Threats and Protections for Machine Learning In Healthcare Systematic Intoxication

Dhrisya Shadevan[1], Sriram Surya Shanmuga sundaram[2], Ponmythili Sundar[3], Radha Viswanaathan[4]

[1,4] Assistant Professor, Department of Computer Science and Engineering, V.S.B College of Engineering Technical Campus, Coimbatore
[2]Assistant Professor, Department of Electronics andCommunication Engineering, Rathinal Technical Campus, Coimbatore
[3]Assistant Professor, Department of Computer Science and Engineering RVS Technical Campus , Coimbatore

Abstract:
Machine learning is being used to uncover patterns in massive datasets across a wide range of application domains. Machine learning findings are increasingly driving crucial decisions in healthcare and biomedical applications. Because health-related apps are frequently sensitive, any security breach would be disastrous. The accuracy of the findings produced by machine learning is, of course, critical. According to recent research, some machine-learning algorithms can be hacked by supplementing their training datasets with harmful material, resulting in a new type of assault known as poisoning attacks. A delay in receiving a diagnosis could be life-threatening and generate distrust. On the other hand, a false positive classification may not only cause users to doubt the machine-learning algorithm and potentially quit the entire system, but it may also cause patient suffering. The suggested attack process provides input data that, when added to the training set, can either cause targeted errors. These attacks can be used on both static and dynamic datasets. Data mining was the most efficient one for identifying undiscovered positive regularities that could aid an organization's efficiency. For many firms, data mining abilities are becoming increasingly vital. Data mining assists in the discovery of previously undiscovered and very profitable data in large amounts of data. Database learning exploration's main goal was to find new patterns in a large amount of data. The emergence of inherent design modifications for Electronic Health Records (EHRs) has typically been hampered by a long-standing emphasis on compliance. As customization and data science encourage individuals to participate in the details of their medical and reclaim control over their health information, we are in desperate need of such technology. We suggest MedRec, a revolutionary, decentralized record management system that uses blockchain technology to manage EHRs, in this study.

Keywords: Machine learning, healthcare, biomedicine, poisoning attacks

1. Introduction

Health issues have an impact on people's life. During medical treatment, health care workers collect medical evidence about each individual patient and apply population in general information to decide how to manage that patient. As a result, data serves a critical role in resolving health issues, and better data is critical to enhancing patient care. A. Rozyyev et al (2011) have illustrate that Deep learning has aided advancements in a variety of fields, including machine vision, natural language processing, and automatic speech recognition, by utilising data. The potential of machine learning to retrieve data from information, combined with the

importance of data in the healthcare, makes deep learning research for healthcare critical. Despite significant initiatives, the direct implementation of machine learning to healthcare persists fraught with drawbacks, such as work in diagnosing diabetic retinopathy, sensing lymph node metastatic disease from breast pathology, autism subtyping by clustering comorbidities, and largescale phenotyping from observational data. Many of these issues arise from healthcare's stated goal of making tailored forecasts using data collected and managed by the health service, where data gathering serves primarily to assist care rather than to enable subsequent analysis. Halatchev et al (2008) have Established medical machine learning studies have concentrated on biological applications, machine learning problems ideally suited for medical, the requirement for transparency, and Arampatzis et al (2005) expained the use of large data in accurate medicine. Here, we focus on the wide range of opportunities that machine learning offers for healthcare, as well as the critical choices that must be addressed. While Tseng et al (2006) have choose to concentrate on the inpatient context since it is the most data-rich situation at the moment, we should emphasise that clinical data is diverse and offered in a range of ways that can be useful in understanding patient health.

The unique technological constraints that should be considered in machine learning systems for healthcare activities are discussed in this paper, particularly when the gap between trained modeling and simulation specialists narrows. Yairi et al (2001) have evaluate these issues adequately can jeopardise the validity and effectiveness of deep learning in healthcare. We provide a taxonomy of clinical opportunities, which are divided into three broad categories: clinical job automation, clinical assistance, and clinical capacity expansion. Umadevi et al v (2020) Finally, discuss the opportunities for machine learning research in healthcare, including adapting to changes in data sources and procedures, ensuring algorithms are interpretable, and discovering good representations. ML algorithms have the ability to be profoundly engaged in all sectors of medicine, from drug development to clinical decision making, dramatically transforming how medicine is done. Between 2006 and 2011, the use of EHR doubled among office-based physicians in the United States, from 12% to 40%. Medical images are an important aspect of a patient's electronic health record (EHR) and are presently evaluated by human physicians, who are constrained by their speed, weariness, and experience. Umadevi et al (2020) have demonstrate that, It requires years and a lot of money to train a trained radiologist, hence some health-care organisations use tele-radiology to outsource radiology reporting to lower-cost countries like India. The patient suffers from a delayed or incorrect diagnosis. As a result, using an automated, reliable, and quick machine learning system to do clinical image analysis is excellent.

Data-intensive methodologies are being adopted in a variety of fields of medicine, resulting in more evidence-based decision-making and assisting in the transition to personalised medicine: The ability to adapt judgments, practises, and treatments to the particular patient is a major goal of modern biomedicine. Anita Priscilla Mary et al (2020) have evaluate that customised medicine is the ideal objective, stratified medicine is the current method, which seeks to find the optimal treatment for groups of patients with similar biological traits. ML methods, such as CIT and aggregated grouping, are essential in this case, as are strategies for deploying such stratified approaches. Uma Devi et al (2019) have Studied the individual treatment effects with ensemble CITs can provide a deeper understanding of individualised treatment. The growing volume of heterogeneous data sets, particularly "-omics" data from genomics, proteomics, metabolomics, and other fields, makes traditional data analysis difficult and knowledge discovery tool optimization essential. Many huge data sets, on the other hand, are actually large aggregates of small data sets. Mercy Beulah et al (2015) have examined the medicine which is especially true in customised medicine, where there may be a lot of data yet just a limited amount of data for each patient. This is known as model personalization, and it is easily accomplished by employing hierarchical Bayesian methods such as hierarchical Dirichlet processes. Bayesian multi-task learning, for instance.

2 . PROPOSED SYSTEMS

The proposed solution for electronic medical record exchange, which is based on the ethereum blockchain, is described in this section. As a consequence, a blockchain-based EHR trading market architecture is proposed. Many methodologies and variables are utilized in the network for log operations. On the suggested approach,

the EHR can be propagated to other users in the blockchain network utilizing a shared secret key and asymmetric key.

Proposed algorithms

Admin, patients, doctors, and lab technicians are among the 4 types of users in the EHR trading system. Algorithm 1 depicts the accurate implementation of admin in a blockchain system.

Algorithm 1 Algorithm on Admin Working.

Input: Enrolment Certificate (E_C) requested from Certification Authority (C_A)
Output: Access to P_{HL}. C_{HL} and L_{HL} transactions for all (P_{HL}. C_{HL}. L_{HL}) ϵ B_N
Initialization: N_{Admin} should be valid node. N_{Admin} can Write/Read/Update/Remove nodes C_{ID}. P_{ID}. L_{ID}

```
procedure ADMIN( P_ID. C_ID. L_ID)
    while (True) do
        if (C_ID is valid) then
            Add_Clinician to the blockchain Network
            Add_Clinician(B_N. C_ID)
            Grant_access(C_ID. U_Name. P_K)
        else
            Not_exist(C_ID)
        end if
        if (P_ID is valid) then
            Add Patient to the blockchain Network
            Add_Patient(B_N. P_ID)
            grant_access(P_ID. U_Name. P_K)
        else
            Not_exist(P_ID)
        end if
        if (L_ID is valid) then
            Add Lab to the blockchain Network
            Add_Lab(B_N. L_ID)
            grant_access(L_ID. U_Name. P_K)
        else
            Not_exist(L_ID)
        end if
    end while
    int N; {0 means bad behaviour. 1 means good behaviour}
    for all (..) do
        if (behaviour_node(N) then
            Not update(C_ID. P_ID. L_ID)
        else
            Remove_update(C_ID. P_ID. L_ID)
        end if
    end for
end procedure
```

The admin's registration license is requested from the certifying agency. The administrator has full power over the system, including the ability to write, read, update, and remove users. Admin can provide each member a proper ID to permit connectivity to the blockchain system if doctors, patients, or lab employees are genuine. If a participant's behavior is deemed inappropriate, the administrator can ban them from the hyperledger ethereum blockchain by leaving a remark. The patient module's methodical implementation is depicted in Algorithm 2.

Algorithm 2 Algorithm on Patient Working.

Input: I_D and key requested from N_{admin}
Output: Get access to P_{HL} transactions
Initialization: P_{HL} should be valid node. P_{HL} can Read/Write/Grant/Revoke EHR records.

```
procedure PATIENT(P_ID)
    while (True) do
        if (P_ID ∈ B_N) then
            if (P_REC_I not B_N) then
                Create_records(P_ID, P_REC_I, B_N)
            else
                Update_records(P_ID, P_REC_I, B_N)
                Read_records(P_ID,P_REC_I, C_ID, L_ID, B_N)
            end if
        else
            Not_exist(P_ID)
        end if
        if Visit(P_ID, C_ID, L_ID, B_N) then
            M_PID = Medrecord(P_ID)
            if thenM_PID ∈ P_HL(B_N)
                Grant_records(M_PID, C_ID, L_ID, B_N)
            else
                (C_ID, L_ID) ← NOTIFY("Medical record does not exist")
            end if
            if (M_PID ∈ C_ID, L_ID Treatment_completed(P_ID)) then
                Revoke_records(M_PID, P_REC_I, C_ID, L_ID,B_N)
            else
                (C_ID, L_ID) ← NOTIFY("P_ID voluntary revoke M_PID")
                Revoke_records(M_PID, P_REC_I, C_ID, L_ID,B_N)
            end if
        else
            Not Visit
        end if
    end while
end procedure
```

In this situation, the patient node requests a private key to gain access to network resources. After being granted entry to the blockchain network, the patient gains several abilities, such as the ability to write, view, and remove EHR records. In this way, the identifier of the patient node in the blockchain network is utilized. If the patient has a legal node, the data of the patient, doctor, and lab staff can be viewed or accessed across the internet. M PID can offer the physician node authorization to view and modify the patient's health records on the ethereum blockchain if M PID is a part of the patient's hyperledger community. If the patient does not want their information to be publicized after the therapy is completed, the patient can delete access from the lab member of staff or doctor in the system. [20] argues that if M PID is in the doctor or lab staff hyperledger network, the client can use the calling mechanism to renounce membership to the blockchain network. Alternatively, the patient might inform the doctor or lab personnel by voluntarily canceling access and then using the calling method. Algorithm 3 shows the exact working of the clinician component.

Algorithm 3 Algorithm on Clinician Working.

Input: I_D and key requested from N_{admin}
Output: Get access to C_{HL} transactions
Initialization: C_{HL} should be valid node. C_{HL} can Read/Write Permissioned EHR records by the patients and write medical records of the patients.

```
procedure CLINICIAN(C_ID)
    while (True) do
        if C_ID ∈ B_N) then
            if (Granted M_PID ∈ C_ID then
                Read_records(C_ID, P_REC_I, M_PID, B_N)
                Update_records(C_ID, P_REC_I, M_PID, B_N)
            else
                Write_records(C_ID, M_PID, B_N)
                Read_records(C_ID, L_ID, B_N)
            end if
        else
            Not_exist(C_ID)
        end if
    end while
end procedure
```

In the input step, the physician requests a key from the network administrator to allow login. During the output step, the clinician has access to clinician hyperledger events. It's best to utilize a real node. The physician has entry to the patient's medical records if C ID is a part of the blockchain network. After that, the practitioner has access to and control over the system's permission EHR. If the doctor does not have knowledge to the patient's IDs, they can use the hyperledger system to write data. A doctor can also use the network to find available doctors and laboratory personnel. Algorithm 4 depicts the orderly implementation of laboratory work.

Algorithm 4 Algorithm on Lab Working.

Input: I_D and key requested from N_{admin}
Output: Get access to L_{HL} transactions
Initialization: L_{HL} should be valid node. L_{HL} can Read/Write Permissioned EHR records by the patients.

```
procedure LAB(L_ID)
    while (True) do
        if L_ID ∈ B_N) then
            if (Granted M_PID ∈ L_ID then
                Read_records(L_ID, P_REC_I, M_PID, B_N)
                Write_reports(L_ID, P_REC_I, M_PID, B_N)
            else
                Read_records(L_ID, L_ID, B_N)
            end if
        else
            Not_exist(L_ID)
        end if
    end while
end procedure
```

The system administrator is asked by laboratory personnel for the private key. The hyperledger connectivity access is granted if the node is deemed valid as a consequence of the input query. The lab node works in the same way as the physician node. The lab network may receive health information and provide reports depending

on patient tests including blood and immunity levels. This router can also look for accessible lab staff and doctors across the whole network.

Evaluation phase

Pre-processing

Evaluation is essential for assessing system flexibility and efficiency in a systematic manner. The pre-processing stage is the first step. The Wire-shark pcap file can be used to get all network traffic. This examines all network traffic and only filters out TCP messages sent across hyperledger fabric. All interaction in the system is performed via the gRPC protocol, which operates on top of TCP.

Reporting

The evaluation is carried out using the spyder IDE, which runs on the Anaconda browser. It makes use of matlablib, a program that allows you to visualize statistical data. It also incorporates pandas3, a data processing and manipulation tool. The python3 program code is used to build graphs in the evaluation process. Wireshark is also used to gather data traffic, which is saved in a pcap file that contains all TCP packets, propagation times, origin line, and destination ip. All network IPs are replaced with the hyperledger calliper and peer organization node identities for better visualization. All of the operations that are run throughout the study, such as transaction send rate, delay, throughput, organizations, peers, maximum CPU utilization, and storage space, are recovered and assessed for translation in an HTML caliper file. Matlablib is then used to display the data in several ways. Test methods are reported to demonstrate the EHR system's performance and to provide insight into the Hyperledger Fabric requirements for the evaluation process. This article models a variety of application situations, including one organization versus. one peer, two organizations vs. one peer, three organizations vs. one peer, two organizations vs. two peers, and three organizations vs. two peers. Each organization in the network has a no. of ledger peers, each of which holds a copy of the ledger. A single orderer host is in charge of block generation, whereas the Caliper host is in charge of workloads. As a consequence, each host is a member of the star topology and conducts the observations and assessments shown in Figure 3.

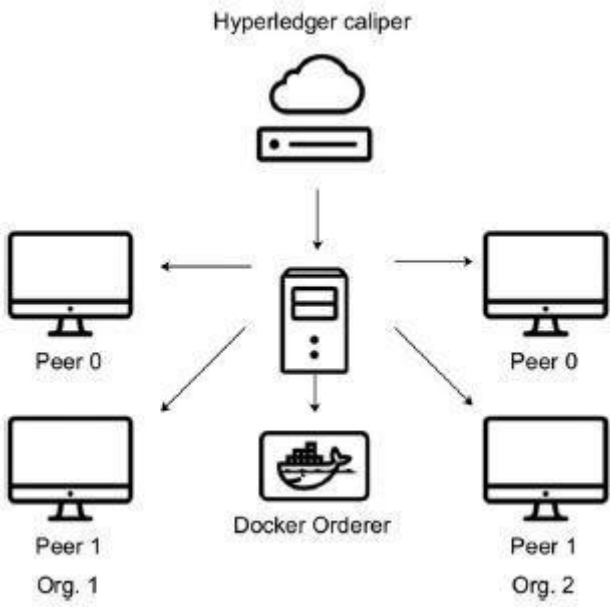

Fig. 1. Network structure

3. RESULTS AND DISCUSSION

***Decryption and Encryption*:**

The message should be displayed on the arc in encryption. Figure 2 shows the proposed protocols. Big data implementation is included in the encrypted text. Examine the 'M' point on the 'E' curve form.' Select 'k' from the list at random;

$$[1 - (n\text{-}1)] \quad (1)$$

C1 and C2 are the two cypher texts that will be created.

$$C1 = k*P \quad (2)$$

$$C2 = M + k*Q \quad (3)$$

C1 and C2 will be the ones to send.

Decryption refers to recovering the message m that was sent to the customer.

$$M = C2 - d * C1 \quad (4)$$

M was the original message which was sent to all.

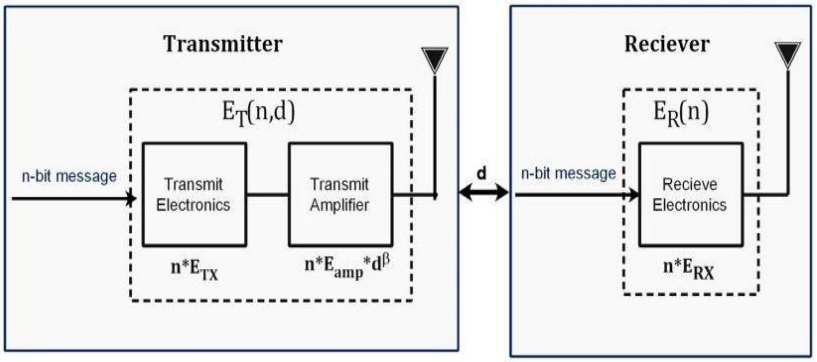

Fig. 2 Proposed protocols

***Throughput ratio*:**

The number of successfully sent packets from origin to target per second is the throughput of a wireless sensor network. The value of a well-designed network must be high, and if it is focused, the value of throughput will be reduced. Figure 3 displays the throughput ratio.

Table 1 Simulation Results

Factors	Malicious node	Simulation Time	No. of Nodes	Protocol	Operating Platform	Packet	Simulator
Quantity	1	100000ms	10	AODV	Ubuntu	TCP	NS-2.3

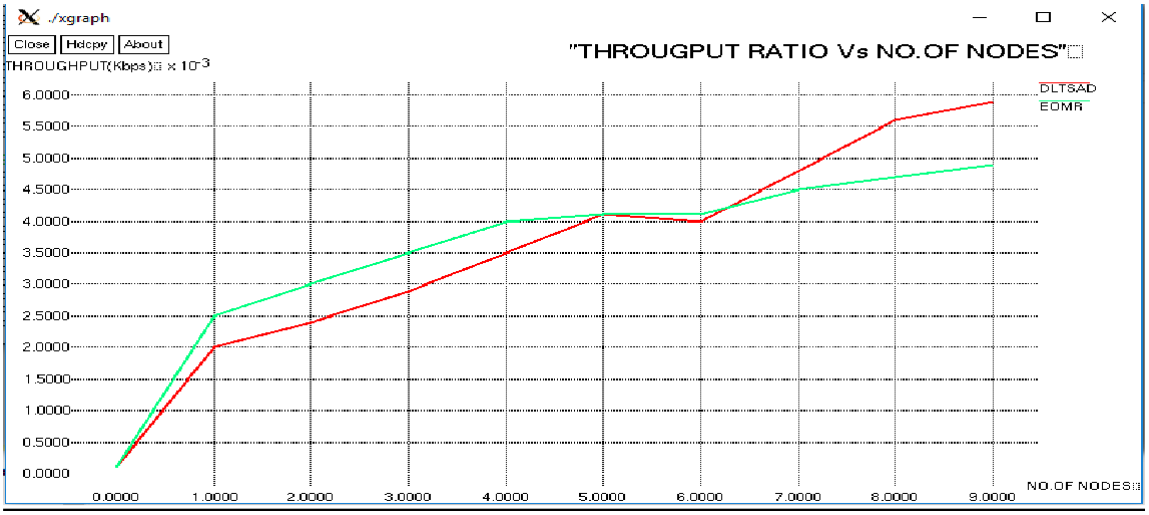

Fig. 3 Throughput ratio

PDR:

PDR is the percentage of total packets transported from an origin node to a target node in a network. The target must be bombarded with as many data packets as feasible. The network output increases in lockstep with the PDR value. PDR is measured by evaluating the network before and after the danger of a black hole. When compared to before the intrusion, the packet delivery ratio was found to be significantly low, implying that fewer transmissions were sent to the sensor nodes. Figure 4 illustrates the graph of PDR.

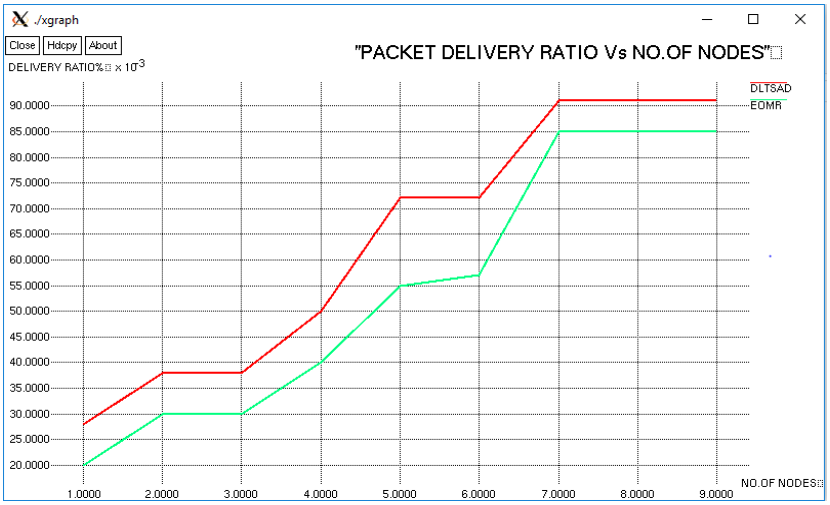

Figure 4 PDR

Energy Consumption:

Energy characterization is essential for determining the needs of a high-volume data process that functions smoothly on mobile devices. The energy consumption of DM algorithms operating on mobile devices is investigated experimentally in this study. Figure 5 shows the graph of energy consumption.

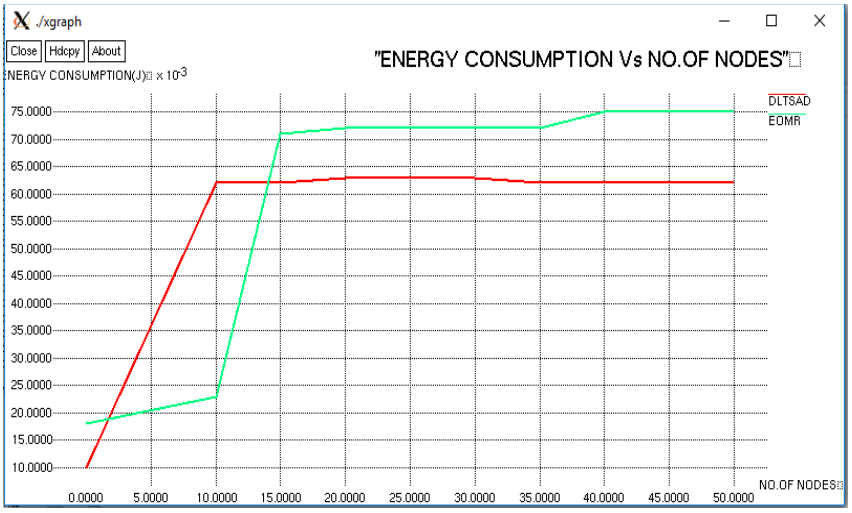

Figure 5 Energy Consumption

E-E delay:

The packet's E-E latency is the sum of delays experienced at each intermediary node along the path to the target. Each delay is made up of a set transmission and propagation delay as well as a variable analysis and waiting time at the nodes. Figure 6 shows the End to End delay.

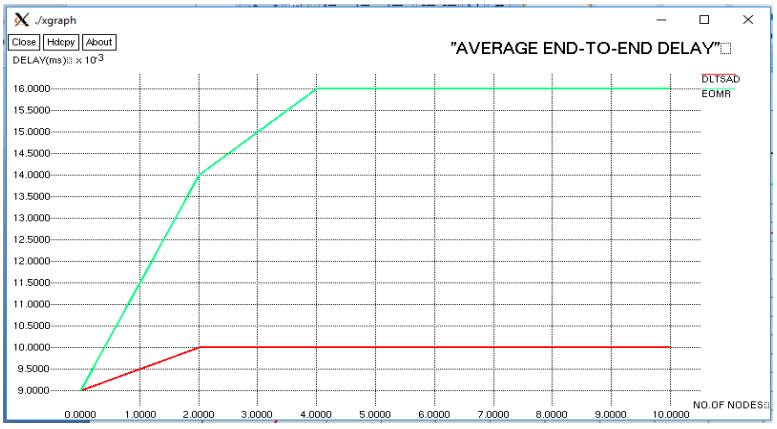

Fig. 6 E-E delay

4. BLOCKCHAIN CASE ANALYSIS IN ENERGY INTERNET

The concept of blockchain technology and its construction method are comparatively well-established, and research data about the determined and analyzed of energy usage have been collected. In the meantime, blockchain is increasingly being used for data security just on energy internet. This section looks at several initiatives' potential for using blockchain to increase data security.

Case 1: Interconnection of Device-to-Device Information

In order to solve the issue of informational connection among devices, the International Business Machines Corporation and the Samsung Group developed ADEPT (autonomous decentralised peer-to-peer telemetry), a blockchain-based internet of things. The system's three parts are BitTorrent, Ethereum, and TeleHash. A protocol for transmitting data is called BitTorrent. It can make sure that networking volatility is avoided and that information propagation characteristics are preserved. A transit cryptography library called TeleHash is used for

application interfaces for controlling equipment and variables. These components can be used to automate contract implementations, register and certify devices, develop interaction rules based on the consensus mechanism, and complete other activities. The Adept system handles shared storage and keeps a record of the connections between participants when data is transmitted between devices. A variety of protocols can be used by the Adept system to establish a bridging data connection between devices. The device's self-describing file inside the blockchain can help it better comprehend how other gadgets work. In other words, it enables the system to record their communications with the user and other devices. Figure 7's representation of the Adept system demonstrates how intelligent washing machines can interact with other devices.

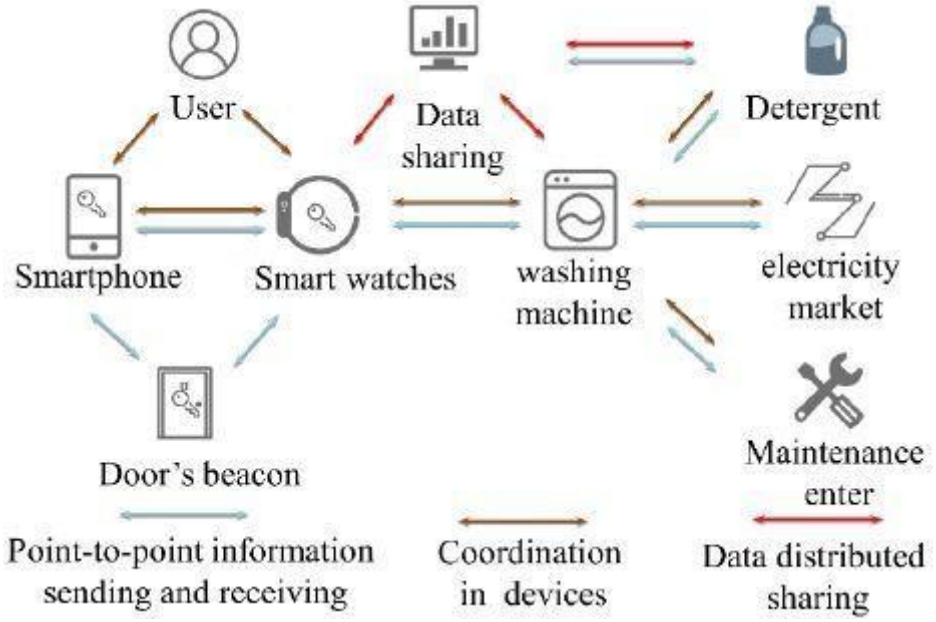

Figure 7. ADEPT system application.

Case 2: Monitoring Device Operation

The blockchain in Figure 8 is the hub of the filament, an IoT technology stack that provides each device a unique personality. The two main hardware components are the Filament Tap and Filament Patch. The Filament platform supports 5 protocols in total, including BitTorrent, Pennybank, Smart contracts, Blockname, and TeleHashes. The first three protocols are necessary for Filament Tap to work, and as a technological advancement, the user can choose a new pair of protocols. Blockname generates a unique identification in the embedded chip of the device and stores it on the blockchain. TeleHash offers peer-to-peer encryption techniques. BitTorrent enables file sharing. A hosted platform from Penny Bank enables two linked devices to settle transactions with each other while online. The ideal connection between the internet and other devices is made possible by the development of an intelligent device directory. Utilizing blockchain technology, filament updates the transmission mechanism used in the normal traditional grid. By placing a series of "taps" for sensory tracking and creating a corresponding communication system, the poles are transformed into a digital node. It might be able to regulate how the equipment works based on the information broadcast and traded in the blockchain system. The smart digital pole would submit a real-time event report to the blockchain and notify the maintenance team to remedy the issue if it caught on fire or started to tilt. The duties of the malfunctioning pole will be assumed by the closest working pole in the interim. Smart digital wires can track their state and share data to diagnose and locate issues. If the digital node discovers any irregularities, the monitoring system will transmit a status alert.

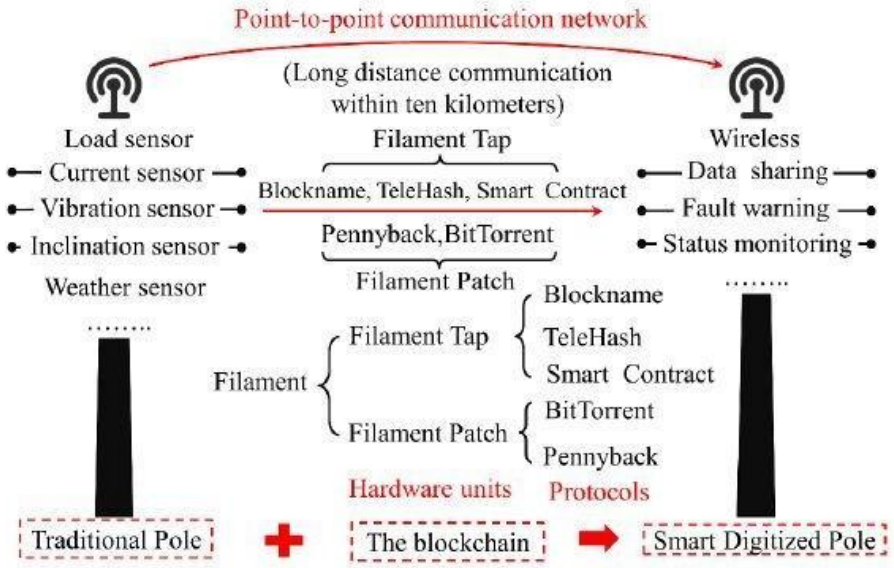

Figure 8. Blockchain implementation in the Filament project's communication poles.

Case 3: Direct and Free Trade Among Micro-grid Users

The transactive grid, a trading platform created by the Lo3 power and consensus systems, is depicted in Figure 9. Solar-powered electricity is produced by project participants' homes' smart metres, which are connected to the blockchain. The smart metre can monitor flow of energy both from the energy supplier and the consumers to keep a steady balance between supply and demand. Energy exchange can be carried out automatically using a smart contract. Participants are free to conduct transactions without the assistance of third parties. Additional power can be delivered directly to users or returned to the grid, depending on the situation. Blockchain-based smart metres can trace energy flow and enable autonomous energy trading. Trusted metering and authentic certification are required for secure and trustworthy transactions. The blockchain's technical properties can assure authority. More crucially, the blockchain can broaden the transaction's reach. Once the trade conditions are met, the authentication method can be used to create trading streams without requiring participants to trust each other.

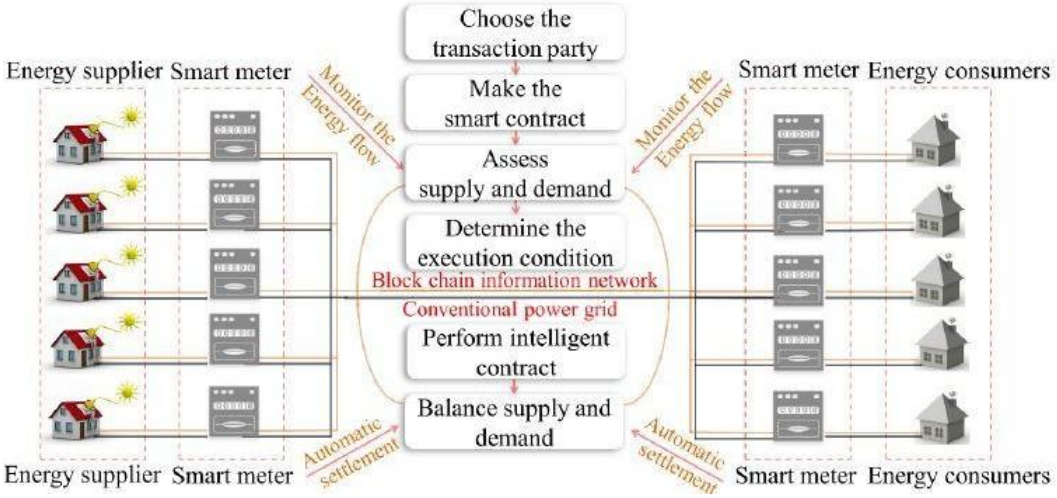

Figure .9 Application of blockchain technology in a smart community's energy market.

5. CONCLUSION

This article examines the use of a blockchain structure in EHRs. We employ a distributed ledger technology that was initially associated with Bitcoin. Based on the superiority of blockchain in data security, the multilayer and multichain data transfer model was created for the low tyranny of scheduling and the decentralisation of transactions. Then, we considered how we may apply this paradigm to enhance the data security of the energy internet. The third and last section looked at the prospect of combining current real-world projects with blockchain in order to increase information security. Attackers would need to alter more than 60% of the node's backup data, that would take a lot of processing power, in order to create a new integrity test condition when tampering with notarized data. Such strong computational capacity would be difficult for a typical information attacker to possess.

Reference:

[1]. A. Rozyyev, H. Hasbullah, and F. Subhan, "Indoor child tracking in wireless sensor network using fuzzy logic technique," *Research Journal of Information Technology*, vol. 3, no. 2, pp. 81– 92, 2011.

[2]. R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring, and D. Estrin, "Habitat monitoring with sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 34–40, 2004.

[3]. S. H. Chauhdary, A. K. Bashir, S. C. Shah, and M. S. Park, "EOATR: energy efficient object tracking by auto adjusting transmission range in wireless sensor network," *Journal of Applied Sciences*, vol. 9, no. 24, pp. 4247–4252, 2009.

[4]. P. K. Biswas and S. Phoha, "Self-organizing sensor networks forintegrated target surveillance," *IEEE Transactions on Computers*, vol. 55, no. 8, pp. 1033–1047, 2006.

[5]. L. T. Lee and C. W. Chen, "Synchronizing sensor networks with pulse coupled and cluster based approaches," *Information Technology Journal*, vol. 7, no. 5, pp. 737–745, 2008.

[6]. Jiang and Gruenwald, S. A. Aljunid, B. Ahmad, A. Yahya, R. Kamaruddin, andM. S. Salim, "Wireless sensor actor network based on fuzzy inference system for greenhouse climate control," *Journal of Applied Sciences*, vol. 11, no. 17, pp. 3104–3116, 2011.

[7]. Tanbeer, Gruenwald "Monitoring forest cover changes using remote sensing and GIS: a global prospective," *Research Journal of Environmental Sciences*, vol. 5, pp. 105–123, 2011.

[8]. Halatchev, B.Mukherjee, and D. Ghosal, "Wireless sensor network survey," *ComputerNetworks*, vol. 52,no. 12,pp. 2292–2330, 2008.

[9]. T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Proceedings of the 20th IEEE International Symposium on Intelligent Control (ISIC '05)*, pp. 719–724, June 2005.

[10]. Y.-C. Tseng, M.-S. Pan, and Y.-Y. Tsai, "Wireless sensor networks for emergency navigation," *Computer*, vol. 39, no. 7, pp. 55–62, 2006.

[11]. T. Yairi, Y. Kato, and K. Hori, "Fault detection by mining association rules fromhouse-keeping data," in *Proceedings of the 6th International Symposium on Artificial Intelligence, Robotics and Automation in Space*, pp. 18–21, 2001.

[12]. O. Horovitz, S. Krishnaswamy, and M. M. Gaber, "A fuzzy approach for interpretation of ubiquitous data streamclustering and its application in road safety," *Intelligent Data Analysis*, vol. 11, no. 1, pp. 89–108, 2007.

[13]. J. Gama, P. P. Rodrigues, and L. Lopes, "Clustering distributed sensor data streams using local processing and reduced communication," *Intelligent Data Analysis*, vol. 15, no. 1, pp. 3–28, 2011.

[14]. Z. A. Aghbari, I. Kamel, and T. Awad, "On clustering large number of data streams," *Intelligent Data Analysis*, vol. 16, no. 1, pp. 69–91, 2012.

[15]. A. Boukerche and S. Samarah, "An efficient data extraction mechanism for mining association rules from wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 3936–3941, June 2007.

[16]. S.Umadevi, S. NirmalaSugirtha Rajini,A. Punitha & Viji Vinod, (2020), " Dimensionality Reduction in Machine Learning Technique using Principal Component Analysis", Test Engineering and Management, January - February 2020 ISSN: 0193 - 4120 Page No. 14546 - 14552 .

[17]. S.Umadevi, S. Nirmala Sugirtha Rajini, A. Punitha & Viji Vinod(2020), "Performance Evaluation Of Machine Learning Algorithms In Dimensionality Reduction", International Journal of Advanced Science and Technology, Vol. 29, No. 9s, pp. 3845-3853

[18]. M.Anita Priscilla Mary , M.S.Josephine , V.Jeyabalaraja & S.Nirmala Sugirtha Rajini(2020), "Identification and Performance valuation for Effective Utilization of Electrical Energy Resource using K Means Clustering Algorithm", International Journal of Advanced Science and Technology, Vol. 29, No. 9s, (2020), pp.55-62.

[19]. S. Uma Devi & S. Nirmala Sugirtha Rajini (2019), " Detection of Traffic Violation Crime Using Data Mining Algorithms", Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No.9, pp. 982- 987.

[20]. Mercy Beulah, E,Nirmala Sugirtha Rajini,S & Rajkumar, N (2016), "Application Of Data Mining In Healthcare: A Survey", Asian Journal of Microbiology, Biotechnology & Environmental Sciences, vol.18, no. 4, pp. 999-1001, ISSN-0972-3005.

[21]. Mercy Beulah, E , Nirmala Sugirtha Rajini, S & Raj Kumar, N(2015)," Data Mining and Business Intelligence applications in Shipping Industry" , *International journal of applied environment sciences(IJAES)*, vol. 10, no.1, pp.87-91, ISSN0973-6077 (Scopus Indexed).

[22]. Kiruthika , C & Nirmala Sugirtha Rajini,S(2014), "An Ill-identified Classification to Predict Cardiac Disease Using Data Clustering", *International Journal of Data Mining Techniques and Applications, vol.* 03,pp. 321-324, ISSN:2278-2419