INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

MEDICAL DATA SHARING WITH ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN

[1]M. Haritha·Ch. Balakrishna[1], P. Vinod[2], R. Amarnath[3], P. Lohith[4]

[1Assistant professor,2,3,4]student, Department Of Computer Science, Siddhartha Institute OfTechnology AndSciences Narapally –Hyderabad , Telangana

[5]Assistant professor, Department Of Computer Science, Siddhartha Institute Of TechnologyAnd Sciences Narapally –Hyderabad , Telangana

ABSTRACT

Data is used by various artificial intelligence (AI) algorithms to extract significant properties. However, data on the Internet is distributed and controlled by various stakeholders who do nottrust each other, and data usage in complicated cyberspace is difficult to authorize orauthenticate. As a result, enabling data sharing for real, vast data and genuine, powerful AI incyberspace is extremely difficult. We present the Sec-Net in this paper. An architecture capableof enabling safe data storage, computation, and sharing in a large-scale Internet environment.The Sec-Net aspires to create a more secure cyberspace with actual big data and, hence, enhanced AI with many data sources by combining these three critical features.1)Artificial intelligence: An AI-based safe computing platform to produce more intelligent security rules, supporting the development of a more trusted cyberspace; 2) blockchain-data sharing on the blockchain with ownership guarantees, allowing for trusted data exchange in a large-scale setting to create real big data;3) Trusted Value: Exchange methods for acquiring security services provide participants with a means of receiving cash compensation for donating their data or services, encouraging data sharing and improving AI performance. We explore Sec- Net's usual use case and numerous different deployment choices, as well as its success in termsof network security and financial advantage.

Index Terms: Artificial Intelligence, Blockchain, Cyberspace, Trusted Value.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

1. INTRODUCTION

The trend of integrating cyber, physical, and social (CPS) systems into a highly integrated information society rather than just a digital Internet is becoming more obvious. The advancement of information technologies in an information society, datais an asset of its owner, and its use should be totally under their control, although this is not always the case. Given that data is undeniably the lifeblood of the information age, virtually every big organization wishes to collect as much data as possible in order to remain competitive in the future. A growing amount of personal information is being collected, such as location data, web search history, and user calls. The built-in sensors within such huge firms' products discreetly record user preferences, posing asecurity risk to the data owners. Additionally, the owners of those data have little influence over how they are used at the moment. There are few reliable ways to track how and by whom the data are used, making it difficult to find or punishindividuals who misuse the data. In other words, it is highly challenging for a personto control the possible dangers associated with the obtained data when they lack the ability to manage it efficiently. For instance,once data has been gathered by a third party,a person's ability to comprehend or control the dangers associated with the data is hampered by the lack of access to that data.

Meanwhile, the hazards of data abuse rise due to the lack of immutable recordkeeping. The effectiveness of artificial intelligence (AI) will improve if there is a reliable and efficient method to gather and combine thescattered data scattered over the entire CPSto create genuine big data. will be greatly strengthened as a result of AI's ability to process enormous amounts of data simultaneously, which has a number of positive effects (such as improving datasecurity) and may even enable AI to outperform humans in more fields.

2. LITERATURE SURVEY

Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm

Abstract- With the expansion of the Internetof Things, a complex CPS system has emerged and is evolving into a workable information infrastructure. Protecting data sovereignty has become more

difficult. Dueto the loss of control over user data, the CPSsystem should encourage innovation while protecting privacy. In this essay, we proposeHyper-Net, a novel decentralised trustworthy computing and networkingparadigm, to address the problem of data loss of control. The intelligent PDC, which can be thought of as a digital representationof a person; the decentralised, trusted connection between any entities based on blockchain and smart contracts; and the three primary parts of the Hyper-Net are the UDI platform, which provides secure digital object management, and an identifier-driven routing mechanism. The future data-oriented information society might be created using Hyper-Net, which is equipped to defend data sovereignty and change the current communication-based information system.

MeDShare: Trust-Less Medical DataSharing Among Cloud Service Providersvia Blockchain
Abstract- As harmful activities on these records seriously harm the reputation, finances, and other assets of all parties associated directly or indirectly with the data, the publication of patient medical records poses a variety of hazards to patients' privacy. It has been established that the procedures used to maintain and preserve medical records are insufficient. Inthis study, we present MeDShare, a system that deals with the problem of medical big data custodians sharing medical data in an environment lacking trust. In cloud repositories, the blockchain-based approach provides data provenance, auditing, and control for huge data entities that exchange medical data. MeDShare tracks entities that access data from a data custodian system for nefarious purposes.MeDShare keeps a tamper-proof record of all operations taken on the MeDShare system, including data migrations andsharing from one entity to another. In orderto effectively monitor the behaviour of the data and revoke access to offending entitieswhen permissions on the data are breached,the design uses smart contracts and an access control mechanism. MeDShare performs on par with contemporary, state-of-the-art technologies for data sharing among cloud service providers. MeDShare would enable cloud service providers and other data guardians to achieve data provenance and auditing while exchangingmedical data with organisations like research and healthcare institutions with nodanger to data privacy.

Blockchain: A distributed solution to automotive security and privacy Abstract- A wireless

ISSN: 2057-5688

vehicle interface (WVI) is used in a future smart car to connect the Internet to the car and its vehicular bus systems. Future smart cars will be connected to the Internet of Things, presenting advantageous development potential for both consumers and the automotive sector. This might expose intelligent vehicles to a variety of security and privacy risks, such as tracking or vehicular espionage. For automotive systems to support the development of new services while safeguarding the security of the vehicles and the end-users' privacy fromintrusions, a thorough security architecture is necessary. In this article, we make the case that Blockchain (BC), a game- changing technology with numerous applications—from cryptocurrencies tosmart contracts—could be a potential answer to problems with car privacy and security. To safeguard user privacy and boost the security of the vehicular ecosystem, we suggest a BC-based design. Examples of how the suggested security architecture is employed include wireless remote software updates and other new automotive services like dynamic vehicle insurance rates. We also talk about how the architecture is protected against significantthreats.

Lightweight RFID protocol for medical privacy protection in IoT

Abstract- Traditional medical privacy information is extremely vulnerable todisclosure,and numerous relevantsituations have happened throughout time.For instance, it is easy for insurance firmsto obtain personal medical information,which not only jeopardises people's right to privacy but also impedes the healthygrowth of the medical sector. The Internetof Things has advanced quickly thanks tothe on going development of cloud computing and big data technologies. Oneof the foundational technologies of theInternet of Things is RFID. This issue of medical privacy can be efficiently resolved by integrating RFID technology into the medical system. Through the reader, RFID tags in the system can interchange and process data, gather important information,and communicate data with a back-end server. The exchange of information takes place mostly through ciphertext. Aninexpensive RFID medical privacyprotection system is presented in the paperwithin the context of the Internet of Things.Through secure authentication, the system guarantees the confidentiality and privacy of the obtained data. According to the security analysis and scheme evaluation, the protocol may successfully reduce the risk of medical privacy data being easily disclosed.

ISSN: 2057-5688

3. EXISTING SYSTEM

Data is everything in the digital world, and all artificial intelligence systems can only learn from past data. For instance, in online shopping applications, information about customer reviews is crucial for assisting new users in making purchasing decisions. Other examples include the medical field, where being aware of the best academic or clinical facilities is essential. Patient health information, which includes contact information and information about the patient's condition, is one type of cyberinformation that cannot be made public. If such details are made public, patient data is not protected. Today, all service providers, including cloud storage services and online social networks, will retain some user data on their servers and might even sell that data to other companies for their own financial advantage. All service providers today, including online social networks and cloud storage, will keep some kind of customer data and sell it to other parties. The user has no control over his data because it is saved on third- party servers by the organisation for their own purposes.

4. PROPOSED SYSTEM

Today, all professional cooperatives, such as online forums or distributed storage, will store some type of client information that they can then sell to other organisations for their own benefits without the client having any control over it because the information is being paid for by outside workers. Private data centres (PDC) using blockchain and AI procedures have been proposed as a solution to the aforementioned problem to provide security for customer data. Three features will be used in this process, as shown below.

1. Blockchain: Blockchain-based data exchange with owner guarantees enables trusted information participants in the context of an extremely broad reach to produce enormous amounts of information. Clients can define access control in this way, indicating which clients have permission to access information and which clients do not. A blockchain product will be created based on that entrance information and will only allow clients who have permission to access the information to access it. Clients will include, purchase, share, and grant approval for blockchain objects.

2. Artificial intelligence (AI): An AI-based, reliable processing stage that produces smarter security rules helps to build a safer internet. Artificial intelligence is capable of performing reasoning to determine whether a customer has given permission to share information. It functions similarly to the

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

human mind. If the door is open, then AI will allow blockchain to display shared information even if there is no demand.

3. Rewards: In this approach, every client that shares information will receive points for doing so each time a customer accesses it. trusted repute trade component for purchasing security services, offering a way for members to boost financial rewards when giving out their information or administration, which promotes data exchange and ultimately leads to improved AI performance.

5. ARCHITECTURE

If the hospital wants to support a critical medical experiment by using Alice's medical records, which are currently kept inanother facility, must first access its PDC

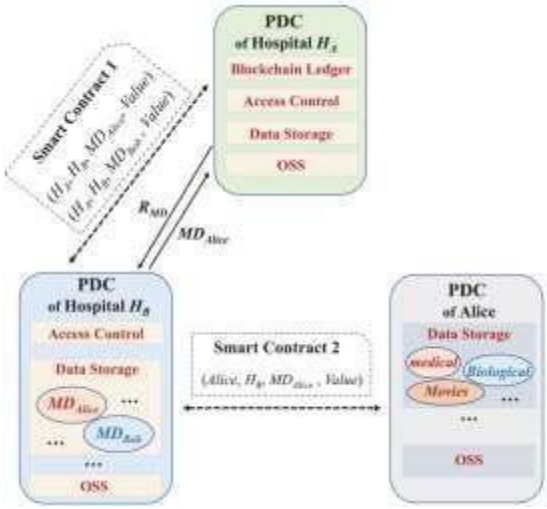

Fig.no.1: Architecture

before sending the data request with the metadata or identifier to the PDC that it belongs to. When the Access Control module receives the data, it analyses it using the ASC module in the OSS, and in the meantime, it records this request behaviour to the Blockchain Ledger as it waits for state synchronisation. The Access Control module communicates with the Data Storage module after the data is excluded from malicious access behaviour in accordance with the analysis output from ASC and its submodule GAN and then triggers the on-chain smart contract between and on the requested data, possibly also triggering the smart contract between and Alice. The first governs the price that should be paid for the requested data, and the second governs the price that should be sent to Alice

ISSN: 2057-5688

because she is the rightful owner. According to the smart contracts, when Alice receives the requested data, a corresponding value (such as tokens, coins,or electronic money) is sent to and from Alice. In other words, she receives compensation for holding Alice's medical data, and Alice receives compensation for authorising the sharing of her medical data with hospital.

METHODOLOGY

Patients: Patients first build their profilewith all of their disease information, and then they choose the hospital they want to share or subscribe to their data with. Whileonly those hospitals will be able to access data thanks to the profile application's creation of a blockchain object with the necessary permissions.

Patient login: Using his profile ID, the patient can access the programme and viewthe total awards he has received for data sharing.

Hospital: This application uses Hospital1 and Hospital2 as two organisations with which patients can share data. Any hospitalcan log in to the programme at once and then enter the disease name in the search field. The AI algorithm will take the hospital's access permissions into account and run a search on all patients to find patients with similar diseases. If the hospital has access permission, the AI algorithm will then display those patients' records to that hospital.

6. RESULTS AND EVOLUTIONMETRICS

7.

Fig.no.2: To open the screen below, click the 'New Patient Register Here' link in the screen above.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

Fig.no.3: On the page above, I'm providing information about the patient's disease and choosing "Hospital1" to submit my data. If you wish to share your data with two hospitals, hold down the "CTRL" key and choose both hospitals to confirm. To createa profile, click the "Create" button now.

Fig.no.4: One patient is created in the web page above with patient ID 1, and Hospital1 can now log in, search for, and retrieve this patient's information because the patient has granted permission to Hospital 1.

Fig.no.5: Click the 'Hospital' link to get the above screen and log in as Hospital1. To log in as Hospital1 and Hospital2, respectively, use Hospital1 as your username and Hospital1 as your password.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

Fig.no.6: In the image above, Hospital 1 is getting patient information, and since Hospital 2 doesn't have access, it cannot obtain patient information. Log out and back in as "Hospital2" to see this.

Fig.no.7: On the web page above, we can see the patient's complete information as well as the block chain-generated hash code. In the last column, we can see the patient reward revenue, which is currently set at 0.5 and will be updated each time a hospital user accesses it.

8.CONCLUSION

We propose SecNet, a different systemsadministration worldview that focuses on secure information putting away, sharing, and registering as opposed to conveying, inorder to use AI and block chain to fit the problem of handling information as well as enable AI with the assistance of block chain for trusted information for executives in a trust-less climate. With the help of block chain innovations, an AI-based secure figuring platform, and a block chain-based incentive mechanism, SecNet offers information proprietorship assurance. It also provides a paradigm and incentives for information combining and even more impressive AI in order to improve networksecurity. Additionally, we go over typical SecNet use scenarios in a clinical consideration framework and offer alternate methods

ISSN: 2057-5688

for utilising the storage feature of SecNet.

9. 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] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Q. Lu and X. Xu, ``Adaptable blockchain-based systems: A case study forproduct traceability," IEEE Softw., vol. 34,no. 6, pp. 2127, Nov./Dec. 2017.

ISSN: 2057-5688

[10] 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.

[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. 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.