EiAiMSPS: Edge Inspired Artificial Intelligence-based Multi Stakeholders Personalized Security Mechanism in iCPS for PCS

Swati Devliyal, Sachin Sharma, Himanshu Rai Goyal
Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India

***Abstract*—Artificial Intelligence (AI) is becoming more prevalent in the healthcare sector like in pharmaceutical care to achieve rapid and precise outcomes. Machine learning techniques are critical in preserving this balance since they ensure both the confidentiality and authenticity of healthcare data. Early sickness projections benefit clinicians when establishing early monetary choices, in the lives of their patients. The Web of Things (IoT) is acting as an accelerator to boost the efficacy of AI applications in healthcare. Healthcare service pharmaceutical care is also in demand and can have AI for good patient care. The sensor gathers the data from individuals, then the data is examined employing machine learning algorithms. The work's major intent is to come up with an automated learning-based user authentication algorithm for providing secure communication. The other goal is to ensure data privacy for sensitive information that does not currently have security. The Federated Learning (FL) technique, which uses a decentralized environment to train models, can be utilized for this purpose. It enhances data privacy. This work proposes in addition to security a differential privacy preservation strategy that involves introducing random noise to a data sample to generate anonymity. The model's performance and data quality are assessed, as privacy preservation approaches frequently reduce data quality.**

Keywords*—Internet of things; pharmaceutical care; machine learning; authentication; artificial intelligence

I. Introduction

Over the last several years, the world of pharmacy has seen a steady and considerable transition. The prior work of the pharmacist, which included medicine production, dispensing, and marketing, is no longer sufficient for pharmacy professionals to still exist [1]. Pharmaceutical care has been widely acknowledged as the main objective of pharmacy. Pharmaceutical care requires practitioners to not only provide drugs but also to take responsibility for enhancing the quality of patients' outcomes [2]. In our assessment of research on the review of pharmaceutical care services, multiple publications highlighted the large beneficial impact that pharmaceutical care services have on long-term healthcare management and healthcare expenses [3]. A number of read ups have been conducted to inquire the implications of artificial intelligence (AI) arrangements on healthcare distribution. AI-powered solutions have the potential to improve forecasting, assessment, and care coordination. AI is anticipated to become more prevalent fundamental element of medical care in the years to come, with applications in a number of clinical settings [4]. As the outcome, various technological companies and government agencies have put money in the growth of clinical tools and medical applications. Patients may be among the most significant benefactors and users of AI-based apps, and their perspectives may have an impact on the broad adoption of AI-based technologies. Patients must be encouraged that AI-based technologies will not damage them, but rather that adopting AI technology for healthcare reasons will help them [5]. Although AI has the potential to enhance healthcare results, any issues and hazards should be addressed before it is integrated into normal clinical treatment. Furthermore, following earlier research, healthcare professionals still have basic concerns regarding the use of AI-based solutions in care services [6]. Researchers must more efficiently comprehend the existing issues associated with AI technologies and analyse the pressing demands of health systems in order to create AI-enabled solutions that can solve them. Technological advancement unleashes a maelstrom of communication and interconnection, allowing the intelligent pharmaceutical care in order to grow more flexible, sophisticated, and smart through the use of artificial intelligence. AI enables systems should naturally emphasis on enhanced analysis of data while maintaining appropriate user experience quality. Despite the fact that the association of AI-concentrated along with CPS considerably boosts productivity in pharmaceutical care, it is still in torment from challenges such as high burden, device incompatibility, security, and privacy [7] [8] [9]. CPS-based systems offer various additional issues, the most difficult of which is authentication. In pharmaceutical care there are so many stakeholders and major are practitioner, pharmacist and patient. When all are communicating through the network need authorisation at each end. We have developed an authentication approach that can be more resilient. In this article, we look at a unique security architecture for CPS that hosts user authentication and provides data security and privacy, device anonymity, and safety.

Our contributions are highlighted below:

- Based on edge assistance, we provide a layer skeleton in CPS. The higher layer is intended for registration management in conjunction with IIoT gadget. It decouples the need for direct interaction with IIoT devices and decreases system complexity. The middle surface is used in data transmission, while the lower surface houses the IIoT gadget.
- We present an authentication system that makes use of a proxy signing for establishing a link. It significantly minimizes the expenditure for signatures on gadgets and prevents unauthorized encounters in the outer limits, establishing the groundwork for protecting the

privacy on gadgets.

- The suggested scheme's security and performance assessments is demonstrating its robustness and practicability in contrast to earlier work. The rest of the sections are as follows: First is literature review which is followed by the proposed model. Further design in presented which focuses at security and privacy concerns, whereas last is performance analysis followed by conclusion.

II. Literature Review

A. Edge-AI in Pharmaceutical

According to the Thakur *et al.* [10] the use of AI in the field of pharmaceutical and biological studies has been significant, including cancer research, for prognosis and diagnosis of the disease state. It has evolved into a tool for researchers in charge of complicated data, covering everything from acquiring supportive results to normal statistical analyses. AI improves the accuracy of estimating treatment impact in cancer patients and decides forecast outcomes. Klumpp *et al.* [11] proposes a methodology for predicting the future based entirely on comprehensive analyses of trends by subject as well as interactive advancements. The findings suggest that the human aspect, as well as human-artificial collaboration skills and attitudes, might be a critical feature in AI and technology use in logistics. Damiati *et al.* [12] examines the historical, current, and future implications of machine learning technologies on several fields of pharmaceutical sciences, including drug design and exploration, revision, and composition. The strategies for researching systems that are often used in pharmaceutical sciences are explained.AI and system learning technology in ordinary everyday pharma demands, as well as commercial and regulatory insights, are examined. For unbalanced ICS data, Jahromi *et al.* [13] suggested a novel two-level ensemble deep learning-based attack detection and identification method. The whole bureaucratic model is a complicated DNN with a partially and entirely linked component that can appropriately blame cyber-attacks. Burki *et al.* [14] suggested obstacle might allow AI to be trained on millions of data points from various drug organisations' databases without jeopardising the possession and privacy of the statistics. Rathi *et al.* [15] provides a scalable, responsive, and dependable AI-enabled IoT and aspect computing-based healthcare system with minimal lag while servicing patients.

B. Stakeholder Authorization

Xu *et al.* [16] presents, an approval strategy based entirely on block chain is presented to identify genuine authorization for information access. The suggested approach divides info warehouses in block chains and HISs, with greater performance, more area-specific, dynamic, and bendy authorisation procedures. Hameed *et al.* [17] proposed, we provide a Block chain-based safe, decentralised, and customisable authorisation mechanism to grapple with the challenge of unauthorised access to IoT networking equipment. We implemented the ABAC version utilising intelligent agreements, which make the technique possible of authorising consumers with safe access to IoT devices to be accomplished largely based on dynamic and fine-grained policies maintained on the distributed immutable ledger. Using a permissioned blockchain community, this article presents a robust and accessible pharmaceutical supply chain gadget. Babu *et al.* [18] designs also includes digital transactions between providers and traders, tracking the source, ok verification, and lowering the risk of supply chains.The Hyperledger network fabric has been used in its deployment of this machine and its effectiveness has been assessed using Hyperledger Calliper. Zukarnain *et al.* [19] aimed to propose an aggregation of multi-component authentication that requires minimal user participation in this work. Because of security concerns, they implemented an unequal encryption technique in which the users' input is utilised as the encryption key. The PKI idea was adopted, yet without the required to communicate with a certificate authority (CA), the value was significantly reduced.

C. Intelligent CPS

Lu *et al.* [20] presents system of authentication for imposing security policies at the edge in CPS discourse for IIoT in order to enable reliable interaction for restricted gadgets.The main concept aims to integrate proxy authentication and process links at the ICN structure in order to provide two-way authentication. Security testing indicated that the suggested strategy provided a more effective protection than competing schemes. Ramasamy *et al.* [21] presents an AI-enabled IoT-CPS that doctors can use to diagnose ailments in patients. AI was created to assist with a variety of illnesses such as diabetes, heart disease, and gait problems. To detect illnesses in the class, the AI-enabled IoT-CPS Algorithm is used. Experiment findings reveal that, when compared to current methods, the proposed AI-enabled IoT-CPS algorithm diagnoses patient diseases and incident actions with more precision in terms of recall, accuracy, precision, and F-measure.Mishra *et al.* [22] developed deeply into novel new technologies such as the machine-to-machine communication, machine learning, artificial intelligence, Internet of Things, big data, and so on. An example NG-CPS structure is proposed, which includes all layout concerns such as physical layout components, cyber layout elements, and design conversations. Makkar *et al.* [23] presented cognitive-inspired architecture for CPS security is investigated. The suggested system, dubbed Secure CPS, is trained with immediate time collective dataset for determining the relevance of a web page using facial expressions as guides. The eye regions are identified using the Focal Point Detector method. The system was tested using device learning models and achieved 98.51% accuracy, outperforming existing frameworks. Adil *et al.* [24] proposed a hybrid light-weight authentication scheme that makes use of SML (supervised machine learning) method in conjunction with CPBE&D (Cryptographic Parameter Based Encryption and Decryption) scheme to ensure the authenticity of criminal patient wearable gadgets with consistent transmission over the Wi-Fi conversation channel.

D. Pharmaceutical Care Services

Alzahrani *et al.* [25] propose a novel TRD (Tag Reapplication Detection) method for detecting reapplication attacks, as well as the usage of low-cost NFC (Near Field Communication) tags and public key cryptography. Because a huge number of modern mobile phones are NFC-enabled, the inclusion of NFC makes TRD user-friendly. TRD uses an

online authentication system to track the number of times a tag in the database has been read delivery chain to detect reapplication attacks. Janardhan *et al.* [26] proposed a contrast the accuracy of the Decision Tree Classifier to the Support Vector Machine Classifier in detecting the authentication attacks. The SVM accuracy was 87.02%, P0.05, whereas the Decision Tree Classifier accuracy was 71.81%, P0.05. SVM performed substantially better in identifying de-authentication attacks.

E. AI Based Privacy Prevention

A lightweight stable encryption technique is developed in this work to preserve the privacy of sensitive data and communication. The scheme is developed by permutation, then with the help of a spread structure. The recombination uses pseudo-random sequences (PRNS), whereas the diffusion employs a key circulate generated (KSG). The algorithm is advantageous for CPS devices because to its simple and secure construction. The test results show that the proposed method is sufficiently robust and unquestionably able to withstanding any known prevention assaults as discussed by Tiwari *et al.* [27] and Lian *et al.* [28]. The possible impacted medical records breach will also cause concerns about security and confidentiality were raised throughout the contact period. We propose to fix these current concerns by DEEP-FEL, a decentralised, green, and privateness-better federated side learning device that enables clinical gadgets in a unique establishment to collectively teach an international framework without confidential data being shared. Zhang *et al.* [29] proposed a PEMFL architecture that Momentum FL (MFL), a chaos-based encryption approach and combines differential privacy (DP). The overall success of this methodology is based entirely on two non-datasets. The PEMFL performs exceptionally well in terms of accuracy and privacy protection, according to theoretical assessment and exploratory results.

III. Discussion

A. Gaps Identified from the Past Research

- Privacy Concerns: Previous research may have adopted basic privacy safeguards, but they failed to handle the difficulties of decentralized systems, exposing critical patient information.
- Inadequate Security Protocols: Other techniques may lack robust user authentication algorithms capable of securing connections in pharmaceutical treatment.
- Trade-offs Regarding Privacy and Data Quality: Highlight that present systems frequently sacrifice data quality to improve privacy, perhaps leading to less accurate healthcare results.

B. Emphasize the Urgency

As AI and IoT modern technology become increasingly woven into healthcare, particularly pharmaceutical treatment, the challenges connected with poor data privacy and security safeguards grow more pressing. Failure to solve these challenges might have serious ramifications, such as data breaches that endanger patient safety and weaken the legitimacy of AI-driven healthcare systems.

TABLE I. Notations Used for Security

Symbol	Description
id_{st}	Identity information of stakeholder
p_{st}	Partial private key
s_{st}	Private key
Q_{st}	Stakeholder Public Key
K	Security Parameters
x_{st}	Stakeholder secret value
m_w	Warrant
M	Message
RL_{st}	Repudiation check
$_{st}$	Starting a hash chain's significance of a st
t_{sti}	i-th timeinterval of stakholder st
tP_{cs}	i-th timeinterval of Server

IV. Problem Statements

A. Syllabary

Table I contains a collection of the syllabary and security assumptions used.

B. System Prototype

The iCPS controls give system performance, infrastructure at the highest point of our paradigm. In our research main focus is patient care. The major elements of it are practitioners which are liable for the system. When a patient need medication plan will be get from the doctor to pharmacist and pharmacist will verify the medication from the doctor and will handover it to patient. After that monitoring will be done by the pharmacist if any modification is required after monitoring then the medication plan will be changed by the pharmacist by taking consent from the doctor. And the things will be done in repetition until patient will be completely ok. The system model is divided into four cluster which are as follows:

- Pharmaceutical healthcare provider: It basically consists of doctors, hospitals, staff, etc. It is the main cluster with which patients contact directly. If patients need pc then will directly communicate with hospital staff. After that, in the background other clusters will communicate with each other.
- Pharmaceutical Distributors: It consists of the medical things distributer like wholesalers, retailers and medical representatives.
- Pharmaceutical manufacturing bodies: This cluster is a collection of drug manufacturers, raw material suppliers, investors and PBM's. PBM is pharmacy business management who is responsible for securing lower drug cost for insurance and insurance companies.
- Pharmaceutical government bodies: It consists of the principal of governance and regulatory agencies which are to establish, screen, and put in force standards of exercise to enhance the excellent of exercise so that registrants avoid: unsuitable behavior, professional misconduct for a registrant, and inept overall fulfillment of obligations.

The pharmaceutical care is basically followed by the interaction foundation is followed by the IIoT devices. The patient communicates with iCPS and iCPS will communicate with the four clusters and after the approval from all clusters

is achieved only communication will take place. Interested stakeholders who desire to connect with one another can be authorized, and following successful authentication, data packets can be accessed using a cryptographic sign. Edge devices are responsible for matching Interest and Data and then storing the relevant information for further requests. The proposed model has four categories: an iCPS server, IIoT gadgets (like actuators, sensors, and machines), stakeholders, and patients. Notably, the iCPS server is in charge of all category registration. Based on the verification findings, an intriguing data packet should be transmitted and destroyed. After that, approval is allowed to perform virtual sign and sign instead of the IIoT providers, such as unexpected inactivity, insufficient time, or computing. capability.

C. Network Model for Proposed Scheme

The network model is shown in Fig. 1. With the help of CPS an architecture is designed in which on bottom we have smart healthcare devices that collect the required information from the environment. After that, the data is analyzed using different latest technologies which is used with the help of an interface. On other hand, we have different stakeholders who want to use this filtered information. In our study, we have selected 11 stakeholders with the patients they are interacting with each other with the help of iCPS.

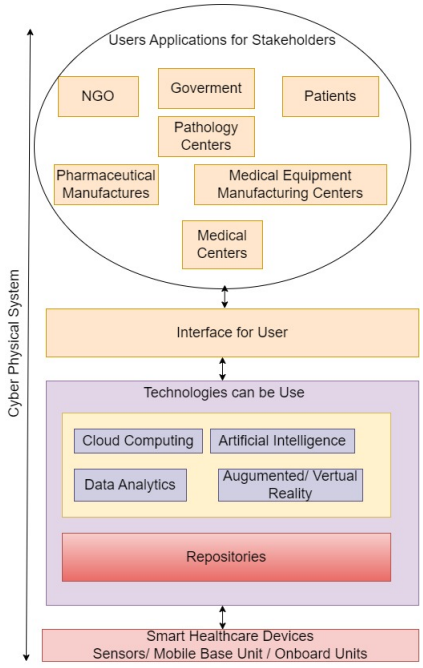


Fig. 1. Network model.

D. Threat Modal

We take into account both passive and aggressive attackers. Passive attacks are those that have amassed a deluge of Interest information to determine who is demanding and who is responding. Activated opponents, as opposed to inactive opponents, have greater power and may perform powerful attacks on any packets channeling, such as catching/exploring Interest packets, changing requests and responses, and spoofing authorized IIoT devices with the intention to transmit packets. According to the layout of framework, each one is needed to be register on the iCPS controller before if they want to communicate and want the system assets. We feel that the iCPS controller is inadequately powerful in order to render our design seem more plausible.

V. Edge-Assisted Intelligent User Authentication in CPS

Fig. 2. depicts the simple architecture of stakeholder authorization in CPS for pharmaceutical care.

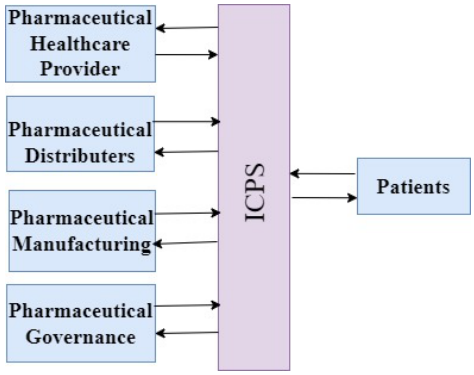


Fig. 2. Stakeholder authentication in cyber-physical system for pharmaceutical care.

To design authentication for IIoT devices, we use a proxy signature and a session-based variation. The proxy signature is used to validate the user, while the session-based variation is used to validate the request using Algorithm 1.

A. Overview

Based on edge assistance, our approach provides aid to do the requirement for CPS intelligent authentication procedures: 1) provides each user with the signing capability, allowing serving similar demands from multiple requesters; 2) allows users to authenticate themselves, allowing Only authorized individuals will receive the content they have requested; and 3) keeps IIoT gadgets unidentified, according to the authentication policy. The system paradigm is simplified, with a single iCPS server, practitioner, and patient. Six steps are included in an in-depth overview of the authentication operation. The start of the process is the identification of participants (intelligent users like practitioners, patients, etc.) and the intelligent server. The second step is to check the legitimacy of the user. The next phase is taken by a user who makes a content request, and it only sends the request while user is found valid in step two. The following phase is carried out on the info side to check the sign. The fifth step is performed to verify the sign if it is matched then only the communication will take place. The session handshake between the practitioner and the patient is the final phase. The practitioner is granted access to the required information once it has been authenticated in the last phase, as seen in Fig. 3.

B. Authentication Scheme

- (Registration) The system is started by the iCPS server, which broadcasts the system parameters var's.

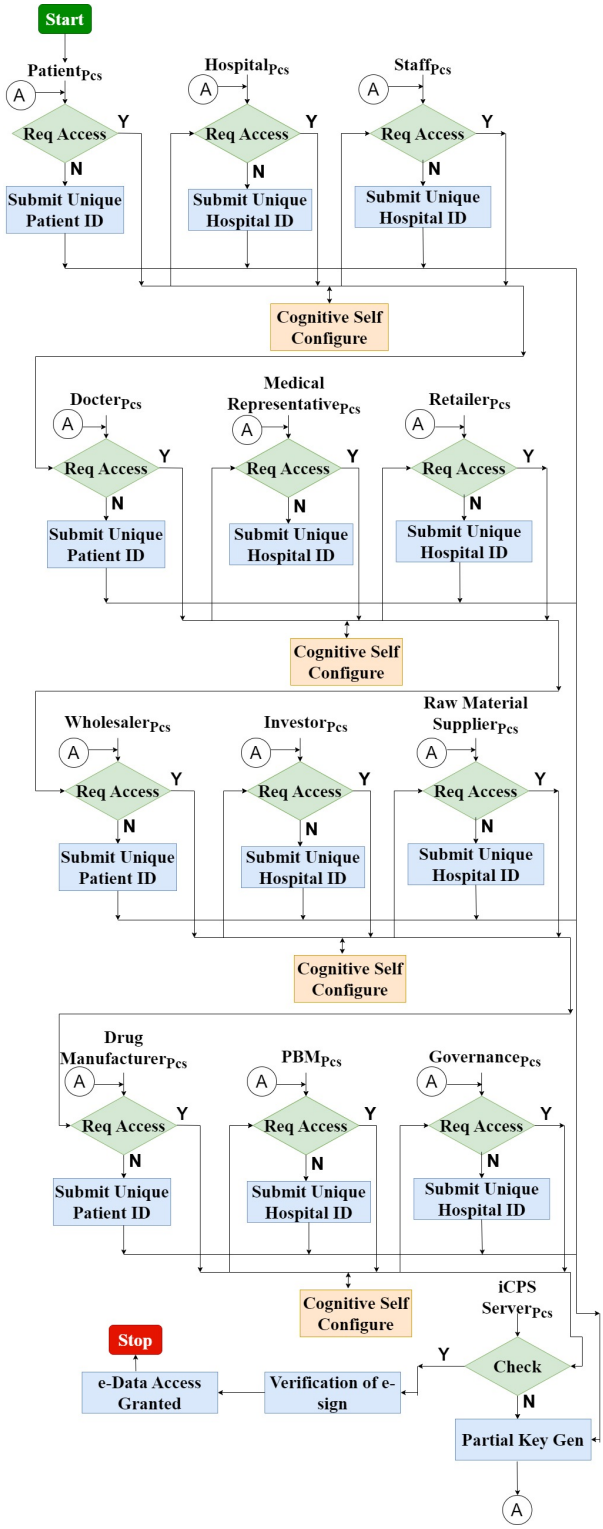


Fig. 3. Stakeholder authentication in cyber-physical system for pharmaceutical care.

Every stakeholder must identify themselves to the iCPS server and get a set of keys (Q_{st}, s_{st}), using the keygen to PartialKeyGen, and setup procedures outlined below. Configuration: The CPS configuration procedure basically is below mentioned. Partial key Generator: The iCPS produces the partial key for each stakeholder. The process takes var's, master key, a secret key x_{st} Z_q selected by stakeholder st and identification for stakeholder st with the value $id_{st} \leftarrow \{0,1\}$ as source. Every partially key is made up of two parts: the repudiation check RL_{st} and the partial secret key p_{st}. The repudiation check is an encrypted network that takes a starting phrase as input. The master-key hashes two identities, id_{st} and $x_{st}P$, to a point multiplier to create the partial secret key. That's accomplished using reliable means. The following are the specifications.

- Stakeholder st deliver ¡$idst, xstP$¿ to iCPS controller
- Make $_{st}\epsilon\{0,1\}$
- Determine
- $R_{evst1} \leftarrow h_5$ (ϵ_{st}),……., $Rev_{stk} \leftarrow h_5$ (Rev_{stk}-1)
- RL_{st1}<Rev_{st1}, t_{st1}>……, RL_{stk}<$Rev_{s_{tk}}, t_{s_{tk}}$> $t_{st} \leftarrow t_{st1}U……Ut_{s_{tk}}$
- RL_{st} RL_{st1}, U…….U t_{stk}
- $D_{st} \leftarrow$ h1(id_{st},x_{stP})
- $P_{st} \leftarrow sD_{st}$
- Key Generator: The iCPS takes var's, the partial secret key p_{st}, and the certified value x_{st} as input as outputs the secret key s_{st} along with public key Q_{st}. A p_{st} and x_{st} repository consists of an entity's entire secret key st and its public key equivalent $x_{st}P$. The operation is carried out by st, who is the only legitimate proprietor of x_{st}.

- (Repudiation Check): If an iCPS rejects a stakeholder, all stakeholders have to exit the system. As a result, the controller distributes a repudiation list to all stakeholders regularly to determine if a stakeholder has been repudiated. The detailed procedure is as follows: Repudiation Check: The repudiation checks are performed at each stakeholder's entering and ensure that a stakeholder is associated to the repudiation index prior to the session connection. It requires var's present period of time t and the repudiation list RL_{st} as variables. The iCPS may validate the consumer's repudiation evidence after investigating the truthfulness of the repudiation variables in the repudiation list. It invalidates anything in the request produced after the time $t_{st}k$ since the timestamp $t_{st}k$ rarely in t_{st}.
- (Interest): Stakeholder introduces a cognitive self-configure to check to set all the parameters so that can communicate further. Each stakeholder can set its parameters. Step 4(Verification and sign)- This is done on the iCPS edge and receives the secret value x_{st} as input, as well as a warrant m_w that comprises the repudiation time frame, message m, and identification information idst, the public key of the iCPS, and all stakeholders Q_{iCPS}, $Q_{st\mathbf{P}pcs}$, $Q_{st\mathbf{H}pcs}$, $Q_{st\mathbf{S}pcs}$, $Q_{st\mathbf{D}pcs}$, $Q_{st\mathbf{MR}pcs}$, $Q_{st\mathbf{R}pcs}$, $Q_{st\mathbf{W}pcs}$, $Q_{st\mathbf{I}pcs}$, $Q_{st\mathbf{RM}pcs}$, $Q_{st\mathbf{DM}pcs}$, $Q_{st\mathbf{PBM}pcs}$, $Q_{st\mathbf{G}pcs}$. The iCPS verifies its rights as follows:

Algorithm 1 Algorithm Stakeholders Verification and Sign

Input: var's, s_{st}, $\mathbf{PK}_{st}$, proxy
Output:Success 0: Fail

Calculate **H2**← h2(id_{iCPS}, $id_{st\mathbf{P}pcs}$, $id_{st\mathbf{H}pcs}$, $id_{st\mathbf{S}pcs}$, $id_{st\mathbf{D}pcs}$, $id_{st\mathbf{MR}pcs}$, $id_{st\mathbf{R}pcs}$, $id_{st\mathbf{W}pcs}$, $id_{st\mathbf{I}pcs}$, $id_{st\mathbf{RM}pcs}$, $id_{st\mathbf{DM}pcs}$, $id_{st\mathbf{PBM}pcs}$, $id_{st\mathbf{G}pcs}$, m_w, Q_{iCPS}, $Q_{st\mathbf{P}pcs}$, $Q_{st\mathbf{H}pcs}$, $Q_{st\mathbf{S}pcs}$, $Q_{st\mathbf{D}pcs}$, $Q_{st\mathbf{MR}pcs}$, $Q_{st\mathbf{R}pcs}$, $Q_{st\mathbf{W}pcs}$, $Q_{st\mathbf{I}pcs}$, $Q_{st\mathbf{RM}pcs}$, $Q_{st\mathbf{DM}pcs}$, $Q_{st\mathbf{PBM}pcs}$, $Q_{st\mathbf{G}pcs}$
if Verify if e(ϵ,Q_{icps}+**H2**$_{icps}$)= e(Q_{icps},D_{icps}) **then**
  Set r ϵ Z_q
  Compute **R**←rP, H3← h_3(m,id_{icps},R,Q_{icps}) **V**← p_{icps} + rH_3+ H_2Q_{icps} + $x_{icps}H_2$P ð←(R,V)
  send 1
else
  send 0
end if

- (Generation of Proxy Signs and Authentication): If the check is successful,the iCPS will get a proxy signing key pair (s_{icps}, $\mathbf{PK}_{icps}$),where PK_{icps} is a collection of public keys. (Q_{iCPS}, $Q_{st\mathbf{P}pcs}$,$Q_{st\mathbf{H}pcs}$, $Q_{st\mathbf{S}pcs}$,$Q_{st\mathbf{D}pcs}$,$Q_{st\mathbf{MR}pcs}$, $Q_{st\mathbf{R}pcs}$,$Q_{st\mathbf{W}pcs}$,$Q_{st\mathbf{I}pcs}$, $Q_{st\mathbf{RM}pcs}$,$Q_{st\mathbf{DM}pcs}$,$Q_{st\mathbf{PBM}pcs}$, $Q_{st\mathbf{G}pcs}$).If this is the case, the iCPS generates a digital signature from a message. A signature is not misleading the provider's identity to the public. It accepts the signature by checking ð is a valid identity that involves message m;else,it denies it.
- (Session Connection): When patient receives sign makes a request by addressing call including four information of a subject, subject name, signature, identity id and subject which is used by iCPS to identify. Upon receiving the request each stakeholder has to authenticate the request. The iCPS gets the access key Q_{st} and identification id, and private key s_{st} . The iCPS does the verification, and if the check succeeds, the current session connection gets established; otherwise, the request isn't deemed valid, and the session connection is terminated.
- Safety Examination: The suggested technique guarantees that the CPS controller obtains the partial secret keys in a unique manner, preventing it from impersonating a real organization. We examine the authentication system in light of the security objectives given below. To keep attackers at bay, we have identified the following authentication mechanism security goals.
- Trustworthiness: The system should ensure that the person signing cannot be untruthful to an information packet.
- Genuineness: The technique should offer evidence that a signed request is valid.
- Authentication: The method should include a way for authenticating that is the broadcaster an Interest and responding to what it intends to be [30].

- Anonymity: The technique should safeguard IoT devices by ensuring that both inner and external assailants are unaware of their identities.
- Key Organisation: The system should offer a negotiated key among all the stakeholders, so that no one controls the key.
- Authenticity: A polynomial-time adversary has the knack of forging a signature assigned to authorised entity in order to prevent the organisation from denying it.

Theorem 1: A polynomial-time challenge exists that may fix the Computational Diffie–Hellman issue along likelihood $\varepsilon(\mathbb{k})^{'}>(\varepsilon(\mathbb{k})/2)\ (1-q_s(q_{h3}+q_s)/2^{\mathbb{k}})(e(q_r+1))^{-}1$ is contingent upon whether or not the opponent £ can forge a sign along with a competitive edge $\varepsilon(\mathbb{k})$, where q_{h3}, q_s, q_r indicate the total quantity of requests made to the h_3, executing, as well as reveal-partial key predictions, providing that $h_i(i=1,2,3)$ hashed routines are arbitrary diviners.

Demonstration: Assume that $X \leftarrow a\rho, Y \leftarrow b\rho \in G1G1$ indicate an arbitrary task.Using the forger £,we can create the algorithmic programme $\in$ to produce $ab\rho \leftarrow G1$.Algorithm $\in$ first generates system-specific var's, as the standard protocol does, and passes var's to the forger £, which then initialises £ with $Q_0 \leftarrow X$ and communicates with £ as below.

1) h1 and h3 Queries: If examines an arbitrary prophet h1(h3) using a number of tuples $<id_{st}, Q_{st}>(<m_{st}, id_{st}, R_{st}, Q_{st}>)$, preserves an index $Lh_1(Lh_3)$ of components $<id_{st}, Q_{st}, x_{st}, c_{st}, \nu_{st}>(<m_{st}, id_{st}, R_{st}, Q_{st}, y_{st}, d_{st}, v_{st}>)$, It is initially empty and yields the following outcomes.

a) Since the inquery $<id_{st}, Q_{st}>(<m_{st}, id_{st}, R_{st}, Q_{st}, Q_{st}>)$ is existing in $Lh_1(Lh_3), \in outputsv_{st}(\nu_{st})$ to .

b) Else, $\in$ picks $x_{st} \in Z*q(y \in Z^*q)$ arbitrary, yields $\nu_{st} \leftarrow x_{st}\rho(\nu_{st} \leftarrow y_{st}Q_0)$ if a tossup $c_{st} \leftarrow 0,1(d_{st} \leftarrow 0,1)$ which gives 0 as a result with likeliness $\sigma(1/2)$ and yields $\nu_{st} \leftarrow x_{st}y(\nu_{st} \leftarrow y_{st}\rho)$ if $c_{st}=1(d_{st}=1)$ having a likelihood $1-\sigma(1/2)$, and adds $(<id_{st}, Q_{st}, x_{st}, c_{st}, \nu_{st}>)$ $(<m_{st}, id_{st}, R_{st}, Q_{st}, y_{st}, d_{st}, \nu_{st}>)$ into $L_{h1}(L_{h3})$.

2) h2 Queries: While asks an arbitrary generator h_{st} with a list of T_{st} tuples, $\in$ keeps the matching list $L_{h_st} \leftarrow <T_{st}, \mu_{st}>$. While the value of the input field is located in the list Lh_{st}, it sends $\in$ the matching element μ_{st}. If not, delivers a random $Z*q$ value.

3) RevealPartialKey Queries: After £ queries the identity id_{st}, $\in$ obtains the matching element $<id_{st}, Q_{st}, x_{st}, c_{st}, \nu_{st}>$ from the list of items L_{h1} and responds as follows.

a) If $c_{st}=1$, then $\in$ outputs and the experiment is aborted.

b) Otherwise, sets $p_{st} \leftarrow x_{st}Q_0$ and restores it to .

4) RequestPublicKey Queries: As £ queries identify id_{st}, $\in$ sets $Q_{st} \leftarrow x_{st}\rho$ for an arbitrary value $x_{st} \leftarrow Z*q$, sends it to , and inserts $<id_{st}, x_{st}>$ to $L\rho K$.

5) Signing Queries: demands an id_{st} verification on an exchange m_{st}, and $\in$ replicates the divination verification and replies in response to the probe.

a) Assuming h_3 is not supplied along with $<m_{st}, id_j, R, Q_j>$, the process continues by replying to h1 requests to get $H_2 \leftarrow \mu_2$ and setting $R \leftarrow r_2Q_0, H_3r_2^{-1}(x_1\rho \leftarrow D_j)$, and $V \leftarrow r_1Q_0+\mu_2Q_i+\mu 2Q_j$ with an arbitrary selected $r_1, r_2 \leftarrow Z*q$. Otherwise, $\in$ will stop and forsake. Because L_{h3} can never have a total of qh_3+q_s entries, the likelihood of not terminating $1-(q_s(qh_3+q_s)/2^k)$.

b) $\in$ yields $\Delta \leftarrow <V, R>$ as the acceptable signing on m.

It is worth noting that opponent $\in$ correctly generates a signature δ with likelihood $\varepsilon(k)^{'}$, which means that £ completely meets the Signing answers. Finally, £ creates a fake sign $\iota* \leftarrow <V^*, \mathrm{R}^*>m^*$ upon a message. After it $\in$ gets the elements $<id^*_{st}, Q^*_{st}, x^*_{st}, c^*_{st}, \nu^*_{st}>$ derived from Lh_1. If $c^*_{st}=0$, the program fails and exits. Otherwise, it proceeds to retrieve the pair $<id^*_{st}, Q^*_{st}, Q^*_j>$ based on the set Lh_2 and $m_{st}, <m^*_{st}, d^*_{st}, \nu^*_{st}, id^*_{st}, R^*_{st}, Q^*_{st}, y^*_{st}>$ based on the record Lh_3. Assuming that $d^*_{st}=0$, then C responds 0 and exits. Otherwise, it will do this: $\ddot{e}(V*,P)=\ddot{e}(y^*_{st}P, R^*_{st})$. $\ddot{e}(Q_0, D^*_{st})\ddot{e}(Q^*_{st}, \mu^*_{st}P)\cdot\ \ddot{e}(\mu^*_{st}P, Q^*_j)$ with $\hbar 1=x^*_{st}y, \hbar 2=\mu^*_{st}, \hbar 3=y^*_{st}$ P along with $R^*_{st}=r^*_{st}$ P for components which are referred as $\mu^*_{st} \leftarrow Z^*_q, r^*_{st}, x^*_{st}$. $(1-\delta)/2$ is the probability of not terminating at particular moment. Henceforth $\ddot{e}(V^*-y^*_{st}R^*_{st}-\mu^*_{st}Q^*_{st}-\mu^*_{st}Q^*_j, P)=\ddot{e}(X, x^*_{st}Y)$

VI. Problem Analysis for Security

Using MATLAB a comparative analysis has been done to check the suggested proposal's effectiveness mechanism with the existing one. The comparison is done with communication and computation consumption under the number of requests with existing schemes [34], [32], [33] and [31] as demonstrated in Fig. 4(a)-(b) along with Fig. 5(a)-(b). In addition, Fig. 4(c) authorization and acknowledge consumption with the amount of request contents. To find out in a better way we have measured the cost of authorization concerning a number of requests made in Fig. 4(b) which depicts it as a linear correlation. In our method there is a slightly heavy burden to other methods [31], [32], [33], and [34]. But in contrast, our method has a better authentication which reflects more reliability. In Fig. 5(b) efficiency of our method as compared to other four methods in terms of patients requests. As it increases the computation cost also increases but not in a drastic way. In Fig. 4(a), the validation execution efficiency of various systems improves when the request quantities grow from 0 to 100. Our method has a somewhat greater inspection processing proportion compared to [30], [28], but lower than [27], and [29]. In our system, verifying a signature requires acquiring all packets containing the delegation information used to calculate it. Our scheme achieves a verification execution efficiency of less than 20% for 50 contents, making it suitable for latency-tolerant uses in the IIoT. Fig. 4(b) highlights our investigation of the transmission load as the content of the request increases. An apparent pattern indicates that the transmission load is linearly related to the quantity of requested contents. Our system has a somewhat higher load compared to [27], [28], and [29], but lower than [34]. Our method offers two-way verification in addition to caching, which sets it apart from other schemes. In Fig. 4(c), we examine the relationship between communication cost, verification versus simultaneous dissemination, and quantity of demanded data to assess the

overhead of communication robustness in the proposed approach. The method of delivery cost grows with the amount of requested material, whereas verification consumes less than the interaction procedure. Raising the quantity of required material from 50 to 100 only leads to a ten percent rise in signature size. Though each signature packet must be transferred from the supplier to the user, the proposed approach is resource-efficient and does not create significant overhead associated with communication modifications. Fig. 5(a) shows that the capacity usage ratio grows with the amount of demanded content. The information usage ratio in [28], [29], and our system is less than forty percent for one hundred packets of requested material, unlike [29] and [30]. Our technique consumes little computing resources on the consumer side and outperforms other systems in terms of safety. Fig. 5(b) shows that the provider's delay increases with the quantity of demanded contents. It uses somewhat more computing resources than [27] and [26], but the growth rate will be slower than [29] and [30]. Compared to the transmission load indicated in Fig. 4(b), our technique requires less time. So to conclude we can say that authentication time improves as the request are getting increased.

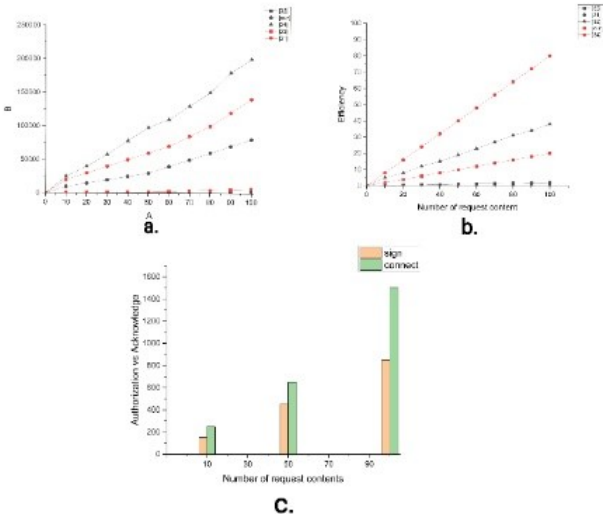
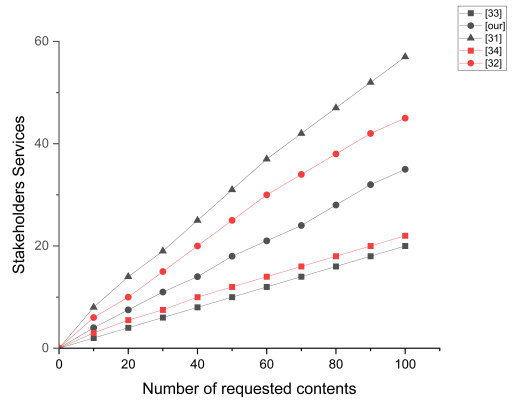
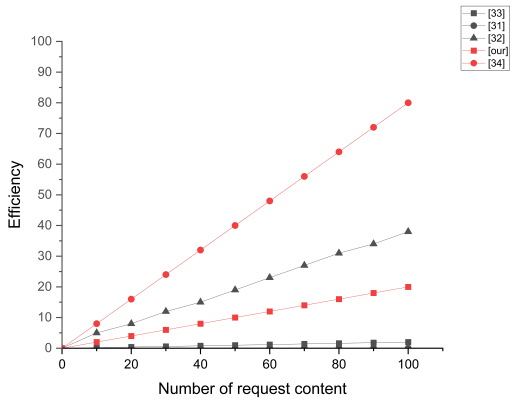


Fig. 4. Estimation value differentiation with a varying number of requests a) Cost for several authentication methods b) The cost of transmission for various methods of authentication c) Authorization price versus acknowledge price.



(a)



(b)

Fig. 5. Comparative analysis of the ability to provide services to stakeholders with varying number of requests a) Stakeholder service cost under different authorization methods b) Efficiency of different authorization methods.

TABLE II. NOTATIONS FOR PRIVACY

Symbol	Description
P_u	Universal prototype
P_i	Localized prototype
P_i^{reform}	Updated universal prototype
S_i	Stakeholders
I_i	Local input
I_i^n	local input with noise
I_i^{np}	Upgrade local input

VII. PROPOSED MODEL FOR PRIVACY

In this paper edge based technique is used to provide privacy in user authentication. In start every stakeholder and patient will download the present universal prototype from the iCPS. The downloaded universal model will act as localized for each edge node. Firstly, noise has been added to the input set to upgrade it. After that, the model has been trained using the classifier. After that training input set is transferred to iCPS. This is done in several repetitions. The updated universal prototype is created using aggregation of different types of prototypes as shown in Fig. 6. Table II represents different notation used while designing the algorithm. Stakeholders using Algorithm 2. There are eleven stakeholders represented by Si where i varies from one to eleven. If any stakeholder has a localized update(Ii), then universal prototype Pu is downloaded from the iCPS. If the universal prototype is not same as the existing one, then only the procedure will start. The universal prototype will act a localized prototype (Pi) for the stakeholder. A noise has been added input set and stored into as I_i^n and upgraded scaled form as I_i^{np}.The updated model is created and transferred to iCPS as P_i^{reform}. The same patient is using Algorithm 3.

Data: Data for all stakeholder's will be private and will be represented by I_i.Correlation Coefficient added with Noise: It describes the association between the features and the target. The value of this varies from 0 to 1. This value denotes the

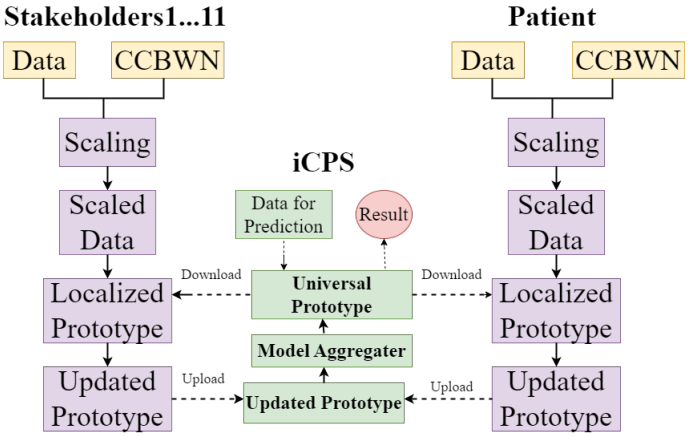


Fig. 6. Block diagram of proposed model.

correlation low value means low correlation and high value means high correlation. Value 0 denotes no correlation.

$$ran = \frac{n(\Sigma ab) - (\Sigma a)(\Sigma b)}{(n\Sigma a^2 - (\Sigma a^2)(n\Sigma b^2 - (\Sigma b^2)} \quad (1)$$

$$a_i^n = a_i + Rand(0, ran) \quad (2)$$

Where,i varies from 0 to l,n is an integer value,a_i is original, a_i^n is after appending noise,Rand(0,ran) is used to generate random numbers between 0 to ran,ran is correlation coefficient of a_i which is mentioned in Eq. 1. Noise is appending using Eq. 2 after that the updated value of input will be I_1^n to I_{11}^n. iCPS using Algorithm 4. iCPS will choose the stakeholder's (Si: i=0 to 11) for training and give response to stakeholder by giving upgraded prototype.

Algorithm 2 Stakeholder's Algorithm

Claim: P_u **received from the validator**
Guarantee:$P_u \neq P_i$
if stakeholder process () **then**
  if Localizedreformaccessible **then**
    Set $P_i \leftarrow P_u$
    $I_i \leftarrow$ Localizedreform
    $I_i^n \leftarrow$ Add noise with I_i
    $I_i^{np} \leftarrow$ upgrade I_i^n
    $P_i^{reform} \leftarrow$ Trainprototype(P_i,I_i^{np})
    Transfer P_i^{reform} to the validator
  end if
end if

VIII. Problem Analysis for Privacy

The dataset used in this study was taken from Kaggle and contains a large no. of instances approximately 2000 with 8 attributes. Attributes are drug-uses, patient symptoms, gender, disease prevention, design therapist plan, age, implementing the therapeutic plan and monitoring therapeutic plan and correlation coefficient values are mentioned in Table III. The class that is targeted has a value of 0 or 1. In the start, iCPS circulates the attributes to the localized model to the randomly chosen patient and stakeholders for the training

Algorithm 3 Patient's Algorithm

Claim: P_u **received from the validator**
Guarantee:$P_u \neq$ **Patient**
if patient process() **then**
  if Localizedreformaccessible **then**
    Set Patient$\leftarrow P_u$
    $I_i \leftarrow$ Localizedreform
    $I_i^n \leftarrow$ Add noise with I_i
    $I_i^{np} \leftarrow$ upgrade I_i^n
    $Patient^{reform} \leftarrow$ Trainprototype(Patient,I_i^{np})
    Transfer $Patient^{reform}$ to the validator
  end if
end if

Algorithm 4 iCPS's Algorithm

Claim: P_i^{reform} from stakeholder's and patient
Guarantee: $P_i^{reform} \neq P_i$ i =1 to 11
Method iCPS()
for each Repetition, r $\in$ Rj: j=1$\rightarrow$m do
Choose 11 stakholder's S_1 to S_n and Patient
for every Stakeholder,s$\in$Si:i=1 $\rightarrow$ 11 in parallel do **do**
  transfer Pu to Si
  for Patient , p$\in P_{patient}$
  transfer $Patient_u$ to Patient
end for
for every Stakeholder,s$\in S_i$:i=1$\rightarrow$11 in parallel do **do**
  P[i]$\leftarrow P_i^{reform}$
  for Patient,p$\in P_{patient}$
  $Patient_u \leftarrow Patient^reform$
end for
$P_u \leftarrow$ ProtypeiCPS(P) transfer P_u to all stakeholders and to the patient

point of view. the stakeholders and patient begins the training just after receiving the universal prototype and saving it as a localized prototype. Stakeholders and patients transfer the updated prototype to iCPS. The iCPS accumulate the prototype and transfer the updated prototype again to selected in further rounds till better accuracy is gained. Different classifiers are used for the study Decision tree as CL1, KNeighbours as CL2, Gaussian as CL3 and Randomforest as CL4, and the outcome is determined by the test score. which is calculated by using Eq. 3 and it shows that correction when the test's score rises.The prototype efficiency improves as the MSE value lowers, with the ideal model having a value of 0. Correlation grows while the R2 score improves. Table IV shows the comparison test scores for CL1, CL2, CL3, and CL4 by utilizing several techniques Gaussian Noise(GN) and Correlation Coefficient based model with Noise(CCBMWN).The test score using CL1 are 0.7205 and 0.7953 using CL2 are 0.7952 and 0.8067 using CL3 0.7678 and 0.8211 using CL4 are 0.8042 and 0.8812. The efficiency of the model is measured based on accuracy, specificity, and sensitivity. Results show that CCBMWN performs better than GN. So our method is better.

$$TestScore = \frac{x + y}{x + y + z + \in} \quad (3)$$

Where x,y,z, $\in$ are True positive(mean actual and predi-

TABLE III. CORRELATION COEFFICIENT VALUES FOR DIFFERENT FEATURES

Symbol	Description
Gender	0.05
Age	0.73
drug-uses	0.62
patient symptoms	0.58
disease prevention	0.65
design therapist plan	0.76
implementing therapeutic plan	0.66
monitoring therapeutic plan	0.56

cated value both are same as 1), True negative(with mean real and projected values are both 0), False positive (mean actual and predicated value both are different actual is 1 and predicted as 0)and False negative (mean actual and predicated value both are different actual is 0 and predicted as 1), respectively. The correlation coefficient value lies between -1 to +1. Table V displays the correlation value of the coefficient for each characteristic. The efficiency of the model is measured on the basis of accuracy, specificity, and sensitivity. Sensitivity is actual positive denoted by (λ) and calculated by using Eq. 4 and specificity is false actual negative denoted by (m_K) and calculated by using Eq. 5. ROC curve is used to show different thresholds by plotting and graphically.

$$\lambda = \frac{x+y}{x+\in} \tag{4}$$

$$m_K = \frac{y}{y+z} \tag{5}$$

$$AUC = \int_l^h f(x)dx \tag{6}$$

In above equation, the ROC is defined as Y=f(X), while both m and n are the curve's limit values. Fig. 7 is the curve for GN and Fig. 8 is for CCBMWN.

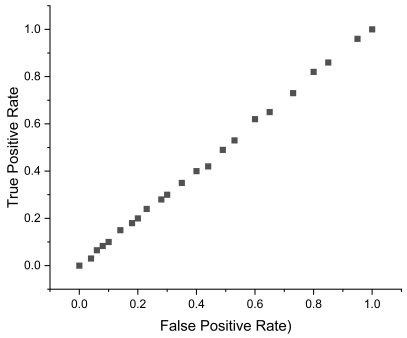


Fig. 7. ROC for GN.

The AUC (area under the ROC curve) is cognizance, received from ROC. It gives a clear picture of which technique is doing better. It is calculated using Eq. 6. In our research it is found that GN is 0.5032 and CCBMWN is 0.5108 which is better in CCBMWN. The comparison is shown in Fig. 9. The model's fulfillment is assessed using sensitivity, accuracy,

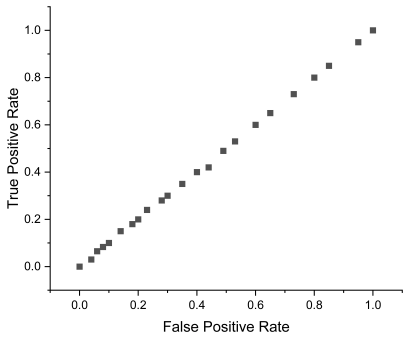


Fig. 8. ROC for CCBMWN.

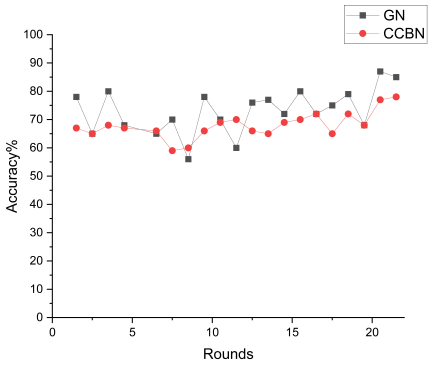


Fig. 9. Comparison of test score.

and specificity. A higher accuracy number indicates excellent accuracy, a higher sensitivity value indicates good prediction of genuine positive, and a higher specificity value indicates good prediction of true negative, as demonstrated in Fig. 10 and Fig. 11. In the first round, the sensitivity is 0.754 and at last, it is 0.82. The specificity is 0.65 in the first round and 0.67 in last round. The accuracy is 71% but the aggregate is 76.

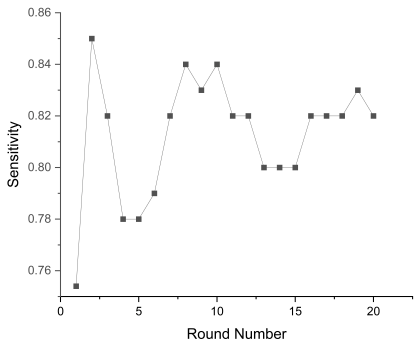


Fig. 10. Round wise sensitivity.

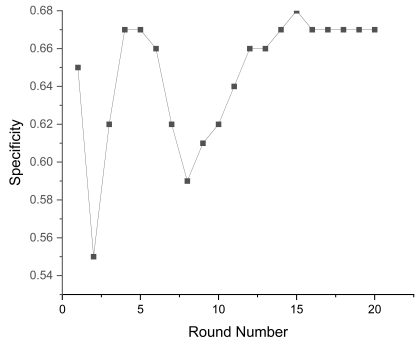


Fig. 11. Round wise specificity.

TABLE IV. DIFFERENT RESULT OF GN AND CCBMWN

Table Head	Test Scores	
	GN	*CCBMWN*
CL1	0.7205	0.7953
CL27	0.7952	0.8067
CL3	0.7678	0.8211
CL4	0.8042	0.8812

TABLE V. CORRELATION COEFFICIENT MATRIX OF FEATURES

	gender	age	drug-uses	patient symptoms	disease prevention	design therapist plan	implementing therapeutic plan	monitoring therapeutic plan
Gender	1	0.03	0.032	0.01	0.052	0.043	0.024	0.002
Age	0.03	1	0.62	0.35	0.56	0.23	0.05	0.34
drug-uses	0.032	0.62	1	0.52	0.43	0.10	0.45	0.52
patient symptoms	0.01	0.35	0.52	1	0.34	0.43	0.45	0.23
disease prevention	0.052	0.56	0.43	0.34	1	0.32	0.63	0.59
design therapist plan	0.043	0.23	0.10	0.43	0.32	1	0.66	0.56
implementing therapeutic plan	0.024	0.05	0.45	0.45	0.63	0.66	1	0.55
monitoring therapeutic plan	0.002	0.30	0.52	0.23	0.59	0.56	0.55	1

IX. CONCLUSION

In this study, an architecture has been proposed for user authentication in pharmaceutical care services. It can be used for secure communication whenever a patient wants to communicate and wants to avail of pharmaceutical care services. In problem analysis, it is observed that as compared to other methods the proposed method is strong. In this, the estimation and transmission value was analyzed. For providing privacy we have proposed a new technique CCBMWN which ensures privacy and results show that proposed method is giving good performance in contrast with existing methods. This study not only addresses the critical requirement for safe and confidential communication in AI-powered pharmaceutical treatment, but it also lays the groundwork for future advances in digitising healthcare operations and explicitly defining stakeholder responsibilities.

REFERENCES

[1] Kilincer, Ilhan Firat, Fatih Ertam, Abdulkadir Sengur, Ru-San Tan, and U. Rajendra Acharya. "Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization." Biocybernetics and Biomedical Engineering 43, no. 1 (2023): 30-41.

[2] Hepler, Charles D., and Linda M. Strand. "Opportunities and responsibilities in pharmaceutical care." American journal of hospital pharmacy 47, no. 3 (1990): 533-543.

[3] Kakhi, Kourosh, Roohallah Alizadehsani, HM Dipu Kabir, Abbas Khosravi, Saeid Nahavandi, and U. Rajendra Acharya. "The internet of medical things and artificial intelligence: trends, challenges, and opportunities." Biocybernetics and Biomedical Engineering 42, no. 3 (2022): 749-771.

[4] Jiao, Ying, Huamei Qi, and Jia Wu. "Capsule network assisted electrocardiogram classification model for smart healthcare." Biocybernetics and Biomedical Engineering 42, no. 2 (2022): 543-555.

[5] Jalali, Jalal, Ata Khalili, Atefeh Rezaei, Rafael Berkvens, Maarten Weyn, and Jeroen Famaey. "IRS-Based Energy Efficiency and Admission Control Maximization for IoT Users With Short Packet Lengths." IEEE Transactions on Vehicular Technology (2023).

[6] Turja, Tuuli, Iina Aaltonen, Sakari Taipale, and Atte Oksanen. "Robot acceptance model for care (RAM-care): A principled approach to the intention to use care robots." Information & Management 57, no. 5 (2020): 103220.

[7] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," IEEE Trans. Ind. Electron., vol. 65, no. 10, pp. 8153–8162, Oct. 2018.

[8] A. Karati, S. K. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced Industrial Internet of Things environments," IEEE Internet Things J., vol. 5, no. 4, pp. 2904–2914, Aug. 2018.

[9] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," IEEE Trans. Inf. Forensics Security, vol. 10, pp. 69–78, 2015.

[10] Thakur, Abhimanyu, Ambika P. Mishra, Bishnupriya Panda, Diana Rodríguez, Isha Gaurav, and Babita Majhi. "Application of artificial intelligence in pharmaceutical and biomedical studies." Current pharmaceutical design 26, no. 29 (2020): 3569-3578.

[11] Klumpp, Matthias. "Innovation potentials and pathways merging AI, CPS, and IoT." Applied System Innovation 1, no. 1 (2018): 5.

[12] Damiati, Safa A. "Digital pharmaceutical sciences." AAPS PharmSciTech 21, no. 6 (2020): 206.

[13] Jahromi, Amir Namavar, Hadis Karimipour, Ali Dehghantanha, and Kim-Kwang Raymond Choo. "Toward detection and attribution of cyber-attacks in IoT-enabled cyber–physical systems." IEEE Internet of Things Journal 8, no. 17 (2021): 13712-13722.

[14] Burki, Talha. "Pharma blockchains AI for drug development." The Lancet 393, no. 10189 (2019): 2382.

[15] Rathi, Vipin Kumar, Nikhil Kumar Rajput, Shubham Mishra, Bhavya Ahuja Grover, Prayag Tiwari, Amit Kumar Jaiswal, and M. Shamim Hossain. "An edge AI-enabled IoT healthcare monitoring system for smart cities." Computers & Electrical Engineering 96 (2021): 107524.

[16] Xu, Boyi, Li Da Xu, Yuxiao Wang, and Hongming Cai. "A distributed dynamic authorisation method for Internet+ medical & healthcare data access based on consortium blockchain." Enterprise Information Systems 16, no. 12 (2022):1922757.

[17] Hameed, Khizar, Ali Raza, Saurabh Garg, and Muhammad Bilal Amin. "A Blockchain-based Decentralised and Dynamic Authorisation Scheme for the Internet of Things." arXiv preprint arXiv:2208.07060 (2022).

[18] Babu, Erukala Suresh, Ilaiah Kavati, Soumya Ranjan Nayak, Uttam Ghosh, and Waleed Al Numay. "Secure and transparent pharmaceutical supply chain using permissioned blockchain network." International Journal of Logistics Research and Applications (2022): 1-28.

[19] Zukarnain, Zuriati Ahmad, Amgad Muneer, and Mohd Khairulanuar Ab Aziz. "Authentication securing methods for mobile identity: Issues, solutions and challenges." Symmetry 14, no. 4 (2022): 821.

[20] Lu, Yanrong, Ding Wang, Mohammad S. Obaidat, and Pandi Vijayakumar. "Edge-assisted intelligent device authentication in cyber-physical systems." IEEE Internet of Things Journal (2022).

[21] Ramasamy, Lakshmana Kumar, Firoz Khan, Mohammad Shah, Balusupati Veera Venkata Siva Prasad, Celestine Iwendi, and Cresantus Biamba. "Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring." Sensors 22, no. 3 (2022): 1076.

[22] Mishra, Ayaskanta, Amitkumar V. Jha, Bhargav Appasani, Arun Kumar Ray, Deepak Kumar Gupta, and Abu Nasar Ghazali. "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective." International Journal of System Assurance Engineering and Management (2022): 1-23.

[23] Makkar, Aaisha, and Jong Hyuk Park. "SecureCPS: Cognitive inspired framework for detection of cyber attacks in cyber–physical systems." Information processing & management 59, no. 3 (2022): 102914.

[24] Adil, Muhammad, Muhammad Khurram Khan, Muhammad Mohsin Jadoon, Muhammad Attique, Houbing Song, and Ahmed Farouk. "An AI-enabled hybrid lightweight Authentication scheme for intelligent IoMT based cyber-physical systems." IEEE Transactions on Network Science and Engineering (2022).

[25] Alzahrani, Naif, and Nirupama Bulusu. "Securing pharmaceutical and high-value products against tag reapplication attacks using nfc tags." In 2016 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1-6. IEEE, 2016.

[26] Janardhan, B., and P. Jagadeesh. "Accurate Deauthentication Attack Detection using Linear Discriminant Analysis in Comparison with Multilayer Perceptron." Journal of Pharmaceutical Negative Results (2022): 1764-1771.

[27] Tiwari, Devisha, Bhaskar Mondal, Sunil Kumar Singh, and Deepika Koundal. "Lightweight encryption for privacy protection of data transmission in cyber physical systems." Cluster Computing 26, no. 4 (2023): 2351-2365.

[28] Lian, Zhuotao, Qinglin Yang, Weizheng Wang, Qingkui Zeng, Mamoun Alazab, Hong Zhao, and Chunhua Su. "DEEP-FEL: Decentralized, efficient and privacy-enhanced federated edge learning for healthcare cyber physical systems." IEEE Transactions on Network Science and Engineering 9, no. 5 (2022): 3558-3569.

[29] Zhang, Zehui, Linlin Zhang, Qingdan Li, Kunshu Wang, Ningxin He, and Tiegang Gao. "Privacy-enhanced momentum federated learning via differential privacy and chaotic system in industrial Cyber–Physical systems." ISA transactions 128 (2022): 17-31.

[30] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," Comput. Security, vol. 88, Jan. 2020, Art. no. 101619.

[31] Q. Zheng, Q. Li, A. Azgin, and J. Weng, "Data verification in information-centric networking with efficient revocable certificateless signature," in Proc. IEEE Conf. Commun. Netw. Security (CNS), 2017, pp. 1–9.

[32] K. Xue, X. Zhang, Q. Xia, D. S. Wei, H. Yue, and F. Wu, "SEAF: A secure, efficient and accountable access control framework for information centric networking," in Proc. IEEE Conf. Comput. Commun. (INFOCOM), 2018, pp. 2213–2221.

[33] I. O. Nunes and G. Tsudik, "KRB-CCN: Lightweight authentication and access control for private content-centric networks," in Proc. 16th Int. Conf. Appl. Cryptogr. Netw. Security (ACNS), vol. 10892, 2018, pp. 598–615.

[34] T. Mick, R. Tourani, and S. Misra, "LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities," IEEE Internet Things J., vol. 5, no. 2, pp. 755–764, Apr. 2018.