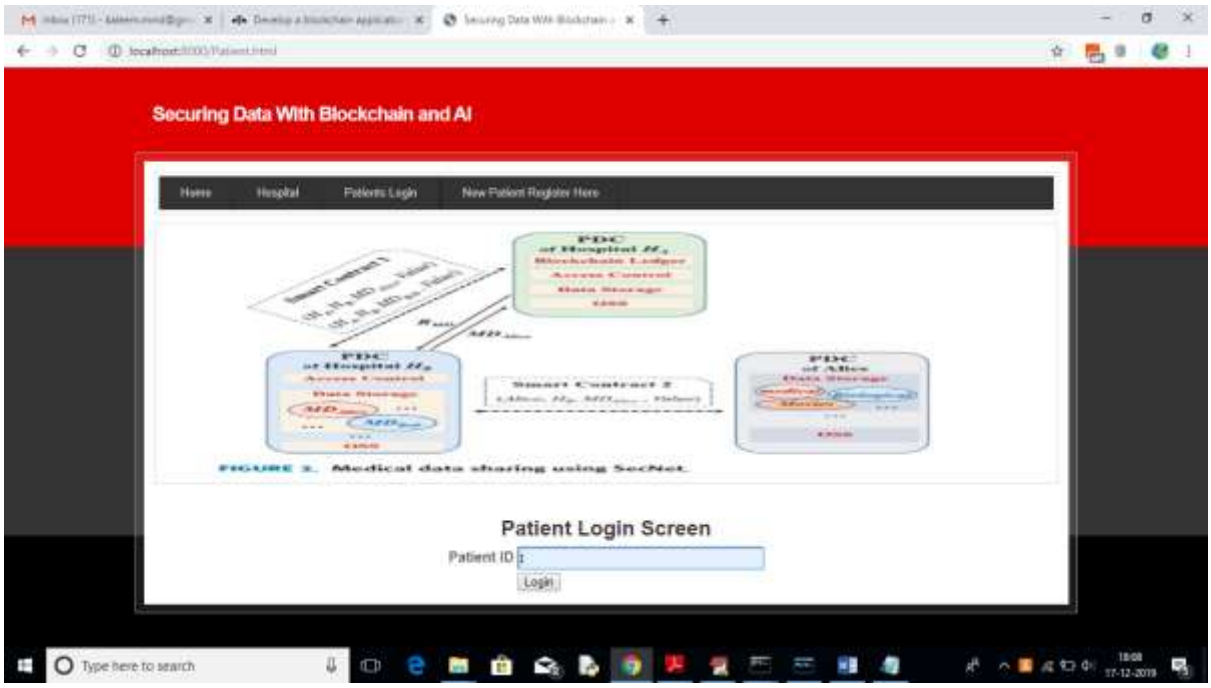
Now click on 'Access Patient Share Data' link and search for same pain disease



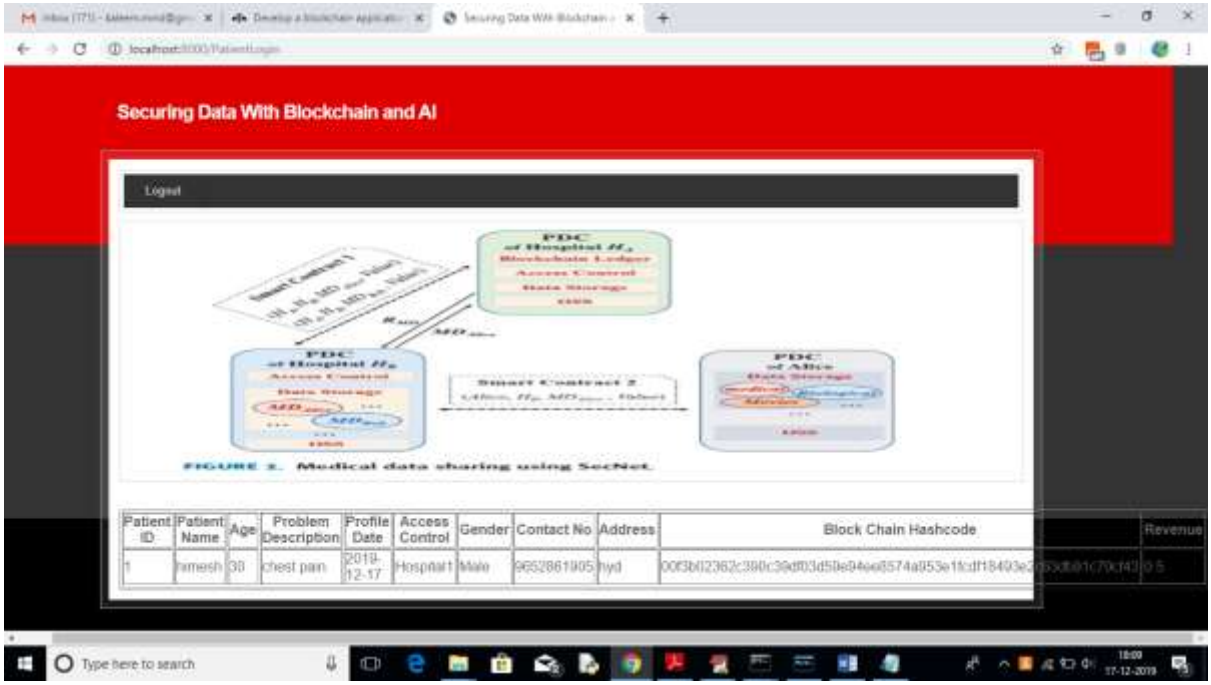
For above query will get below result



Hospital2 cannot access patient data. Thus, authorized users may see block chain data. Logout and then log in as a patient by providing the patient id.



After login will get below details for patient 1



The patient's entire information, including the blockchain hash code, is shown in the preceding pane. The supplemental revenue from patient awards is shown in the final column at a rate of $0.5 per new hospital user.

CONCLUSION

We introduces a novel networking approach named SecNet, which focuses on data storage, sharing, and processing as opposed to transmission. This design aims

to prevent data exploitation while facilitating trustworthy data management for AI in a trust-less society. Furthermore, SecNet is supported by blockchain technology. Blockchain technology is utilized to validate data ownership, AI is employed to offer a secure computing platform, and a blockchain-based incentive system is established to incentivize data consolidation and the development of more powerful AI in order to increase network security. We also describe a typical SecNet deployment in healthcare systems and provide ideas for how its storage capabilities might be effectively used. We also assess its efficacy in stopping DDoS assaults and investigate its novel approach to inviting users to suggest security rules for a safer network.

REFERENCES

[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. 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.

[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. 4453, 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. 5561, 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. 2127, 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. 814, 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. 1475714767, 2017.

[11] D. E. O'Leary, ``Articial intelligence and big data," IEEE Intell. Syst., vol. 28, no. 2, pp. 9699, Mar. 2013.

[12] A. Halevy, P. Norvig, and F. Pereira, ``The unreasonable effectiveness of data,"

IEEE Intell. Syst., vol. 24, no. 2, pp. 812, Mar. 2009.

[13] Z. Cai and X. Zheng, ``A private and efcient mechanism for data upload- ing 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. 119125, 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. 1754517556, 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. 843852.

[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. 1017910188, 2018.

[18] J.-H. Lee, ``BIDaaS: Blockchain based ID as a service," IEEE Access, vol. 6, pp. 22742278, 2017.

[19] K. Wang, H. Yin, W. Quan, and G. Min, ``Enabling collaborative edge computing for software dened vehicular networks," IEEE Netw., vol. 32, no. 5, pp. 112117, Sep./Oct. 2018.

[20] A. B. Kurtulmus and K. Daniel, ``Trustless machine learning con- tracts; 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. 11531176, 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 net- works," 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) ooding attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 20462069, 4th Quart., 2013.

[26] A. Praseed and P. S. Thilagam, ``DDoS attacks at the application layer: Challenges and research perspectives for safeguardingWeb applications," IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661685, 1st Quart., 2019.

[27] J. Benet, ``IPFSContent addressed, Versioned, P2P le system," 2014,

arXiv:1407.3561. [Online]. Available: https://arxiv.org/abs/1407.3561

[28] G. Wood, ``Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2018. Accessed: Jun. 5, 2019. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf