Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Secured Blockchain framework using deep learning to reduce the service latency in a 5G based distributed networking environment

[*1]Anju Raveendran, [2]Dr. R. Dhanapal
*[*1]Ph.D. Scholar, Dept. of CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, 641021; Email id: anju1981rave@gmail.com*
[2]Assistant Professor, Dept. of CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, 641021. Email id: dhana85pal@gmail.com
Corresponding Author: Dr. R. Dhanapal,dhana85pal@gmail.com

Abstract: The Internet of Things (IoT), which is also represented as Internet of Health Things (IoHT), has witnessed numerous progresses in recent existences, particularly in the management of healthcare-related data. Because those healthcare statistics ensure greater accuracy, security with improvedreliability, and higher data feature, supplying those data to those healthcare apps is a time-consuming difficulty this organisation is facing. To developstatisticsestablishing, data must be more secure and privacy-protected, as deep learning and privacy policies are enabled with 5G network. If the information is private, the information owner may be able to learn about it. The data process flow associated with IoHT is now connected to a variety of IoT devices as edge nodes, thanks to recent advancements. Learning at the nodes is more difficult because of the issue of a missing or insufficient amount of training data, which necessitates a completely distributed setting, as well as new, better datasets, their establishing, and their security. In this work, a Hy-FL-based Blockchain strategy is proposed since it is enabled with blockchain, which maintains trust ability and skilled data based on deep learning with enhanced validation. With the help of the suggested method, training information on the deep nodes can be encrypted and aggregated. In the analysis, data management is managed securely based on IoHT in terms of projected value, energy usage, and data correctness.

Keywords: Blockchain, Healthcare, Privacy Deep learning, Internet of health Things, and Security, 5G.

I. INTRODUCTION

The proliferation of IoHT [1, 2] has resulted in a rise in the quantity and quality of health data available for use by the healthcare sector. Recent advances in deep learning applications have made it possible for IoHT data to be automatically interpreted with high accuracy, allowing for continuous health monitoring with minimal human intervention. In order to reduce patient wait times, hospitals can use cutting-edge deep learning algorithms for triage and diagnosis. Yet, the IoHT records private information about people's health and the environment, so it must be protected [3]. [5] This is because of the possibility of legal ramifications. Some of the security and privacy worries surrounding IoHTfacts can be allayed thanks to recent improvements in edge learning, which allow for sensitive patient data to be learned locally within a hospital [6]. There is no requirement to upload learning data to the cloud when using modern machine learning algorithms for remote and collaborative training, such as deep learning (FL). As a result, the owner can continue to maintain control over the sensitive data.

Using the wireless network asset of IoHT nodes, an additional thought-provoking lightweight security and attribution approach was proposed in [7]. In [8], for instance, the authors looked at how the authenticity of AI algorithms could be tested by analysing the decision-making processes of deep learning applications. This is another facet of where something came from. [9] Data privacy and security in the IoHT were analysed using blockchain and machine learning, and the results are depicted in Figure 1.

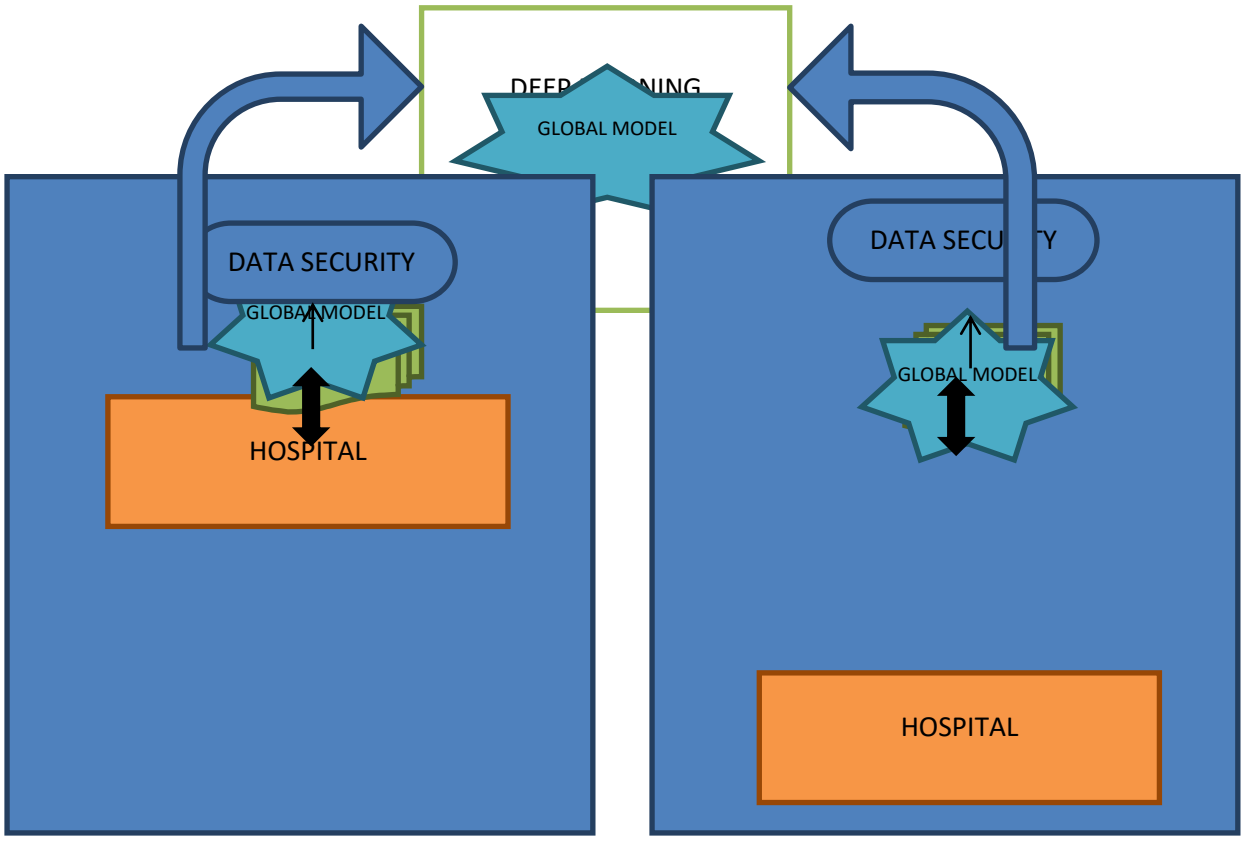


Figure 1.Deep learning based IoT Healthcare

It has been looked into how deep learning could be used at the periphery to improve healthcare and IoHT [10] data. In this era of strict security standards and close scrutiny of health data privacy, researchers, for example, are increasingly relying on deep learning representations that allow for protectedpreparation, modelling aggregates, and broadcasting of whichever the model or the inference findings. When using FL, numerousremote nodes can share a single, encrypted deep model that has been trained on regional data to produce highly specific predictions. The deep learning model and teaching dataset need to be kept locally [11] to enable secure and private IoHT improvements.

A different study [12] recommended a two-stage FL approach, with the first stage allowing for the selection of a trustworthy committee member via a federation-based method. To elect a trustworthy federation member to the committee, Phase 1 of the FL approach was advocated in another study [13]. The recent pandemic has created the potential for extensive IoHT use [14]. IoHT-based healthcare is growing more and more popular as a result of the pathogen's ability to spread brain tumour disease among the persons in all ages. The prospects for the current secure and privacy-focused FL approaches are positive.

II. RELATED WORKS

While users collaborate to train the global model, their anonymity is preserved by FL. The security of FL, however, can be easily compromised by clients who are hostile. Fortunately, blockchain [15] provides a workable answer to these problems. Blockchain technology can be used to accumulate ML/DL models and limitations for improved data safety and genuine decentralisation in FL. The consensus efficiency in blockchain technology can also be enhanced by employing FL. Even more so, blockchain technology allows for the trading and confirmation of updates to local learning models on mobile devices. Blockchain has a number of important characteristics, including immutability, authenticity, distribution, transparency, and decentralization [16]. Security, data integrity, centralization, and individual privacy are all issues that can be addressed with the help of these capabilities in smart healthcare. In their article, Georgios et al. delved into the various ways in which AI is being used to improve medical care. They discussed the state of the art and the way forward for federated, secure, and privacy-preserving AI techniques [17], with a particular emphasis on their use

in medical image applications. A blockchain-based framework has been proposed by Marulli et al. to facilitate machine learning research on cloud services with additional security, privacy, and scalability.Thedeep models benefited from this change. Privacy in a deep learning environment was analysed along with potential solutions in [18].

A new method for keeping your data secure on the blockchain has been released, one that makes use of a trusted execution environment to guarantee the safety of your personal information. The issue with classic blockchain, wherein a rogue node's intrusion prevents the Merkle tree from providing nonmember evidence, was brought up. A password accumulator is proposed by the authors as an alternative to the Merkle hash tree for secure data storage. Using a blockchain chain approach, [19] suggested that IoT data may be shared and secured among various data providers. ACOMKSVM with ECC is presented in this work for safe and dependable data sharing. The proposed blockchain-based private FL framework makes use of the distributed nature of the blockchain to provide proof-of-change. FL to take a closer look at the issues that need fixing and the possible ways to fix them. The cited works provide further reading material on the subject of Blockchian technology, deep learning, and their integration with the Internet of Things and artificial intelligence.

A. Blockchain enabled with privacy:

The value of the blockchain to DP has been debated. The authors in [20] propose using a blockchain to footpathentire and separatesecrecyresources, the amount of sound contributed to inimitableinquiries, and the amount of noise that can be tolerated before reducing dataset excellence and privacy cost after artificial interference has been injected to mitigate a data leak through data query. As a follow-up [21], researchers provided a platform for sharing training data in a multiplayer game setting and made the improved method accessible via blockchain.

The work published in leveraged blockchain for alleviate private information, poisoning threats, and network latency. With the help of a consensus mechanism, miners checked the legitimacy of the uploaded models from the deep edge nodes. FL administered via blockchain, according to the authors [22], would be the most effective method for preventing the disclosure of sensitive data in 5G ultra-dense mobile periphery networks. BlockFlow's creators have established an auditable and responsible framework for FL collaboration by rewarding legitimate contributions while excluding fraudulent ones. To protect the privacy and security of IoT data stored in edge devices, as it is adopting a blockchain built on a decentralised FL architecture. They examined the data privacy and its security risks of introducing IoHT data into FL's data combination cycle in a smart home [23].Ensuring Security on Deep Learning Models:

Researchers in [24] analysed the current state of security and its privacy in deep learning presentations using 5G edge networks. The authors of crafted a protocol using FL within 5G networks to protect private information that can be accessed by network functions or networking slices, as well as the privacy of updates to local deep learning models. A worldwidepreparationcomponent was governed by a cryptographically secured smart contract, and the researchers used FL to train the private data of a single railway line using an SVM RBF kernel function. More and more local FL models are being verified for authenticity and integrity using the blockchain [25].

The authors of [26] have developed a secure deep learning model called secure SVM that does not require the use of a trusted third party. The Paillierhomomorphic cryptosystem was used to encrypt the IoHT data before it was added to the blockchain, making it immutable and auditable in the process.Reviewed attacks on FL algorithms that involve data poisoning and inferencing. The survey makes design recommendations for a resilient FL model [27] and [28].

Provenance in the food market has made use of blockchain technology and deep learning, with the latter being used for fruit classifications. Authors of showed that IoT trustworthy zones included in smart contracts can guarantee the integrity of IoHT data.

III. PROBLEM STATEMENT

The integrity of the training data and models that are distributed among stakeholders and deep nodes is crucial to the success of IoHT. We use block chain technology and off-chain to safeguard the data information from being changed or accessed by people who shouldn't be able to see it. Gradient mining that cannot be tampered with and a distributed consensus-based aggregator take the place of the central gradient aggregator, which is notoriously unreliable. An additional layer of security at the various nodules collecting the gradients is provided by our Hy-FL-based blockchain, which features a

safe for the nativeprototypicalcombination process. The hash of the encoded global model is written to the blockchain once aggregation within the secure enclave is complete. To ease communication and computation on the FL edge nodes, the proposed model combines secret sharing with the privacy of model gradients. When trying to find a happy medium between privacy and model accuracy, we suggest a particular level of DP. This level reduces the likelihood of a model inferencing attack that reveals particular pieces of training data. To counteract anexterminatingoccurrence, in which a mischievous FL node subtly inserts a deadly model into the training data, leading to distorted inference, secure model aggregation is employed.

IV. REASEARCH METHODOLOGY

A. Typical FL and its characteristics:

- The ability to train in parallel;
- Training at the edge and locally with complete independence;
- A less load on data management;
- Minimal labelling requirements for data; and
- The ability to deliver individualized learning via domain adaptation [7].

Integrating IoHT sensors for sensing, a FL algorithm for learning and reasoning, and human decision-makers or an AI algorithm based on statistics analytics for making decisions are the main components of any IoHT-based health method. Traditional FL presents a number of difficulties for IoHT-based applications.

- Users in FL may represent a wide range of specialisations, each with their own set of skills and access to ancillary resources.
- Each FL node could have a unique assortment of training data that is not independent, identically distributed (non-IID), or publicly available.
- During the process of aggregating the models, there may be lags and erratic communication costs.

There could be many different kinds of clients in FL, each with their own set of skills and advantages. Each FL node may have its own unique source of training data, and that source may use non-IID (non-independent, identically distributed) data of varying quantities and qualities. When combining multiple models, there is a possibility of sluggishness and unreliable communication delays and costs. Harmful nodes or an aggregating node could compromise network security and user privacy.

When a training model is exposed to cyberattacks such as adversarial networks that are generative, its effectiveness may decrease. The authors of [10] demonstrated how a malicious cloud model aggregation node might learn private information about an edge node by examining common gradients. Data owners in the IoHT, hospital administrations that jointly own electronic IoThealthrecords and government bodies that deliver healthcare facilities to citizens have a responsibility to maintain the confidentiality and integrity of this information [11].

Implementing privacy and data provenance in the IoHT for deep learning applications can be aided by a variety of strategies [12], [13]. Researchers have proposed various methods to prevent any infringements on participants' privacy during collaborative training. In [15], the authors develop a method for secret information to leak out in a FL setting. Using privacy and obfuscation, the authors of [16] proposed a quantitative trustworthiness metric for gauging the provenance of IoHT data. When compared to a centralised training node, the accuracy of training data may improve when more deep nodes are used, especially if some of the nodes have higher quality and more datasets. Each deep node's privacy can be protected with some edge-level training.

B. FL based Information security:

Even though FL is effective at protecting sensitive data, it is not the best choice if the training data must be kept secret or anonymized from third parties [17]. Trained models that are used by multiple entities in a distributed network can be de-identified. Since the FL exemplarypermits for multiple nodes to take part in the training process, it is important to pinpoint malicious nodes that take part in the training, model aggregation, or inference processes and compromise them. Then, a reliable control system based on secure defence mechanisms must be implemented.

A standard FL assumption is that the central aggregating server can be relied upon. Researchers have suggested using a fully decentralized gradient aggregation approach to get around issue [24]. Blockchain enables secure transactions between untrustworthy parties and has strong cryptography

capabilities [25], [26]. Blockchain and off-chain technologies have shown significant promise for IoHT data provenance. InterPlanetary File System (IPFS) and similar off-chain storage systems have grown in popularity due to their ability to preserve the veracity and authenticity of data from reliable deep nodes, their datasets, the credibility of all networks, the accurateness of the representations produced by all devices, and the consistency of the global model itself [27].

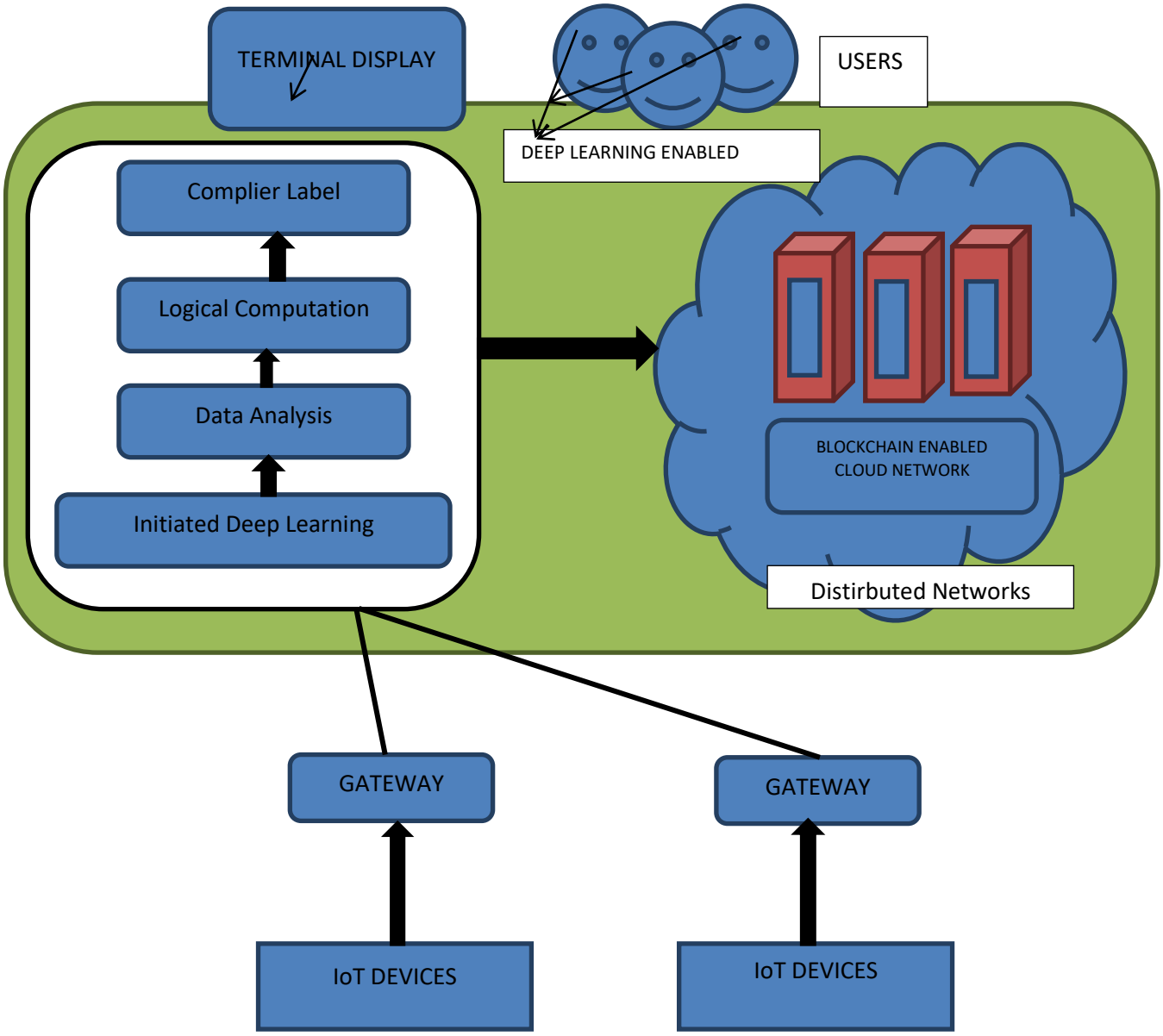


Figure 2. Hy-FL based Blockchain Approach

Aadvanced overview of the scheme architecture of a blockchain-based IoT cloud platform is shown in Figure 2.

The core elements of the system are as follows:

- It's the sensor network, off of which the data publishers operate their own personal data centres.
- The user interface showed various Internet of Things (IoT) gadgets, as well as a blockchain cloud network where data is validated, processed, and distributed to a third party, such as monitors, MRI machines, smartphones, heart rate and other phenomenon measuring gadgets, and so on.

- Body data such as temperature, heart rate, blood pressure, electrocardiogram, and many others can be collected by using the aforementioned instruments.

The rest web service provides a straightforward interface for sensors to communicate with the cloud and retrieve the information they need. The cloud server provides high-powered machines with lots of CPU, computation power, RAM, GPU, and enough network bandwidth so that data can be managed quickly and globally through a wide variety of interfaces (such as PCs, TVs, and smartphones). To ensure safe computation and communication, a Blockchain cloud layer sits atop the control layer's public data.

In order to aggregate data and collaborate on it, the blockchain technology keeps track of data usage patterns and maintains data validity. Our system takes care of the requisite data, processes it, and sends back the results when a data user applies it. As data ownership can be separated and permissions can be granted, data rotation can be made safe and easy to manage. To what extent a model performs well when labels are applied to training data depends heavily on the quality of the training data. In order for the FL model to be able to learn and compile the raw data, it must be labelled with relevant identifiers. The three methods of label assignment are as follows:

- Adding data items to a dataset with labels already allocated;
- Assigning labels to data items using a console; and
- Adding labels to data items manually.

Using universal data Centre, uniform information acquisition with FL with multi-lateral computing is finished. While users' data is safely stored in a private data centre, FL uses data calculations instead of raw data to ensure privacy. Through advanced analysis and practical applications, computational logic facilitates research into linguistic tensions. Additionally, the data analyst examines both recent and old healthcare data in order to forecast patterns and lines of data and enhance outreach as represented in Figure 3.

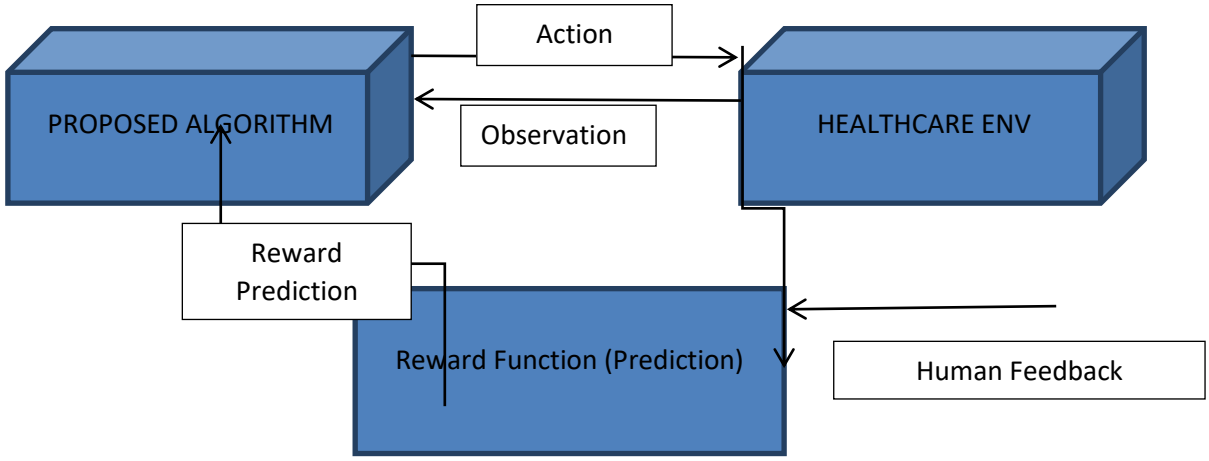


Figure 3.Modified Reward Function

Algorithm 1: Modified Reward Function
Input: Optimal Value (OP_V)
Output: Determine the maximum value function'
Defining the function for Optimal Value (OP_V)

```
While True
    QLearning = 0;
        For t in array (env.NodeB)
Value.tb = np.zero (env.NodeB)
        For b in array (env.NodeB)
            For prob_t, succeed formal, Reward function, _in env.P[t][B]
Q_tb[B] + = R(Ent, ImRewardt)
        Max. costTask_t = np.max(Q_tB)
```

Whereas,
R(Ent, ImRewardt) = S_1, S_2, S_3, and S_4

$$R(Ent, ImRewardt) \rightarrow [S1 * (UD / UDmax)] - [S2 * (E / Emax)] - [S3 * (L / Lmax)] - [S4 * (FP / FPmax)]$$

Whereas,

S → Scaling Factors;
UD ←Unit Data;
E ←Device used for energy consumed per unit;
L ←Latency total
Based on device cost, final payment → FP

V. PERFORMANCE ANALYSIS

According to the performance analysis, Analysed is made on the enactment of the proposed Hy-FL based Blockchain grounded on confident parameters such as, data accuracy, data precision, data privacy, scalability & malicious activity. Those parametric value is compared with other thee algorithms such as, CNN-BC-Cryo-FL; KCDP and SSEA.

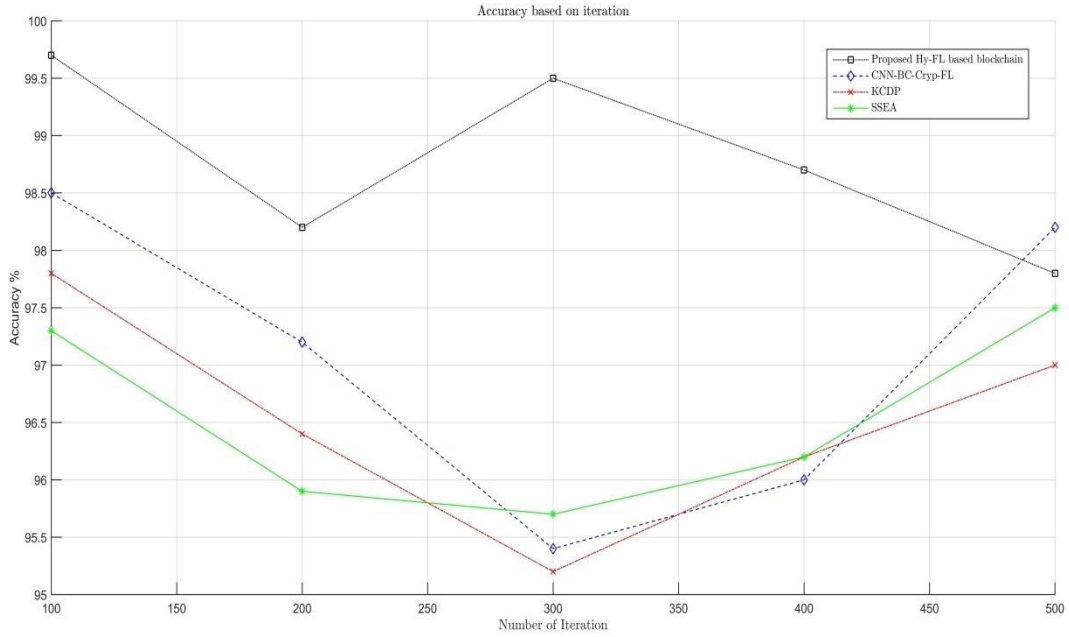


Figure 4. Number of Iteration Vs. Accuracy

In Figure 4, the accuracy among the information based on healthcare is calculated with the variation on iteration from 100 to 500. The proposed one has attain percentage level between 92 t0 96 and it outperforms better than the existing ones such as, CNN-BC-Cryo-FL; KCDP and SSEA.

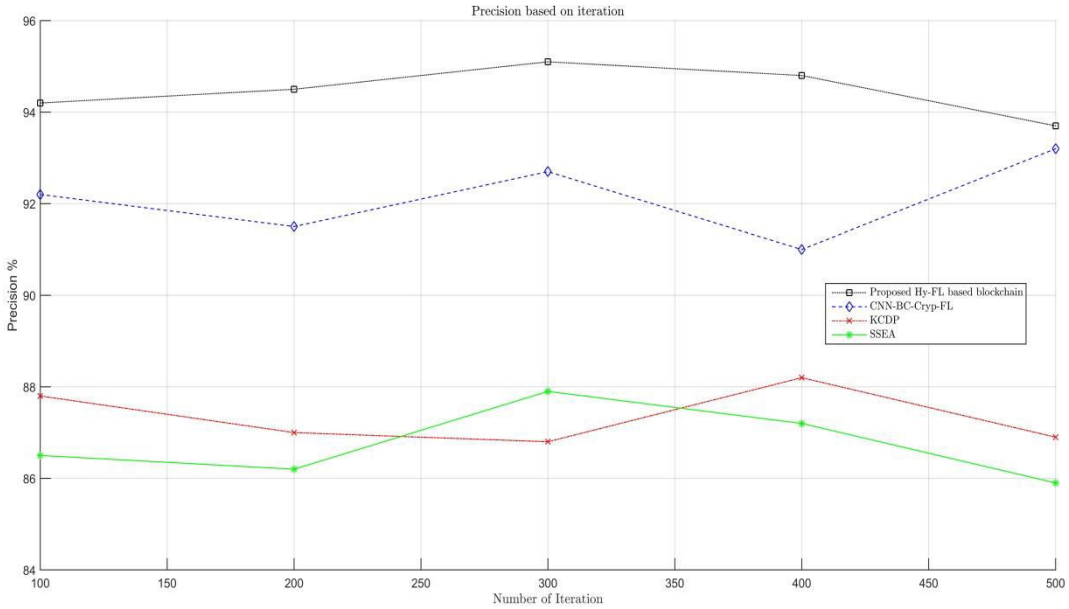


Figure 5. Number of Iteration Vs. Precision

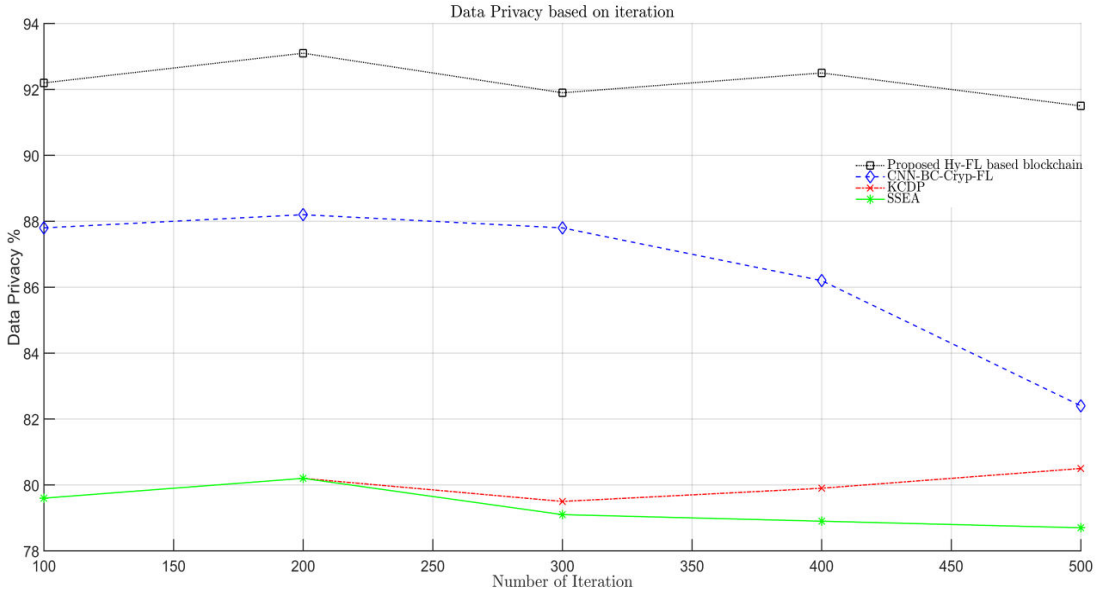
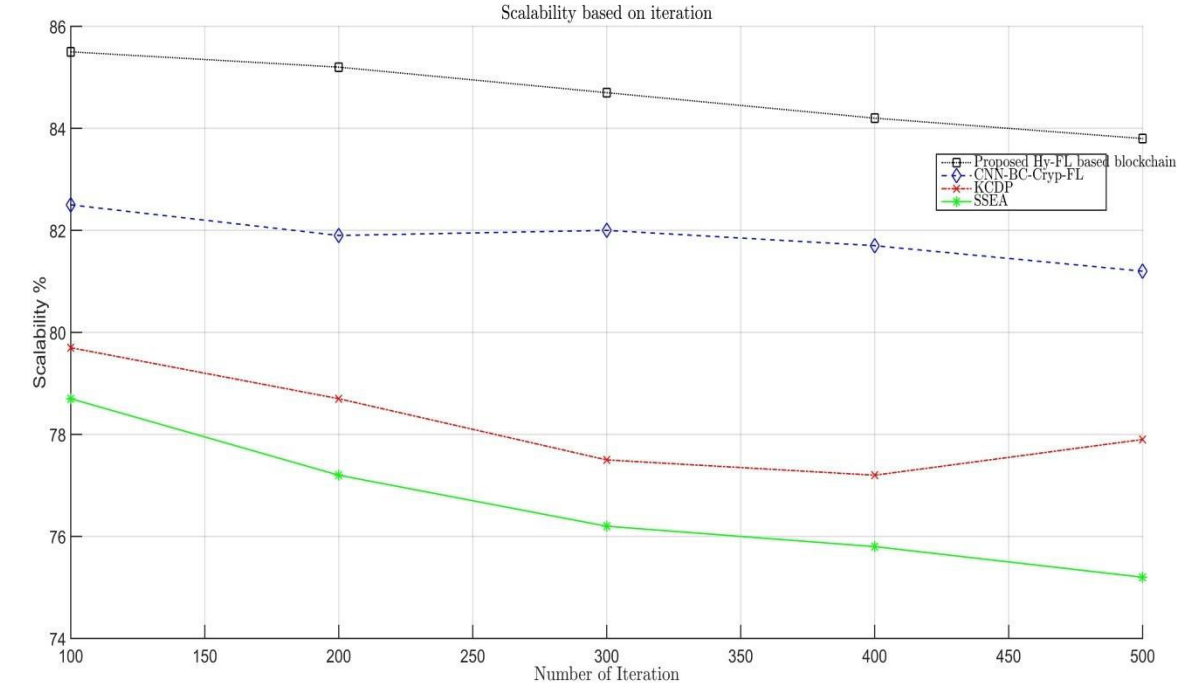


Figure 6. Number of Iteration Vs. Data Privacy

In Figure 6, the data privacy is calculated based on the variation from 100 to 500 as the data occurs in the healthcare organization. The data privacy value analysed between 82 to 86 percentages for the proposed one as compared to the existing ones.



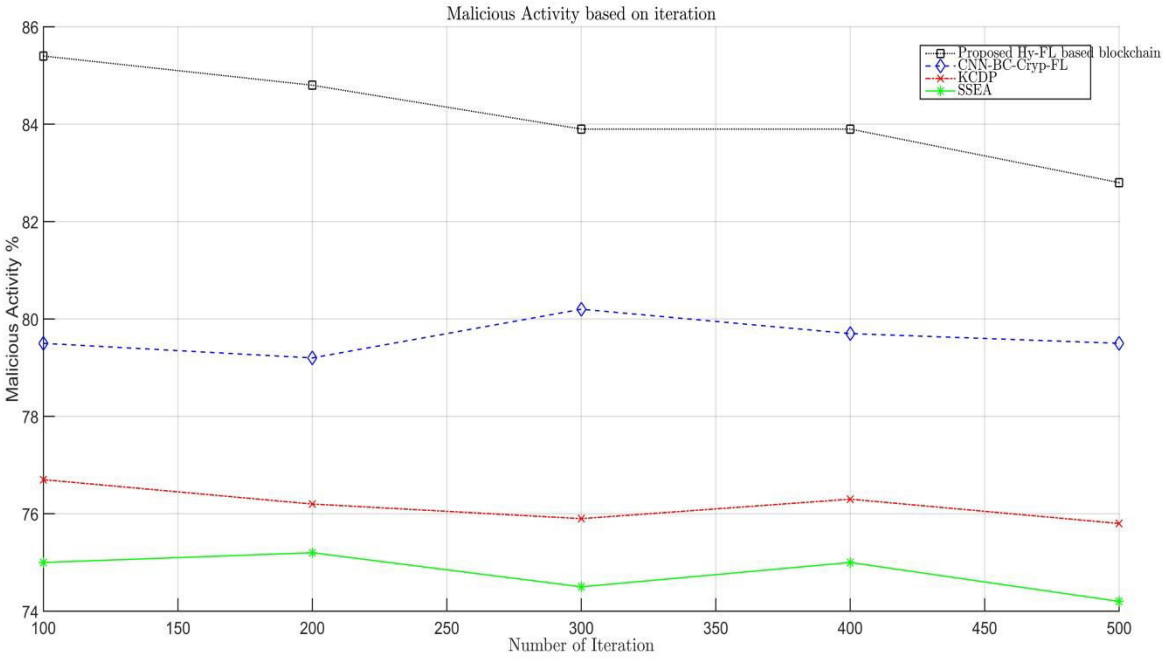


Figure 7. Number of Iteration Vs. Scalability

Figure 8. Number of Iteration Vs. Malicious Activity

Based on the figure 7, the data scalability is attained using the variation in the number of iteration from 100 to 500. The scalability value gets improved for the proposed one and malicious activity gets improvement also attained as it is represented in figure 8. The proposed one is compared with the existing ones such as, CNN-BC-Cryo-FL; KCDP and SSEA.

VI. CONCLUSION

Deep learning is a game-changer for machine learning because it allows for greater scalability, security, and privacy. Secure data cooperation for its cloud computing ecosystem was further attained by the scheme replicated relying cryptographic cloud environment. The FL training mechanism safeguards patient confidentiality by confining sensitive information to regional organisations; this is achieved through the model's client-server architecture. Also, it's easy to implement, extensible, and compatible with other 5G systems. Through effective broker management, cloud computing service providers increase the benefits for healthcare users. And a decentralised network that is both scalable and powered by Blockchain technology makes it possible for potentially unreliable nodes to communicate with one another. The success of Blockchain and FL technology is essential for end-device privacy in this study. However, with the creation of a trust model based on blockchain technology and the introduction of a novel consensus approach to maintaining FL nodes, this restriction on relying solely on the protocol will be lifted. Future plans include cutting down on wait times and data storage requirements. Furthermore, we will design the user device's incentive system and trust level.

References:

[1]. EthemAlpaydin, Introduction to Machine Learning, MIT Press, 2020.

[2]. V. Sharma, I. You, K. Andersson, F. Palmieri, M.H. Rehmani, J. Lim, Security, privacy and trust for smart mobile-internet of things (M-IoT): A survey, IEEE Access 8 (2020) 167123-167163.

[3]. W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, Y.C. Liang, Q. Yang, D. Niyato, C. Miao, Deep learning in mobile edge networks: A comprehensive survey, IEEE Commun. Surv. Tutor. (2020).

[4]. Qiang Yang, Yang Liu, Tianjian Chen, Yongxin Tong, Deep machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. (TIST) 10 (2) (2019) 1–19.

[5]. G.A. Kaissis, M.R. Makowski, D. Rückert, R.F. Braren, Secure, privacy preserving and deep machine learning in medical imaging, Nat. Mach. Intell. (2020) 1–7.

[6]. FiammettaMarulli, Emanuele Bellini, Stefano Marrone, A security-oriented architecture for deep learning in cloud environments, in: Workshops of the International Conference on Advanced Information Networking and Applications, Springer, Cham, 2020, pp. 730–741.

[7]. Z. Li, V. Sharma, S.P. Mohanty, Preserving data privacy via deep learning: Challenges and solutions, IEEE Consumer Electron. Mag. 9 (3) (2020) 8–16.

[8]. S. Singh, P.K. Sharma, B. Yoon, M. Shojafar, G.H. Cho, I.H. Ra, Convergence of Blockchain and Artificial Intelligence in IoT Network for the Sustainable Smart City, Sustainable Cities and Society, 2020, p. 102364.

[9]. BordelBorja, Alcarria Ramon, Martin Diego, Sanchez Picot Alvaro, Trust provision in the internet of things using transversal blockchain networks, Intell. Autom. Soft Comput. 25 (1) (2019) 155–170.

[10]. Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, ``Deep learning for data privacy preservation in vehicular cyber-physical systems," IEEE Netw., vol. 34, no. 3, pp. 50-56, May 2020.

[11]. M. Elkhodr and B. Alsinglawi, ``Data provenance and trust establishment in the Internet of Things," Secur. Privacy, vol. 3, no. 3, pp. 1-11, May 2020, doi: 10.1002/spy2.99.

[12]. M. Heikkil, A. Koskela, K. Shimizu, S. Kaski, and A. Honkela, ``Differentially private cross-silo deep learning," vol. 1, no. 1, pp. 1-14, 2020.

[13]. M. S. Hossain and G. Muhammad, ``Cloud-based collaborative mediaservice framework for HealthCare," Int. J. Distrib. Sensor Netw., vol. 10,no. 3, Mar. 2014.

[14]. G. Muhammad, M. S. Hossain, and N. Kumar, ``EEG-based pathologydetection for home health monitoring," IEEE J. Sel. AreasCommun., early access, Aug. 31, 2020.

[15]. V. Sharma, I. You, F. Palmieri, D.N.K. Jayakody, J. Li, Secure and energyefficienthandover in fog networks using blockchain-based DMM, IEEECommun. Mag. 56 (5) (2018) 22–31.

[16]. Xin Jiang, Mingzhe Liu, Chen Yang, Yanhua Liu, Ruili Wang, A blockchainbasedauthentication protocol for WLAN mesh security access, Comput.Mater. Contin. 58 (1) (2019) 45–59.

[17]. A. Bhowmick, J. Duchi, J. Freudiger, G. Kapoor, R. Rogers, Protection againstreconstruction and its applications in private deep learning, 2018.
[18]. Sana Awan, Fengjun Li, Bo Luo, Mei Liu, Poster: A reliable and accountable privacy-preserving deep learning framework using the blockchain. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2561–2563. 2019.
[19]. Nicola Rieke, Jonny Hancox, Wenqi Li, FaustoMilletari, Holger R. Roth, ShadiAlbarqouni, SpyridonBakas, et al., The future of digital health with deep learning, NPJ Digital Med. 3 (1) (2020) 1–7.
[20]. Saurabh Singh, Pradip Kumar Sharma, Byungun Yoon, Mohammad Shojafar, Gi Hwan Cho, In-Ho Ra, Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, Sustainable Cities Soc. 63 (2020) 102364.
[21]. Jieren Cheng, Jun Li, NaixueXiong, Meizhu Chen, HaoGuo, Xinzhi Yao, Lightweight mobile clients privacy protection using trusted execution environments for blockchain, CMC-Comput. Mater. Contin. 65 (3) (2020) 2247–2262.
[22]. YongjunRen, Yan Leng, Jian Qi, Pradip Kumar Sharma, Jin Wang, ZaferAlmakhadmeh, AmrTolba, Multiple cloud storage mechanism based on blockchain in smart homes, Future Gener. Comput. Syst. 115 (2021) 304–313.
[23]. Jieren Cheng, Jun Li, NaixueXiong, Meizhu Chen, HaoGuo, Xinzhi Yao, Lightweight mobile clients privacy protection using trusted execution environments for blockchain, CMC-Comput. Mater. Contin. 65 (3) (2020) 2247–2262.
[24]. Bo Yin, Hao Yin, Yulei Wu, Zexun Jiang, FDC: A secure deep deep learning mechanism for data collaborations in the internet of things, IEEE Internet Things J. 7 (7) (2020) 6348–6359.
[25]. E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, O.Y. Song, A.K. Bashir,A.A. Abd El-Latif, DITrust chain: towards blockchain-based trust models forsustainable healthcare IoT systems, IEEE Access 8 (2020) 111223-111238.
[26]. X. Guo, H. Lin, Y. Wu, M. Peng, A new data clustering strategy for enhancingmutual privacy in healthcare IoT systems, Future Gener. Comput. Syst.113 (2020) 407–417.
[27]. A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacypreservinghealthcareblockchain for IoT, Sensors 19 (2) (2019)326.
[28]. S.M. Razavi, D. Yuan, F. Gunnarsson, J. Moe, Exploiting tracking area listfor improving signaling overhead in LTE, in: 2010 IEEE 71st VehicularTechnology Conference, IEEE, 2010, pp. 1–5.