JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 10, ISSUE 04, 2023

SECURING DATA WITH BLOCK CHAIN AND AI

Putta. Srivani[1], Ch. Rakshitha[2], S. Navaneetha[2], K. Srujana[2], M. Priyanka[2]

[1]Professor, [2]UG Scholar, [1,2]Department of CSE-Cyber Security

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

Abstract

Data is the input for various artificial intelligence (AI) algorithms to mine valuable features, yet data in Internet is scattered everywhere and controlled by different stakeholders who cannot believe in each other, and usage of the data in complex cyberspace is difficult to authorize or to validate. As a result, it is very difficult to enable data sharing in cyberspace for the real big data, as well as a real powerful AI, by integrating three key components: 1) blockchain-based data sharing with ownership guarantee, which enables trusted data sharing in the large-scale environment to form real big data; 2) AI-based secure computing platform to produce more intelligent security rules, which helps to construct a more trusted cyberspace; 3) 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.

Keywords: Securing data, Block chain, AI.

1. INTRODUCTION

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. In such an information society, data is the asset of its owner, and its usage should be under the full control of its owner, although this is not the common case. Given data is undoubtedly the oil of the information society, almost every big company want to collect data as much as possible, for their future competitiveness. An increasing amount of personal data, including location information, web-searching behavior, 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. Moreover, the usage of those data is out of control of their owners, since currently there is not a reliable way to record how the data is used and by who, and thus has little methods to trace or punish the violators who abuse those data. That is, lack of ability to effectively manage data makes it very difficult for an individual to control the potential risks associated with the collected data. For example, once the data has been collected by a third party (e.g., a big company), the lack of access to this data hinders an individual to understand or manage the risks related to the collected data from him. Meanwhile, the lack of immutable recording for the usage of data increases the risks to abuse them. If there is an efficient and trusted way to collect and merge the data scattered across the whole CPS to form real big data, the performance of artificial intelligence (AI) will be significantly improved since AI can handle massive amount of data including huge information at the same time, which would bring in great benefits (e.g., achieving enhanced security for data) and even makes AI gaining the ability to exceed human capabilities in more areas. According to the research in, if given large amount of data in an orders of magnitude more scale, even the simplest AI algorithm currently (e.g., perceptrons from the 1950s) can achieve fanciest performance to beat many state-of-the-art technologies today. The key lies in how to make data sharing trusted and secured. Fortunately, the blockchain technologies may be the promising way to achieve this goal, via consensus mechanisms throughout the network to guarantee data sharing in a tamper-proof way embedded with economic incentives. Thus, AI can be further empowered by

blockchain-protected data sharing. As a result, enhanced AI can provide better performance and security for data.

2. LITERATURE REVIEW

S. Yu states that due to rapid pace of technology and the introduction of Internet of Things or IoT, there has been a swift increase in the number of intelligent devices being connected to the internet. These devices are capable of generating a large amount of data due to the fact that it is connected and is interacting with the internet. A large number of devices generate equally large amount of data which cannot be processed efficiently. Therefore, the authors propose an effective technique based on blockchain that can provide a low-cost alternative to create economic value for the IoT data generated. A major drawback of this methodology is that it has the potential to be misused by uploading large amounts of malicious data.

R. Wang elaborates on the foundation of network security construction which is the PKI or The Public Key Infrastructure. The researchers also commented on the reliability and the robust security offered by the blockchain platform. Therefore, the authors amalgamated both the methodologies to strengthen the Public Key Infrastructure by a permissioned blockchain that converts the PKI into a privacy-aware PKI. This is crucial as the implementation of a permissioned blockchain also improves the efficiency of the configuration and certificate application. The major drawback is that this technique has been a very specialized approach towards the blockchain paradigm.

C. Ehmke explains that the innovative paradigm of Blockchain has been popular and has seen extensive usage recently. The blockchain was utilized for financial applications and that is how it gained immense popularity and limelight. The blockchain was readily picked up by a plethora of researchers and implemented in various different fields, which has greatly helped in bringing increased security to numerous applications. Due to the fact that the blockchain paradigm requires a user of the blockchain to download the whole chain to gain an overview. To ameliorate this effect, the authors have implemented a scalable and lightweight blockchain protocol.

R. Wang introduces the video surveillance system as an irreplaceable tool that can be used to efficiently manage and survey big cities. When a video surveillance system is installed it can easily transmit environment information remotely, this is highly useful as the person does not need to travel long distances and physically be present in the location for the management. Due to a large-scale increase in the monitoring standards with the inclusion of IoT and realtime monitoring, it is susceptible to attacks. Therefore, the authors developed a system for video surveillance based on permissioned blockchains and Convolutional Neural Networks for a seamless and secure system. A Major drawback in the system is that large scale testing of the System has not been performed and will be done in the upcoming researches.

J. Lou states that there has been a lack of a key management feature in the Named Data Networking, which is utilized to name each and every object by the producer and also digitally sign it. There are some disadvantages of the conventional approach such as lack of trust between the sites as well as the high chances of failure observed in the centralized architecture if the main node fails. Therefore, the authors in this paper propose an efficient key management scheme based on blockchain for the Named Data Networking paradigm. The blockchain increases the trust between the sites as well as the decentralized architecture is highly useful in overcoming failure. The drawback of the proposed scheme is that it has not been evaluated extensively for its feasibility in reducing the NDN cache pollution.

S. Wang explains that there has been a very fast development of cryptocurrency in recent years, which has led to detailed scrutiny of the paradigm. This has uncovered a lot of irregularities in the

ISSN- 2394-5125 VOL 10, ISSUE 04, 2023

paradigm such as the Smart Contracts that have been the cause of "The DOA Attack" which has resulted in a huge loss. Therefore, the authors have presented a comprehensive and systematic review of the smart contracts in the blockchain paradigm. The authors have presented a six-layer architecture for smart contracts for increasing the security of the system. The authors have not implemented a formal verification which can provide confidence.

Y. Xu introduces the concept of decentralized storage that is based on the blockchain framework. The blockchain is one of the most innovative concepts that can be used to design a highly secure decentralized framework. The authors have proposed section blockchain protocol, which aims to eliminate the storage problem that is encountered in certain devices. The proposed methodology is highly resilient to failure due to the decentralized architecture, as well as, it has the ability to withstand heavy loads and optimization gracefully due to the implementation of the Blockchain paradigm.

M. Marchesi in his keynote speech details the rapid development and ongoing researches going on in the field of blockchain. This is due to the increased attention to this paradigm and increased demand in this sector. The author indicates that this increased pressure on a nascent framework has led to an increase in security lapses that are evident in the various different incidents on the Ethereum platform and the cryptocurrency exchanges.

A. Maksutov elaborates on the paradigm of Blockchain and its uses. The authors have proposed an innovative concept for the detection and identification of various money laundering schemes that use the blockchain framework for their nefarious activities. The proposed methodology has been used to deanonymizing the transactions and tracking the coin join transactions, which allows the authors to evaluate user participation. All of this information is used to determine if the transactions are being fraudulent or used to launder money.

F. Wessling states that the addition of blockchain to existing platforms is problematic as it is different from building the applications from scratch by incorporating the Blockchain into the application. The authors determine the amount of blockchain required for various different implementations, this is done by analyzing the attributes of blockchain such as anonymous, trustless and immutable, etc. The authors have outlined the various different processes that utilize various different elements of the blockchain technology that can be implemented based on the specific application and use case of the application.

J. Wang explains that most of the applications based on crowd sensing gather a huge amount of data by using pervasive smartphone users to provide the data. But most of the time the users are not compensated enough for their contribution to the system. Therefore, the authors have presented an innovative framework for a privacy-preserving reward and penalty scheme that rewards the users for contributing to the large data sensing paradigm using the trustless and secure blockchain. The major drawback of this paper has been that the authors have not discussed the solutions for a possible collusion attack.

S. Pandey introduces the benefits of utilizing the Blockchain paradigm for its security and decentralized architecture. The author states that there has been a jump in the number of researches is going on in this field and there has been increased interest in implementing the blockchain framework to make existing systems resilient and secure. To this effect, the authors have formulated an ingenious and practical simulation tool for planning, stability, and design of the systems and applications as well as networks in a blockchain environment. The BlockSIM is an opensource and comprehensive solution for all the Blockchain simulation needs. The major drawback is that the authors have not modeled the internet latency that would affect the accuracy of the simulation

ISSN- 2394-5125 VOL 10, ISSUE 04, 2023

3. PROPOSED SYSTEM

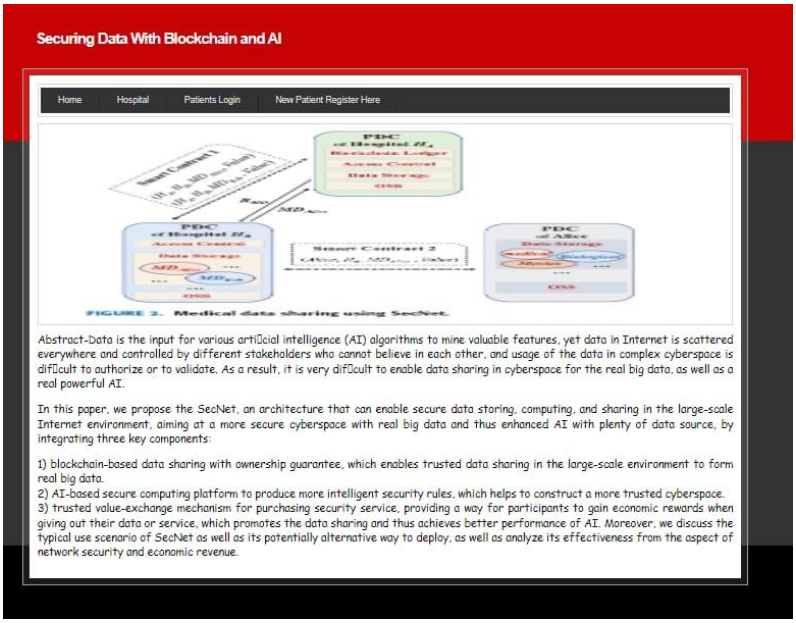
Now a day all service providers such as online social networks or cloud storage will store some type of users' data and they can sale that data to other organization for their own benefits and user has no control on his data as that data is saved on third party servers. To overcome from above issue author has describe concept called Private Data Centers(PDC) with Blockchain and AI technique to provide security to user's data. In this technique 3 functions will work which describe below

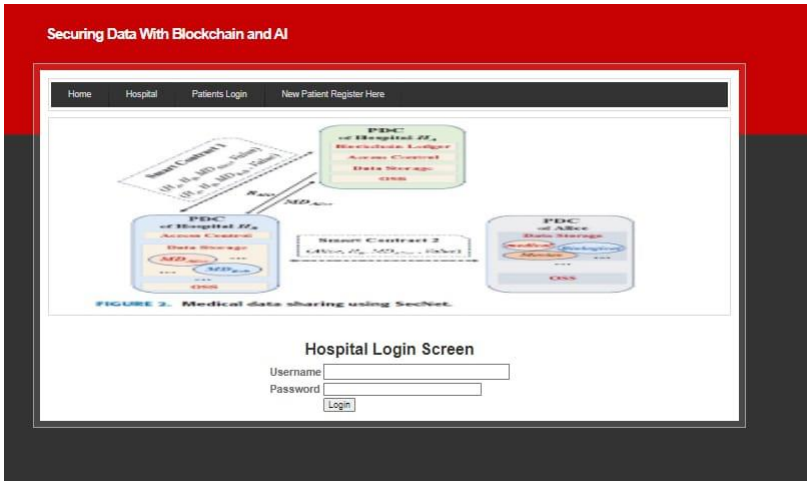
1) Blockchain: Blockchain-based data sharing with ownership guarantee, which enables trusted data sharing in the large-scale environment to form real big data. In this technique users can define access control which means which user has permission to access data and which user cannot access data and 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.

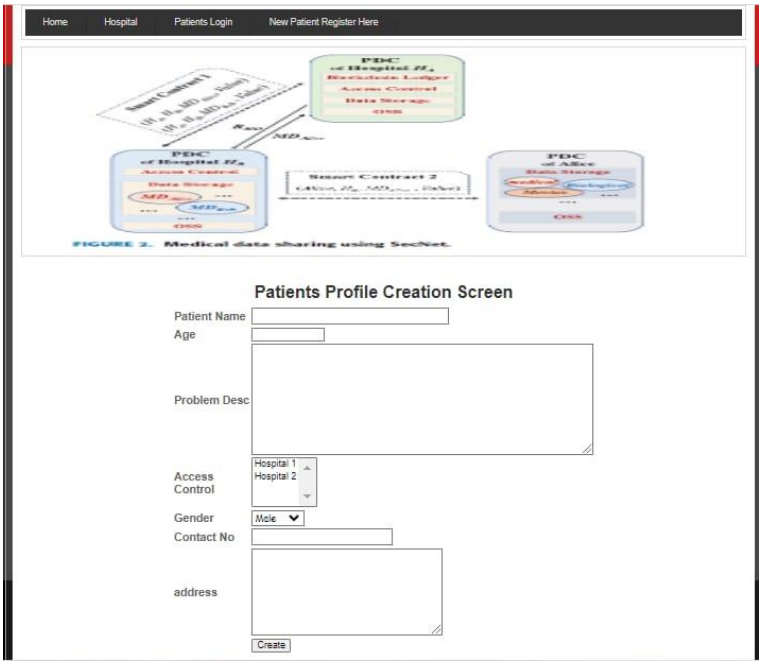
2) Artificial Intelligence: AI-based secure computing platform to produce more intelligent security rules, which helps to construct a more trusted cyberspace. AI work similar to human brain and responsible to execute logic to check whether requesting user has permission to access shared data. If access is available then AI allow Blockchain to display share data otherwise ignore request.

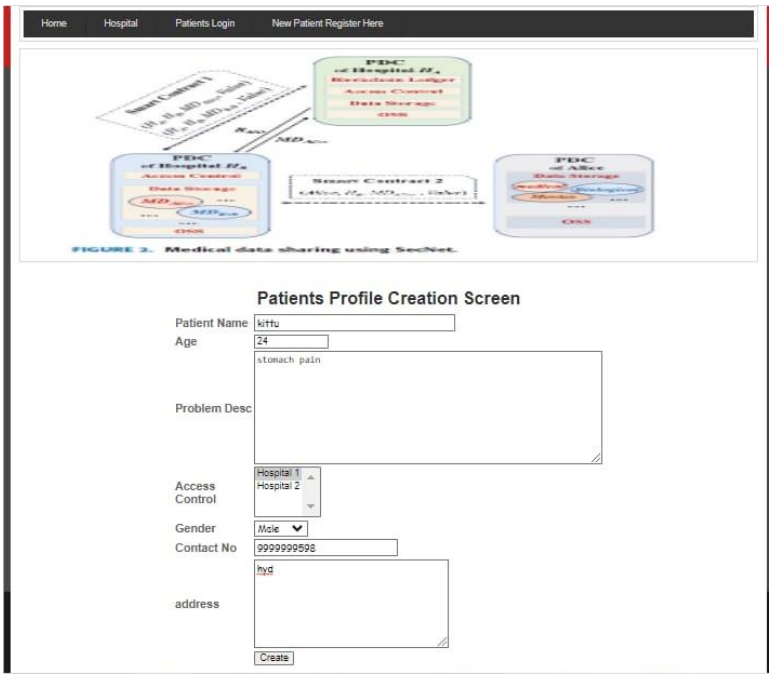
3) Rewards: In this technique all users who is sharing the data will earn rewards point upon any user access his data. trusted value-exchange mechanism for purchasing security service, providing a way for participants to gain economic rewards when giving out their data or service, which promotes the data sharing and thus achieves better performance of AI.

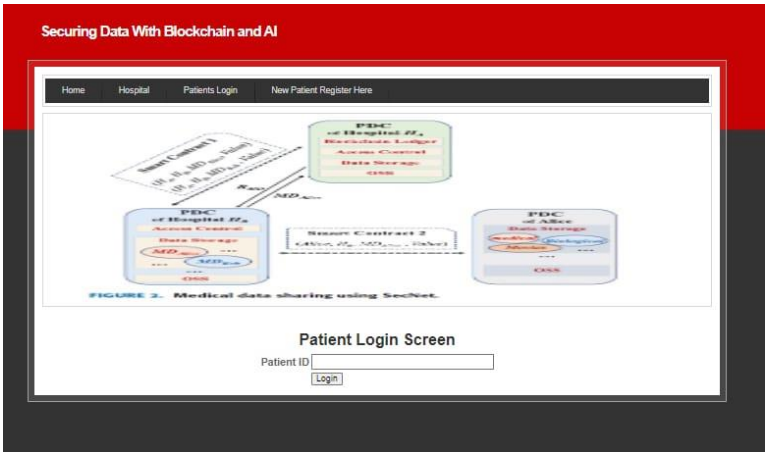
4. RESULTS




Securing Data With Blockchain and AI
Home
Hospital
Patients Login
New Patient Register Here
Hospital Login Screen
Username
Password
Login


Home
Hospital
Patients Login
New Patient Register Here
Patients Profile Creation Screen
Patient Name
Age
Problem Desc
Access Control
Hospital 1
Hospital 2
Gender
Male
Contact No
address
Create


Home
Hospital
Patients Login
New Patient Register Here
Patients Profile Creation Screen
Patient Name
kittu
Age
24
stomach pain
Problem Desc
Access Control
Hospital 1
Hospital 2
Gender
Male
Contact No
9999999598
hyd
address
Create



5. CONCLUSION

In this paper, In order to leverage AI and blockchain to fit the problem of abusing data, as well as empower AI with the help of blockchain for trusted data management in trust-less environment, which is a new networking paradigm focusing on secure data storing, sharing and computing instead of communicating. provides data ownership guaranteeing with the help of blockchain technologies, and AI-based secure computing platform as well as blockchain-based incentive mechanism, offering paradigm and incentives for data merging and more powerful AI to finally achieve better network security. Moreover. 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.

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. 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 distributed 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 crowd sensing 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. Praseed 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

ISSN- 2394-5125 VOL 10, ISSUE 04, 2023

[28] G. Wood, ‘‘Ethereum: A secure decentralised generalised transaction ledger,’’ Ethereum Project Yellow Paper, 2018. Accessed: Jun. 5, 2019.