IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Security Mechanism for Securing Data With Blockchain and AI using Ring Signature Scheme

1Anshu Singh, 2Sudhir Agarwal
1student, 2HOD
1BIT,Gida,Gorakhpur,
2BIT,Gida,Gorakhpur

***Abstract*— Data is the input to mine useful features for different artificial intelligence (AI) algorithms, but Internet data is distributed everywhere and managed by numerous stakeholders who can not believe in each other, and it is difficult to approve or verify the use of data in complex cyberspace. An AI will need large data to produce a digital copy of a delectable, or a full image. In turn, this practical AI-based digital copy would hit pandemonium, and well, it would be really hard, not to mention, unlikely for AI to operate with anyone without a very strong password. In this article, we propose SecNet, an architecture that will allow safe data collection, computing, and sharing in the large-scale Internet world, with AI improved by plenty of data, and more secure cyberspace. By incorporating blockchain-enabled data sharing, ownership assurance, and trustworthy computation, we plan to build a more stable Internet with plenty of big data and hence improved AI based on a fantastic dataset. In addition to listing out auditing criteria, we decide a typical implementation scenario and an unusual way to enforce its procedures. We then assess its effectiveness from the perspective of the network protection component and the Net Neutrality issue.**

Keywords*— *Data security, data systems, artificial intelligence, cyberspace..

I. INTRODUCTION

The growing integration of electronic, physical, and social structures into a highly structured knowledge society is becoming increasingly apparent, as information technology expand in sophistication. Data is the property of its user, it can be used in a manner that respects its owner's privacy, although this is not always the case. In light of the reality that data is indisputably the oil of the knowledge society, all major companies demand data to the fullest degree necessary to maintain their long-term competitiveness. The various built-in sensors in their products are gathering a significant amount of personal data which puts data owners at risk of privacy leakage. In comparison, the usage of data also makes the details be held by someone else.

The data are difficult to monitor, contributing to little ways to control or discipline violators who exploit the data irresponsibly. That is, the lack of listening capacity makes it very challenging for people to create a difference about the possible hazards of the noises they encounter. When a third party (such as a multinational company) has access to someone's records, it prohibits the user from learning or taking care of the details. The number of data types that is processed, but how poorly it is held, enhances the risk of data misuse. If there is an effective and trustworthy way to collect and integrate data scattered across the entire CPS to form real big data, artificial intelligence can be enhanced so AI can manage large amounts of data at the same time, including huge data.

.

II. LITERATURE SURVEY

Blockchain technology is attracting interest from various organisations for its usefulness in developed industries. Various encryption and security algorithms have been researched to enhance the security and privacy of blockchain technology. From the theory of Chaum stated in 1981, the currency mixing process of digital currencies borrows from the mixing of several unrelated inputs between the input wallet and the output wallet, rendering the outside world unable to correlate both the input and output addresses, so that the digital currency "ow" cannot be differentiated. This groundbreaking technology is funded by the Bitlaunder, Bitcoin Fog, and other technology-powered websites. Bonneau et al. suggested a single method for the mixing and audits in Mixcoin. As long as third-party node is operating illegally, consumer would be allowed to release his signature data and get his funds back. Soon enough, the integrity of the facility would be lost; thus, services won't be trusted. A blind coin scheme was introduced by Valenta and Rowan that enhanced the efficiency of Mixcoin. A blind signature is used to encrypt all outputs such that a 3rd party will not "link" the outputs to individual inputs. CoinJoin was developed by Maxwell Gregory. The end purpose is to achieve a series of transactions in order to yield a desired

result. If the input address that the signed transaction can use appears in the input address set, the transaction would be signed using the user's private key. The way money is exchanged in a contract is blurred or obfuscated through this method. Any of the mixing schemes involve a third person to combine the products. As a third party offering mixed currency services, it is difficult to deter third parties from hacking to access the user's input address, and the issue of leak of consumer privacy still remains.

Dash is a type of cryptographic digital currency because it behaves similarly to this. And preserve the privacy of consumers. To better comprehend the mixture of coins, one must use chained hybridization and blind technology. Dash's coin mixing feature is poor which can make it easy for malicious master nodes to manipulate the network. A coin mixing scheme known as CoinShuffe was introduced by Ruffing et al.[19], which added the output address shuffle feature with CoinJoin while not enabling other nodes to join in. Participants could be online at around the same time to guarantee sufficient coverage in a denial of service attack.

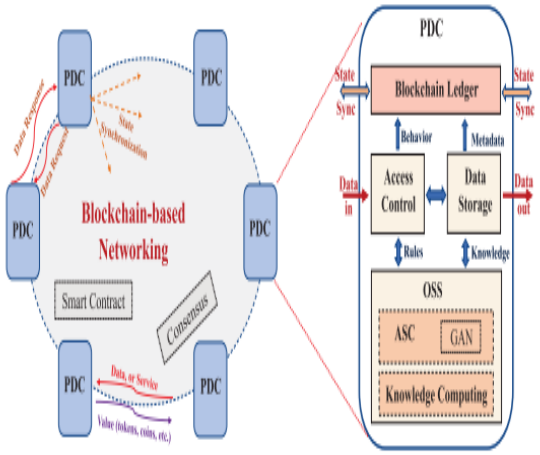
To reclaim customer privacy, Meyer et al. [21] proposed utilizing zero awareness methods in an effort to hide the identification of the consumer. The users can use Zerocoin to obscure the addresses of the transfers, making them untraceable. Zerocoin will mint only a fixed-amount currency and proof-of-work provides for their zero-knowledge proof info. Szabo et al.[22] launched a new type of digital currency named Zerocoin. In order to preserve the privacy of the parties, Zerocash utilizes a pledge scheme to denote the meaning and pattern of the transactions. At the same time, to uphold the highest level of privacy and anonymity in existing " digital currency " transactions, Zero-cash added zk-SNARK technology to " digital currency ". The mechanism used to generate zero-knowledge proofs, but it is slow and complex. The production of results requires an average of one minute and there is a bench bottleneck.

The details in the distributed public ledger are kept in the distributed collection The King but it is not always The King. As long as personal data isn't used in the public ledger, the blockchain will have addressing the privacy problem.

On-chain payment networks also use this technology. Suggested two-way micro-transfers, lightning network networks, sprites, bolt and other off-chain payment technology are used to provide safer off-chain transactions, i.e. much of the transaction details are performed off-chain between users, users just need to record the first and the last transactions in the blockchain ledger. Unidentified transfers between users by third parties are all counterfeited by the latest off-chain transaction technology, but still there are still some shortcomings. For example, the transaction background of an entity has to be checked freely at all occasions, and how do we ensure that a transaction is fair without revealing their personal details. A multi-signature address is a special type address. Whenever one signs a community post, their signature is even tougher to infer than a simple signature. Monero utilizes ring signatures, ring hidden transfers, and cryptographic addresses to hide the origin and destination of all transactions. In the art of electronic payments, privacy is key.

III. PROPOSED METHODOLOGY

Blockchain - the latest technology of data exchange with ownership assurance, which allows trustworthy data sharing at large scale. 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.



A.] Module description

Emotion Recognition Using Physiological Signals :-

Biosensors track the activity of a human nervous system that is regulated autonomously. The electrodes will calculate skin conductivity, blood pulse, temperature, heart rate, and more. In this analysis, GSR and PPG signals have been used.

Emotion Representation

• Several explanations have been suggested by psychologists about how people perceive emotion terms. According to the Kanizsa triangle, there are only a few independent emotional aspects inside a person. The two most important elements of depressive feelings are severity and negative behaviors (the intensity of an emotion as good or negative).

Feature extraction: -

• The process of feature extraction is a necessary step in a machine learning pipeline and is applicable to the representation of signals by vectors. To capture physiological signals reliably, each signal has been broken down into its individual time domain elements and features have been extracted based on numerous statistics. After capturing GSR and PPG data to distinguish signals, the various signals are segregated to capture localized data.

Data Fusion: -

• Data fusion is known as a blended logic. The primary aim of decision-level methods is to integrate multiple classifiers into one in order to obtain higher precision and robustness. Classifier fusion consists of classifying items together and thus merging certain classifications.

B.] Classification

• The participants reach valence and arousal values during the learning process, which varies between 1 and 9. The documents are important for teaching models and modelling. Due to the label-based info.

C.] Algorithms used in this project: -

- **K-means clustering algorithm: -**

KNN Algorithm:

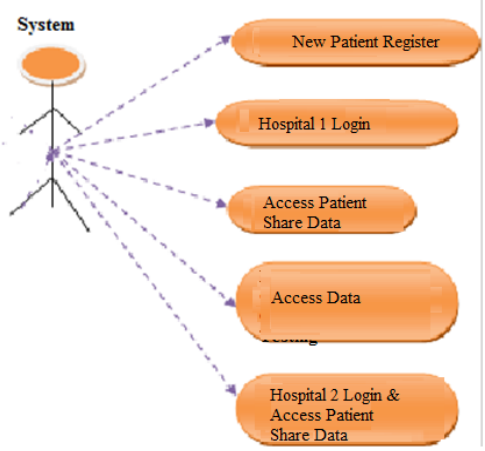
- k nearest algorithm tests and blends k nearest points depending on how far apart they are and how well they complement others. ·

- **Artificial neural network**

Artificial neural networks are used in the development of deep learning algorithms. As the "neural" aspect of its name implies, the device is built to imitate how we learn as humans. Neural networks consist of input, secret and output layers, and a middle layer that converts the input into what the output layer may use. They are outstanding instruments for identifying trends which are too complicated or multiple to be found by a human programmer.

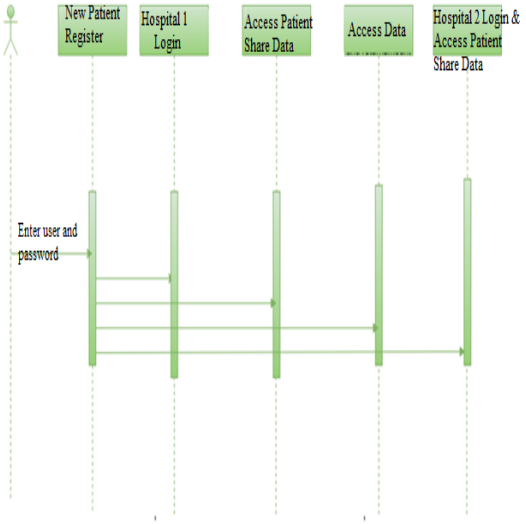
- **Use Case Diagram:**

a use case diagram is a type of behavioral diagram generated by use case analysis; a UML use case diagram. This paper attempts to provide a schematic description of what a device should do, and what actors are involved in achieving the capability. Usage Case diagrams may be used to display the machine roles a product executes on various actors. The functions of each actor may be established.



- SEQUENCE DIAGRAM:

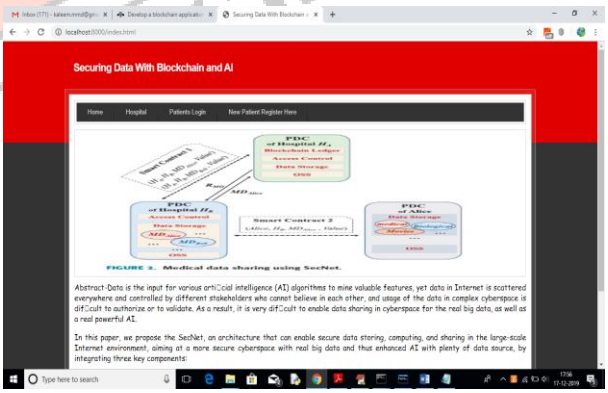
A series diagram is an integrated diagram demonstrating how systems communicate with one another and how they function in the order they do. That is a technical summary of a Message Series Map. Sequence diagrams are also referred to as event diagrams, event situations, and pacing
diagrams.



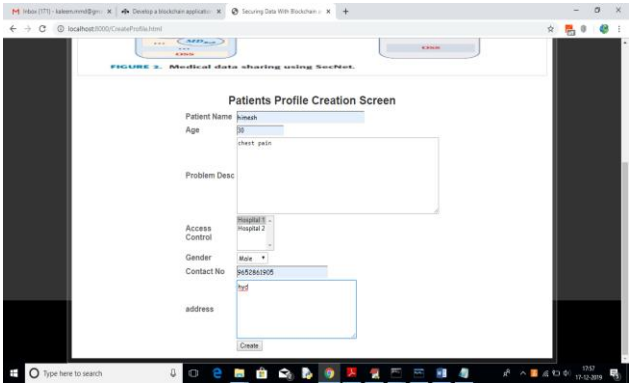
1V. RESULTS AND SCREENSOTS

IV. RESULTS

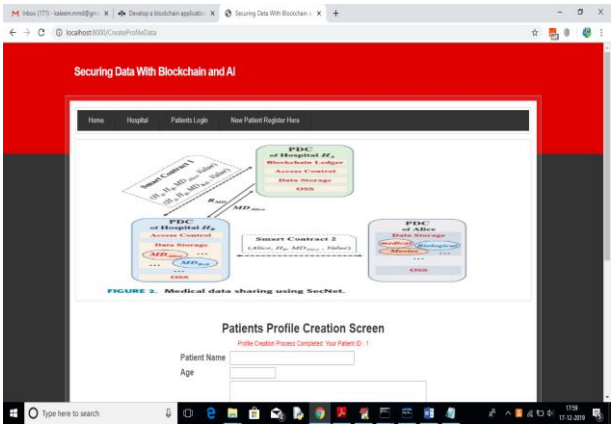
Deploy code on DJANOGO and start server and run in browser to get below screen



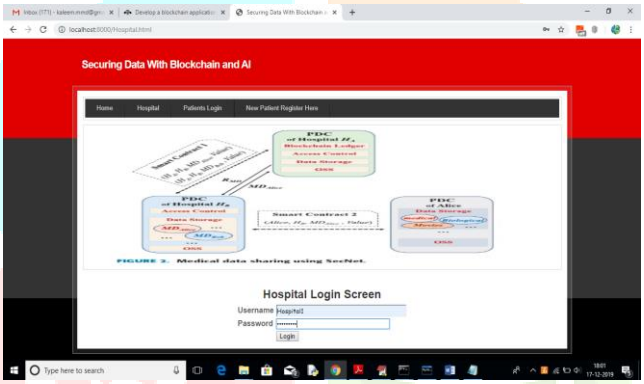
In above screen click on 'New Patient Register Here' link to get below screen



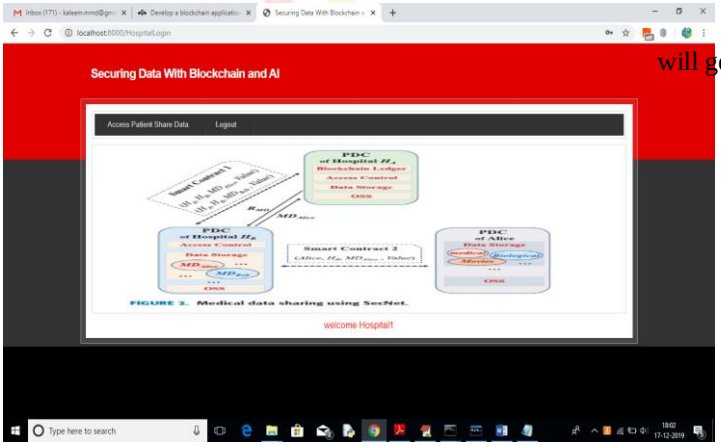
In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile



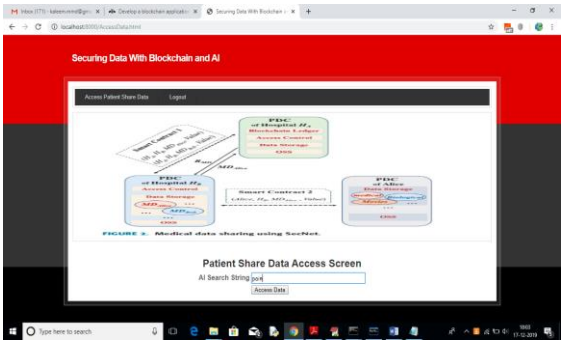
In above screen one patient is created with patient ID 1 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1



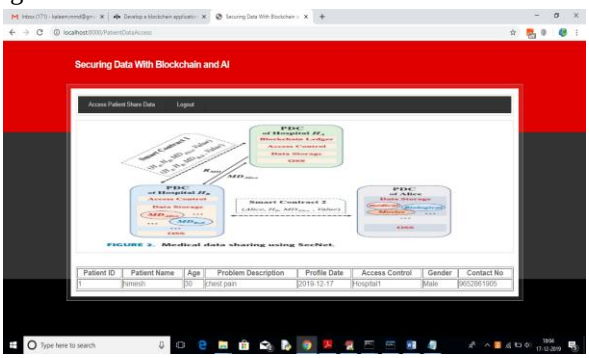
In above screen to login as Hospital1 click on 'Hospital' link to get above screen. Use 'Hospital1' as username and 'Hospital1' as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen



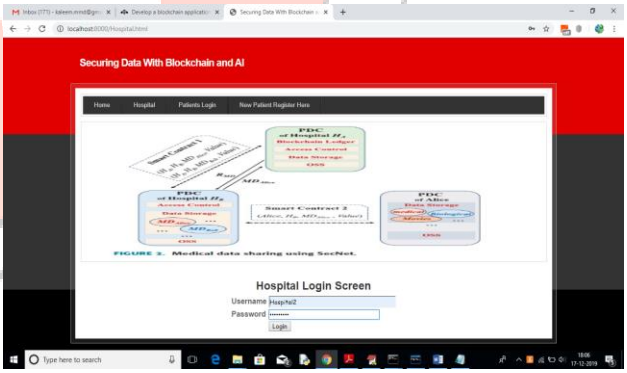
In above screen click on 'Access Patient Share Data' link to search for patient details



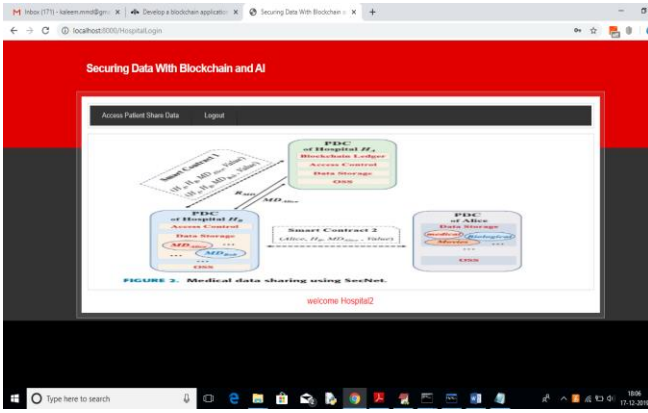
In above screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get below screen



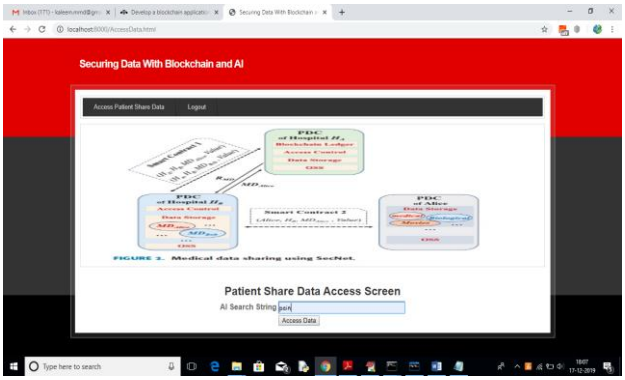
In above screen Hospital1 getting details of patient and Hospital2 not having permission
so it will not get details. To see this logout and login as 'Hospital2'



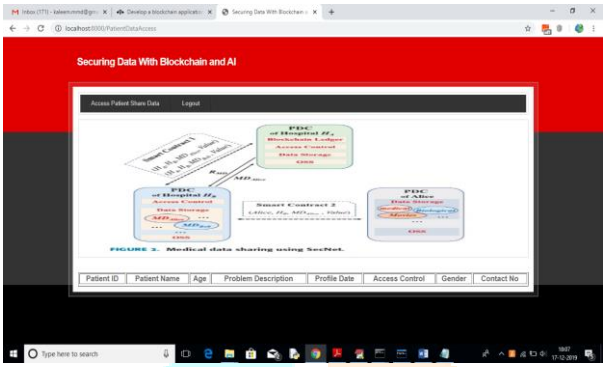
In above screen 'Hospital2' is login, after login will get below screen



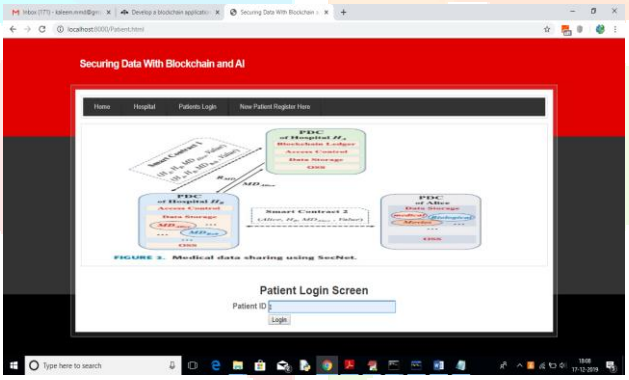
Now click on 'Access Patient Share Data' link and search for same pain disease



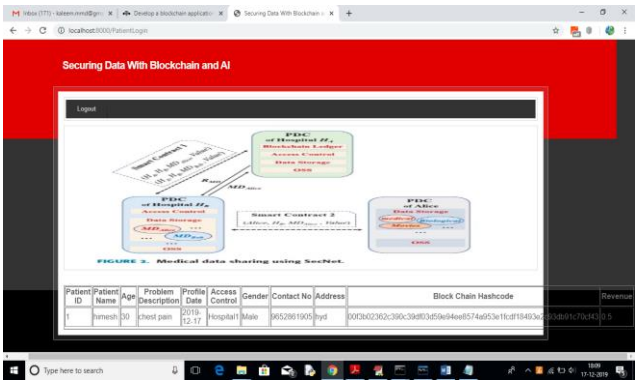
For above query will get below result



In above screen no patient details are showing as Hospital2 not having permission. So block chain allow only those users to access data who has permission. Now logout and login as patient by entering patient id in below screen



After login will get below details for patient 1



In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

V. CONCLUSION

Within a data-driven and trust-less framework, we propose the SecNet, a modern networking paradigm focused on stable data management. SecNet provides the incentive system and market system for data assimilation and the open application platform for AI growth. We discuss how SecNet is beneficial for researchers in the medical sector and demonstrate many common ways of using SecNet. Furthermore, we discuss how to solve a Distributed Denial of Service attack, and how the mechanism can enable users to share security policies. Later on, we will discuss possibilities for data sharing and higher AI processing in the SecNet. We can use SecNet to run projections simulations to assess the project performance (e.g., integrating IPFS [27] and Ethereum [28] to form a SecNet-like architecture).

REFERENCE

1. M. Jamshidi et al., "Artificial Intelligence and COVID-19: Deep Learning Approaches for Diagnosis and Treatment," in IEEE Access, vol. 8, pp. 109581-109595, 2020, doi: 10.1109/ACCESS.2020.3001973.
2. A. A. Hussain, O. Bouachir, F. Al-Turjman and M. Aloqaily, "AI Techniques for COVID-19," in IEEE Access, vol. 8, pp. 128776-128795, 2020, doi: 10.1109/ACCESS.2020.3007939.
3. V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341.
4. F. Shi et al., "Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation and Diagnosis for COVID-19," in IEEE Reviews in Biomedical Engineering, doi: 10.1109/RBME.2020.2987975.
5. Q. Pham, D. C. Nguyen, T. Huynh-The, W. Hwang and P. N. Pathirana, "Artificial Intelligence (AI) and Big Data for Coronavirus (COVID-19) Pandemic: A Survey on the State-of-the-Arts," in IEEE Access, vol. 8, pp. 130820-130839, 2020, doi: 10.1109/ACCESS.2020.3009328.
6. N. Zheng et al., "Predicting COVID-19 in China Using Hybrid AI Model," in IEEE Transactions on Cybernetics, vol. 50, no. 7, pp. 2891-2904, July 2020, doi: 10.1109/TCYB.2020.2990162.
7. R. Sethi, M. Mehrotra and D. Sethi, "Deep Learning based Diagnosis Recommendation for COVID-19 using Chest X-Rays Images," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 1-4, doi: 10.1109/ICIRCA48905.2020.9183278.
8. Y. Oh, S. Park and J. C. Ye, "Deep Learning COVID-19 Features on CXR Using Limited Training Data Sets," in IEEE Transactions on

Medical Imaging, vol. 39, no. 8, pp. 2688-2700, Aug. 2020, doi: 10.1109/TMI.2020.2993291.

9. M. U. Ashraf, A. Hannan, S. M. Cheema, Z. Ali, K. m. Jambi and A. Alofi, "Detection and Tracking Contagion using IoT-Edge Technologies: Confronting COVID-19 Pandemic," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 2020, pp. 1-6, doi: 10.1109/ICECCE49384.2020.9179284.
10. D. Dong et al., "The role of imaging in the detection and management of COVID-19: a review," in IEEE Reviews in Biomedical Engineering, doi: 10.1109/RBME.2020.2990959.
11. M. Sethi, S. Pandey, P. Trar and P. Soni, "Sentiment Identification in COVID-19 Specific Tweets," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 509-516, doi: 10.1109/ICESC48915.2020.9155674.
12. A. Ramchandani, C. Fan and A. Mostafavi, "DeepCOVIDNet: An Interpretable Deep Learning Model for Predictive Surveillance of COVID-19 Using Heterogeneous Features and Their Interactions," in IEEE Access, vol. 8, pp. 159915-159930, 2020, doi: 10.1109/ACCESS.2020.3019989.