IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907128 |

Preserving Data with Blockchain Technology and the Simulation of Intelligent Behavior (AI)

Ganesh kumar, Priyanka.Y

PG Student, Dept. of C.S.E., Bheema Institute of Technology & Science, Adoni, India

Assistant Professor, Dept. of C.S.E.,Bheema Institute of Technology & Science, Adoni, India

ABSTRACT: Data is the source for various AI algorithms like SHA256 to dig valuable features, yet data in Internet is placed everywhere and controlled by different partners who cannot trust one another, and usage of the knowledge in complicated cyberspace is difficult to authenticate or to validate. As a result, it's extremely difficult to enable data sharing in cyberspace for large amount of data, likewise as a true powerful AI. during this paper, we propose the secured private network, an architecture which can enable secure data saving, computing, and sharing within the large-scale Internet environment, aiming at a safer cyberspace with real big data and thus enhanced AI with many data source, by integrating three key components: 1) blockchain-based data sharing with ownership guarantee, which enables trusted data sharing within the large-scale environment to make real big data; 2) AI-based secure computing platform to supply more intelligent security rules, which helps to construct a more trusted cyberspace; 3) trusted value-exchange mechanism for purchasing international intelligence, providing the way for participants to realize economic rewards when giving out their data or service, which promotes the knowledge sharing and thus achieves better performance of AI. Moreover, we discuss the standard use scenario of private network similarly as its potentially alternative due to deploy, further as analyze its effectiveness from the aspect of network security and economic revenue.

KEYWORDS: Artificial Intelligence, Blockchain, Cyberspace, SHA256

I INTRODUCTION

With the event of data technologies, the trend of integrating cyber, physical and social Central systems to a highly unified information society, instead of just a digital Internet, is becoming increasing obvious. In such an information society, data is that the asset of its owner, and its usage should be under the complete control of its owner, although this is often not the common case. Given data is undoubtedly the oil of the knowledge society, almost every big company want to gather data the maximum amount as possible, for his or her future competitiveness. An increasing amount of non-public 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 knowledge owners. Moreover, the usage of these data is out of control of their owners, since currently there's not a reliable thanks to record how the info is employed 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 a private to manage the potential risks related to the collected data. For instance, once the info has been collected by a 3rd party (e.g., a giant company), the shortage of access to the current data hinders a personal to know or manage the risks associated with the collected data from him. Meanwhile, the dearth of immutable recording for the usage of information increases the risks to abuse them. If there's an efficient and trusted thanks to collect and merge the information scattered across the full central systems to create real big data, the performance of AI are going to be significantly improved since AI can handle massive amount of knowledge including huge information at the identical time, which might herald great benefits and even makes AI gaining the power to exceed human capabilities in additional areas. According to the research in , if given great deal of knowledge in an orders of magnitude more scale, even the best AI algorithm currently are able to do fanciest performance to beat many state-of-the-art technologies today. The key lies in the way to make data sharing trusted and secured. Fortunately, the blockchain technologies could also be the promising thanks to achieve this goal, via consensus mechanisms throughout the network to ensure data sharing in a very tamper-proof way embedded with economic incentives. Thus, AI maybe further empowered by blockchain-protected data sharing. As a result, enhanced AI can provide better performance and security for data.During this paper, we aim at securing data by combining blockchain and AI together, and style a Secure Networking architecture (termed as protected network) to significantly improve the safety of knowledge sharing, and so the protection of the entire network.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907128 |

II. EXISTING SYSTEM

An increasing amount of private 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 giant companies, which brings in big risk on privacy leakage of knowledge owners. Moreover, the usage of these data is out of control of their owners, since currently there's not a reliable thanks to record how the information is employed 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 a personal to regulate the potential risks related to the collected data. In cyber world everything relies on data and every one computing algorithms discover knowledge from past data only, as an example in online shopping application users review data is incredibly important for brand new comers to require decision on which product to get or to not purchase, we are able to take many examples like health care to understand good hospitals or education institutions etc. Not all cyber data are often made publicly available like Patient Health Data which contains patient disease details and get in touch with information and if such data available publicly then there's no security for that patient data. Now a day's all service providers like online social networks or cloud storage will store some form of users data and that they can sale that data to other organization for his or her 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 own data centers with Blockchain and AI technique to supply security to user's data. during this technique functions will work which describe below

Blockchain: Blockchain-based data sharing with ownership guarantee, which enables trusted data sharing within the large-scale environment to create real big data. during this technique users can define access control which implies which user has permission to access data and which user cannot access data and Blockchain object are going to be generate thereon access data and permit only those users to access data which has permissions. In Blockchain object user will add/subscribe share data and provides permission.

Artificial Intelligence: AI-based secure computing platform to supply more intelligent security rules, which helps to constructs more trusted cyberspace. AI work like human brain and responsible to execute logic to test whether requesting user has permission to access shared data. If access is on the market then AI allow Blockchain to display share data otherwise ignore request.

Rewards: during this technique all users who is sharing the information will earn rewards point upon any user access his data. Trusted value-exchange mechanism for purchasing Military Intelligence , providing the simplest way for participants to realize economic rewards when giving out their data or service, which promotes the information sharing and thus achieves better performance of AI.,

III. PROPOSED SYSTEM

Data protection is among key concerns of any network architectures, and is that the underside for AI algorithms to spice up due to its requirement for large amount of information from the foremost amount as possible places in Internet. Meanwhile, with a powerful AI, data protection is further protected at a way better level as an updated AI can determine advanced and complex threats more easily than normal AI. To boost the safety of information in central systems, numbers of efforts are conducted. The add presents an architecture named Amber to enable decoupling data from the net applications, which provides control ability to web users over their personal data, further as provides a strong web-wide query function to appear personal data. to increase the decoupling mechanism of knowledge and applications from only web services to any or all or any varieties of applications, the research group from the Media Lab in Massachusetts Institute of Technology designs the open own data centers, acting as a secured virtual space for users to gather, store and manage their data, separating all kinds of applications from operating on data directly. Besides, the emerging blockchain technology provides an efficient and effect because of guarantee the protection of information in central systems, by providing tamper-proof and traceable recording features additionally as incentive mechanisms.AI is additionally a promising due to enhance data security in central systems, since it can deeply analyze huge amount of knowledge, learn hidden patterns so make accurate predictions, with the assistance of availability of enormous data and increased computational power

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907128 |

Advantages: Data Protection

Disadvantages: Hash code has to be match to get output

IV. RESULTS

To implement this project author has taken medical data sharing example.
Modules Information:
This project consists of two modules
1) Patients 2) Hospital

Patients: Patients first create his profile with all disease details and then select desired hospital with whom he 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.
Patient Login: Patient can login to application with his profile id and check total rewards he earned from sharing data.

Hospital: 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.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

Figure 1: Home Page

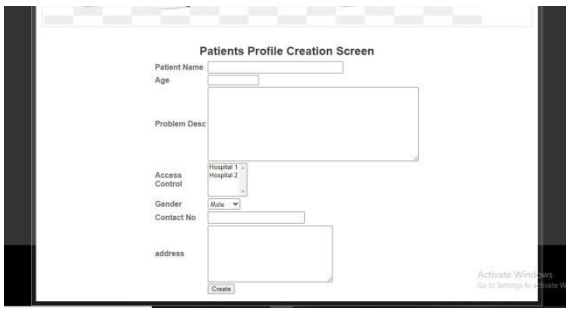

Figure 2: Patient Register

Figure 3: Hospital Login

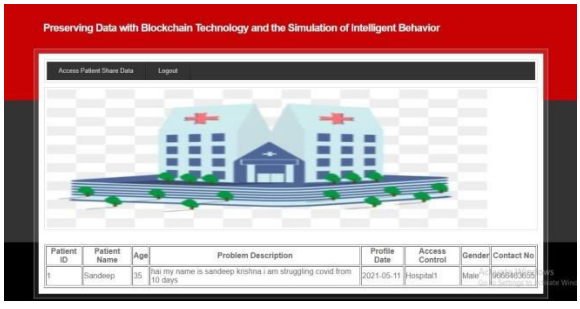

Figure 4: Accessing Data

1) In above screen click on 'New Patient Register Here' link to get below screen
2) In above 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
Patient is created with patient ID 1 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1
3) In above screen to login as Hospital1 click on 'Hospital' link to get above screen. Use 'Hospital1' as username and 'Hospital1' as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907128 |

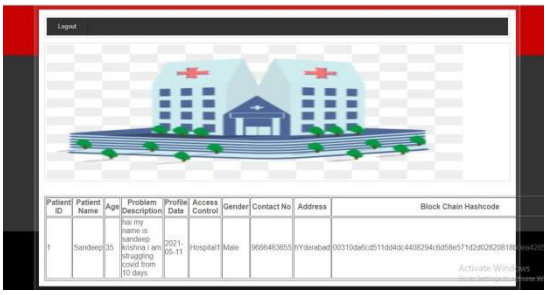

Figure 5: Searching Data

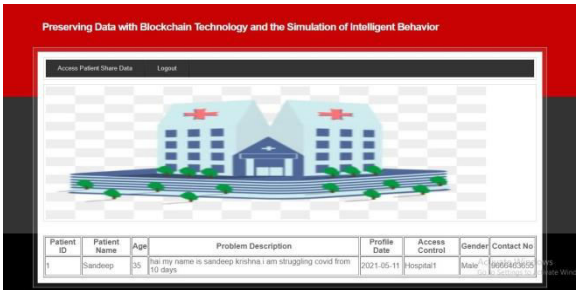

Figure 6: Hospital 1 Data

4) In above screen click on 'Access Patient Share Data' link to search for patient details
5) In above screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get below screen

6) In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as 'Hospital2'.

V. CONCLUSION

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 envi- ronment, we propose the Secured network, which is a new networking paradigm focusing on secure data storing, sharing and computing instead of communicating. Secured network 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.

REFERENCES

1. https://docs.python.org/3/reference/
2. https://www.python.org/doc/
3. https://docs.djangoproject.com/en/3.2/
4. https://dev.mysql.com/doc/refman/8.0/en/symbolic-links.html
5. https://en.wikipedia.org/wiki/Blockchain
6. http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf
7. http://tomcat.apache.org/

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details