Adversarial ML-based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare

Jitendra Kumar Samriya, Chinmay Chakraborty*, *Senior Member, IEEE*, Aditi Sharma, *Senior Member, IEEE*, Mohit Kumar, and Sravanth Kumar R

***Abstract*—The profound era of cloud computing (CC) is revolutionizing Industry 5.0in which users have online access to network services including better, transparent user management and the capacity to gather and analyze data. The services of the cloud paradigm have been adopted by academia, industries, healthcare, smart homes, and other areas due to cost-efficient and on-demand resources for IoT applications, but security and privacy of patient data is a major issue with cloud paradigm. For intrusion detection systems (IDS), adversarial machine learning (AML) has been promising to secure individual IoT devices from various modern threats. Network traffic anomalies brought on by both well-known assaults and recently discovered attacks are typically detected by adversarial machine learning-based intrusion detection systems (AML-IDS) in real time. This research proposes a novel technique in cloud security enhancement based on consumer IoT utilizing AML techniques in smart healthcare. The security of cloud networks is enhanced using trust-based encryption cryptographic analysis. The healthcare data is analyzed using structure-based Markov sparse Bayesian neural networks in smart healthcare. The experimental results are improved up to 9% in terms of data transmission ratio, specificity, training accuracy, validation accuracy, and security analysis.**

***Index Terms*—Adversarial Machine Learning (AML), cloud security enhancement, consumer IoT, cryptographic analysis, Industry 5.0, smart healthcare.**

I. INTRODUCTION

Demand for mobile devices (MDs) is rapidly rising due to the rapid growth of mobile networks and extensive use of city Internet of Things (IoT) in numerous industries. memory capacity, power reserve, and sustainability consciousness, are typically constrained [1]. Resources available to MDs, such as central processing power, Examples of these resources include smartphones, tablets, unmanned aerial vehicles (UAVs), and wearable technology. There is a diverse set of smart cities IoT applications exist, comprising both delay-tolerant and delay-sensitive ones, which can also result in a wide range of varied compute and transmission costs. Offloading the upcoming IoT workload from MDs to a central cloud is an efficient technique to reduce the constraints of mobile computation capacity. We can relieve some of the burden on mobile devices to handle jobs locally by utilizing abundant virtual resources as well as the quick processing speed of cloud servers. Mobile cloud computing (MCC) has received a lot of attention as a way to transfer task burdens to cloud data centres with lots of processing power [2]. However, this strategy still confronts numerous difficulties, including high latency, poor bandwidth, and network congestion, because of restrictions of centralised service mode and access bandwidth. Healthcare firms may be able to take advantage of cost savings by outsourcing computing activities thanks to cloud computing. The application of this idea enables users to utilise cloud-based imaging systems to remotely process patients' electronic health data. The key advantage of this idea is that imaging applications may be made widely accessible without the need to purchase and maintain these instruments. It is widely acknowledged that the management, storage, processing, and usage of health records have all undergone a complete revolution thanks to cloud computing [3]. To support E-health systems and address the expanding demand for healthcare services, cloud providers offer a wide range of health solutions in this model. This suggests that since the cloud has great benefits for healthcare businesses, there will be a significant increase in demand for cloud adoption. In contrast to a traditional paradigm, using the cloud raises security concerns because client data is frequently processed and stored on remote data centres. Quite a few elements, such as virtualization security hazards, data storage location issues, potentially insecure storage web technology, system interoperability problems, and regulatory restrictions, might have an impact on cloud solution considerations [4]. However, these methods frequently fall short of QoS (quality of services) requirements, which are clearly stated in the Service Level Agreement (SLA). Firstly, digital records are large and latency-sensitive and need more processing power within a minimum time. Second, these safeguards are still insufficient in terms of compliance with medical data privacy laws. A range of applications, including intrusion detection systems (IDS), have recently shown the usefulness of machine learning approaches. Since learning-based approaches can train models to manage a tonne of complex, changing data utilising huge

Jitendra Kumar Samriya is with Indian Institute of Information Technology, Sonepat, (e-mail: jitu.samriya@gmail.com)

Chinmay Chakraborty is with Birla Institute of Technology, Jharkhand, India, (e-mail: cchakrabarty@bitmesra.ac.in)

Aditi Sharma is with Symbiosis Institute of Technology, SymbiosisInternational (Deemed University), Pune, (e-mail: aditi.sharma@ieee.org)

Mohit Kumar is with Dr. B.R, Ambedkar National Institute of Technology, Jalandhar (e-mail: kumarmohit@nitj.ac.in)

Sravanth Kumar R is with VNR VJIET, (e-mail: sravanthkumar_r@vnrvjiet.in)

*Corresponding author – Chinmay Chakraborty, Aditi Sharma

datasets, they may be useful for security applications. Such learning models can be combined with firewalls to improve their efficiency. The efficiency of anomaly detection would be significantly increased by a well-trained model with a variety of attack types at a reasonable cost and complexity.IDS models have already been the subject of a significant amount of research in recent years. However, there are two difficulties in categorising different attack types and applying such studies to multi-cloud environments. Most researchers in this domain have focused on anomaly detection problems without any consideration for categorizing the attacks. We argue that this classification is crucial for locating system weaknesses and putting in place the required defences and countermeasures against different sorts of attacks [5]. The research offers the following contributions:

- To propose a novel method for enhanced cloud security for consumer IoT utilizing adversarial ML technique in smart healthcare.
- To offer healthcare services with minimum delay, energy, and high accuracy over the cloud platform. This effort was driven by the dearth of models or frameworks that combine the strength of deep learning models with cryptographic analysis that improve the security of cloud networks.
- The proposed work used clustering method to improve the energy efficiency. The user subsystem, cloud subsystem, and alert subsystem are the three main components that the described technique.
- The user subsystem first contributes to the data collecting process when IoT medical devices are used by an individual. Structure-based markov sparse Bayesian neural networks have been used in smart healthcare to interpret healthcare data.

II. Related works

IoT is the connecting of multiple physical items to continuously observe the events. Advanced wireless networks and sensors are used to communicate with one another in connected IoT [6].Privacy and security of data play a crucial role in IoT system, and infrastructure. The lacks of secure encryption algorithm and protocols collapse the IoT infrastructure. Authors have proposed a lightweight attack detection model that perform multiclass classification, optimal feature selection to detect the attacks. The developed lightweight model focused at some basic attacks and need the improvement. In IoT-based frameworks, RFID tags, sensors, and actuators are frequently used. Healthcare initiative created by Harvard University is called CodeBlue project. Monitoring of people's health indicators using ECG, EKG, EMG, SpO2, pulse oximeters, and Mica2 motes is crucial to the CodeBlue project's success [9]. The CodeBlue initiative makes use of a variety of electronic tools, including PDAs, laptops, and personal computers, to enable doctors and caretakers to take the appropriate action when a patient's health deteriorates [10]. Artificial Intelligence (AI) based models especially machine learning and deep learning are required to secure the IoT network. Authors have discussed various cyber attacks and their solutions along with limitations for IoT network [11].Acquisition, analysis and aggregation of collected healthcare data is a crucial step that determine the efficiency and effectiveness of proposed system. We need to push such data at network edge for processing and decision, but it brings with some security challenges. Therefore, authors have proposed a cost effective, and scalable approach to execute the data over fog environment and secured by blockchain technology [12]. To store and analysis of data is a challenging issue, authors have used machine learning based model for secure storage and retrieval of data by ML model [13] to overcome the issues. Moreover, authors have presented deep learning based secure framework using blockchain technology for smart healthcare system [14]. The developed framework ensures secure transaction by orthogonal particle swarm optimization, hash value encryption by NIS algorithm and medical diagnosis using deep neural network.

AI based models are deployed over the cloud datacenters because IoT devices are resource constraints and cannot analyze the massive amount of data [15]. The main issue with this work is to analyze and process the latency sensitive applications. The authors rigorously reviewed several ML/DL based approaches and intrusion detection system to detect the anomalies in the network and found that few ML based approaches detect the adversary with high accuracy [16]. Sometimes healthcare data in images form where ML fail to predict the results and need to apply the DL based models to find the accuracy and other decision parameters [17] to secure and improve the healthcare system. To detect and monitoring the COVID-19 symptoms, authors have proposed ML based model over the data collected by IoT sensor devices and find the prediction so that early decision can be taken before reaching to severe condition [18] [20].

Accuracy, latency, monitoring and security are major issues with advanced healthcare system. Cloud assisted deep learning-based approach has been depicted by the authors in which DL model is deployed over cloud where IoT based collected data (heart rate, blood pressure etc) is process [19] and improved the communication efficiency and accuracy. The preceding discussion highlights the significant effort that has been devoted to investigating IoT security [21]. Nevertheless, research in this area is still in its early stages, and the full scope of asset management for IoT terminal devices throughout their life cycles has yet to be fully addressed. Meanwhile, blockchain technology has gained the attention of both academics and businesses [22]. Based on a decentralized peer-to-peer network, blockchain technology enables data traceability and verification, integrating consensus procedures, time-series data, and encryption technology. In the meantime, sharing and privacy protection are also ensured.

III. System Model

This section discusses novel method in cloud security enhancement based on consumer IoT utilizing Adversarial ML technique for smart healthcare. The security of cloud network is enhanced using trust encryption cryptographic analysis. the healthcare data has been analyzed using structure based markov

sparse Bayesian neural networks(SMBNNs) for smart healthcare.The role of SMBNNs is very crucial in advance healthcare system. It improves predictive accuracy of models and disease diagnosis. By analyzing patient data such as medical images, genomic sequences, and clinical records, SMBNNs can identify subtle patterns and biomarkers associated with specific diseases. This can aid clinicians in making early and accurate diagnoses, potentially saving lives and reducing healthcare costs. It can be used to monitor the progress of patients continuously and analyze the diseases or patients' health condition based upon the data collected from wearable devices, electronic health records, and medical imaging. Healthcare providers can use this information to make timely interventions and adjustments to treatment plans that leads to improve the efficiency.

The proposed IoT enabled cloud architecture is given in figure 1. Stakeholders uses different IoT devices to collect the data of patients and send the data over the wired or wireless channel in secure manner to computing paradigm (edge or cloud) for processing and analyzing. Big medical data is used to configure a sizable medical database and provide IoT endpoints to cloud paradigm over the internet, enhancing medical services. Sending and receiving requests over the cloud is the responsibility of the cloud broker, who serves as a mediator. Heterogeneous types of data is collected from the patients and provides the services based upon the conditions of patents or level of dieses. If condition of patients is severe then an alarm is generated to provide the immediate healthcare services to patient i.e., priority is given to such types of patients.

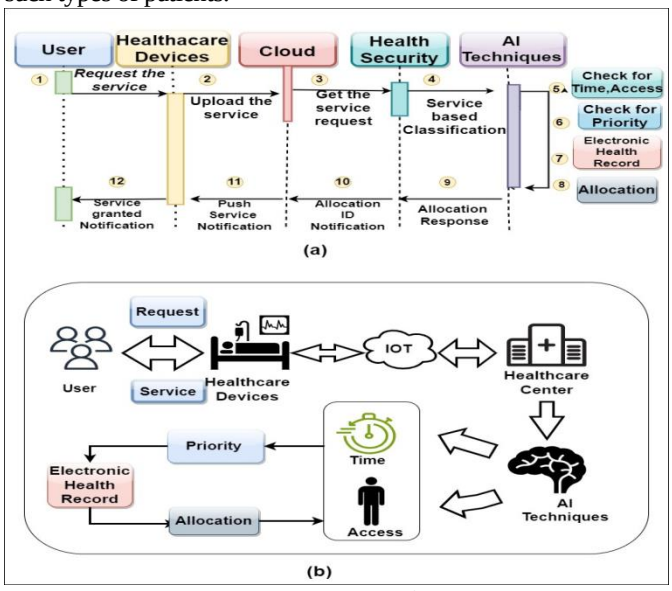

Fig.1. Intelligent model of cloud-IOT

Every network may have a number of application hosts, such as "Host1, Host2,, and Hostn," that offer SaaS and assigned to carry out requests from cloud stakeholders. For the upcoming requests from stakeholders. A network administrator is in charge of organizing communication between hosts on each network as well as between that network and other networks in the clouds. The role of the network administrator is to implement the most effective intelligent techniques to determine the best selection of VMs (virtual machines).

Trust encryption cryptographic analysis:

User Registration subsystem: During this sub-phase, the end user *(Ui)* is registered by the control server*(CS)*. *Ui* and *CS* communicate with each other via a secure connection. The subsystem consists of the following steps:

Step1. Initially user $U_i$chooses an identity (ID_i), pseudoidentity (PID_i), password (PW_i), and nonce (b_i).Afterthat user send the request packet M_1 to CS to establish the connection.

Step2. CS evaluates$C_1^* = h(PID_i \parallel ID_{CS} \parallel x)$and $C_2^* = h(ID_i \parallel x)$. $M_2 = \{C_1, C_2, ID_{CS}\}$to U_i. Control server evaluate the packet coming from user side and after verifying the authentication, it sends the message M_2 to user side, where h represents the hash of message.

Step3. After receiving registration response message M_2, U_ievaluates$C_1 = C_1^* \oplus HP_i, C_2 = C_2^* \oplus h(ID_i \parallel HP_i)$and $C_3 = b_i \oplus h(ID_i \parallel PW_i)$, and stores all the information$(C_1, C_2, C_3, PID_i, ID_{CS})$ in his smart card.

Step4. Cloud server is represented by $S_j$chooses an identity (SID_j) and pseudo-identity $(PSID_j)$. Then, S_j sends registration request message $M_3 = \{SID_j, PSID_j\}$ to CS.

Step5. Upon receiving registration request from S_j for message M_3, CS evaluates$B_1 = h(PSID_j \parallel ID_{CS} \parallel x)$and $B_2 = h(SID_j \parallel x)$, $M_4 = \{B_1, B_2, ID_{CS}\}$ to S_j.

Step6. After S_j receives registration response message M_4, S_jstores $(B_1, B_2, SID_j, PSID_j, ID_{CS})$.

Authentication Phase

Step1. After registering successfully by the users U_i, they required the services in secure manner from control server and need the authentication to access the services S_j. After that, $U_i$evaluates $b_i = C_3 \oplus h(ID_i \parallel PW_i), HP_i = h(PW_i \parallel b_i), C_1^* = C_1 \oplus HP_i, C_2^* = C_2 \oplus h(ID_I \parallel HP_I), D_1 = C_1^* \oplus r_U, D_2 = h(PID_i \parallel ID_{CS} \parallel r_U) \oplus ID_i, D_3 = C_2^* \oplus h(ID_i \parallel HP_i) \oplus PID^{new} \oplus h(r_U \parallel ID_i)$, and $D_4 = h(ID_i \parallel PID_i \parallel PID_i^{new} \parallel r_U \parallel D_3)$. Then, U_i sends authentication request message $M_5 = \{PID_i, D_1, D_2, D_3, D_4\}$ to S_j through an open communication channel.

Step2. After submitting the credential for secure authentication by the end users, the credential is validated at server side as, S_j evaluates $S_j$evaluates $D_5 = B_1 \oplus r_S, D_6 = h(r_S \parallel PSID_j \parallel ID_{CS}) \oplus SID_j, D_7 = B_2 \oplus PSID_j^{new} \oplus h(r_S \parallel SID_j)$, and $D_8 = h(SID_j \parallel PSID_j \parallel PSID_j^{new} \parallel r_S \parallel D_7)$. Finally, S_j sends authentication request message $M_6 = \{PID_i, D_1, D_2, D_3, D_4, PSID_j, D_5, D_6, D_7, D_8\}$ to CS through an open communication channel.

Step3. CS evaluates$r_U = D_1 \oplus h(PID_i \parallel ID_{CS} \parallel x), ID_i = D_2 \oplus h(r_U \parallel PID_i \parallel ID_{CS})$, and $PID_i^{new} = D_3 \oplus h(ID_i \parallel x) \oplus h(r_U \parallel ID_i)$. CS evaluates$r_S = D_5 \oplus h(PSID_j \parallel ID_{CS} \parallel x), SID_j = D_6 \oplus h(r_S \parallel PSID_j \parallel ID_{CS})$, and $PSID_j^{new} = D_7 \oplus h(SID_j \parallel x) \oplus h(r_S \parallel SID_j)$. CS chooses random number (r_{CS}) and evaluates session key $SK_{CS} =$

$h(r_U \oplus r_S \oplus r_{SC})$. Later, CS evaluates $D_9 = h(PSID_j^{neav} \parallel ID_{CS} \parallel x)$

Login and Authentication Phase

In this phase, mutual authentication is carried out byUi andSj with the help of CS.

Step1. U_i inputs his identity ID_i^* and password PW_i^* and imprints biometric b_i^*. If it holds, smart card evaluates$O_i = t_i \oplus H_1(T_1 \parallel H_1(y \parallel r_1)), C_i^* = D_i \oplus A_i^*, R_i = T_\alpha(x)$, and $L_i = H_1(ID_i^* \parallel C_i^* \parallel R_i \parallel SID_j \parallel O_i \parallel T_1)$.

Step2. after getting $\{PID_i, R_i, L_i, O_i, T_1\}, S_j$ verifies whether T_1 is fresh. If it holds, $S_j$produces a random number β and evaluates $R_S = T_\beta(x), G_i = H_1(P_{ID} \parallel R_i \parallel R_S \parallel sm_j \parallel T_2), Q_i = H_1(sm_j \parallel R_i)$, and $N_i = E_{Q_j}(R_S \parallel G_i)$, where T_2 is current timestamp. $S_j$sends$\{PID_i, R_i, L_i, O_i, T_1, N_i, T_2\}$ to CS via public channel.

Step3. After receiving $\{PID_i, R_i, L_i, O_i, T_1, N_i, T_2\}, CS$ checks freshness of T_2 and evaluates$(ID_i \parallel r_1^{'}) = D_y(PID_i), t_i^{'} = O_i \oplus H_1\left(T_1 \parallel H_1(y \parallel r_1^{'})\right), C_i = H_1(s \parallel ID_i)$, and $L_i^{'} = H_1(ID_i \parallel C_i \parallel R_i \parallel SID_j \parallel O_i \parallel T_1)$and verifies $t_i^{''} = t_i, L_i^{'?} = L_i$. If $t_i^{'} = t_i, L_i^{'} \neq L_i$, smart card is probably compromised. CS executes "Counter = Counter + 1" is executed by CS for the item "ID_i, t_i".If the predetermined value is reached, CS suspends U_i. However, if $t_i{'}$ equals $t_i$and $L_i^{'}$ equalsL_i, CS accepts the veracity of U_i and proceeds to the next stage.

Step4. CS computes $m_j = H_1(SID_j \parallel s), Q_i = H_1(sm_j \parallel R_i), (R_S^{'} \parallel G_i^{'}) = D_{Q_i}(N_i)$, and $G_i^{''} = H_1(PID_i \parallel R_i \parallel R_S^{'} \parallel sm_j \parallel T_2)$, and verifies $G_i^{'} \oplus G_i^{''}$. If it holds, CS believes authenticity of S_j.

Step5. CS picks a nonce r_2, evaluates$PID_i^{new} = E_y(ID_i \parallel r_2), K_i = H_1(C_i \parallel R_i), F_i = E_K(Q_i \parallel R_S^{'} \parallel PID_i^{new})$, and $M_1 = H_1(sm_j \parallel R_i \parallel F_i \parallel T_3)$, where T_3 is current timestamp. CS transmits $\{F_i, M_1, T_3\}$ to S_j through open channel.

Step6. after getting $\{F_i, M_1, T_3\}, S_j$ checks freshness of T_3 and evaluates$M_1^{'} = H_1(sm_j \parallel R_i \parallel F_i \parallel T_3)$, and verifies $M_1^{'} =^i M_1$. If they are equal, S_j authenticates user U_i successfully. $S_j$computes $E_i = T_\beta(R_i), SK = H_1(E_i \parallel Q_i)$, and $M_2 = H_1(SK \parallel F_i \parallel Q_i \parallel T_4)$. $S_j$transmits$\{F_i, M_2, T_4\}$ to U_i via public channel.

Step7. upon receiving $\{F_i, M_2, T_4\}$, smart card checks freshness of T_4. Then, smart card evaluates$K_i = H_1(C_i^* \parallel R_i), (Q_i^{'} \parallel R_S^{n} \parallel PID_i^{new}) = D_{K_i}(F_i), \quad E_i = T_a(R_S^{''}), SK = H_1(E_i \parallel Q_i^{'})$,and $M_2^{'} = H_1(SK \parallel F_i \parallel Q_i^{'} \parallel T_4)$, and checks $M_2^{'} = M_2$. If it holds, U_i authenticates cloud server S_j successfully. Smart card replaces PID_i with PID_i^{new} in memory.

Password Update Phase:

In this stage, original password is changed for a new one.

Step1. U_i enters ID_i^* and PW_i^* and imprints b_i^*. Smart card evaluates$A_i^* = H_1(PW_i^* \parallel H_2(b_i^*))$and $Z_i^* = H_1(A_i^* \oplus ID_i^*) mod \mu$. If they are not equal, protocol terminates. Step 2: U_i keys a new password $PW_i^{new.}$. Smart card evaluates$A_i^{new} = H_1\left(PW_i^{new} \parallel H_2(b_i^*)\right), Z_i^{new} = H_1(A_i^{new} \oplus ID_i^*) mod \mu$, and $D_i^{new} = D_i \oplus A_i^* \oplus A_i^{new}$ .The smart card replaces Z_i, D_i, with Z_i^{new}, D_i^{new} .

First of all, as indicated in Fig. 2, layer of data is lowest plane in design. This plane design provides gateway with SDN (software defined network) support for properly connecting the sensor-based devices. Additionally, it provides two separate switches that link to software-based switches, like virtual switches, that commonly run Linux OS. This frequently transitions to network-based systems that can send, receive, and exchange network packets. Additionally, networking devices and SDN controllers frequently communicate among each other with the help of more dependable connectors. The SDN controller(s) and data plane then communicate with one another via OpenFlow protocol. All protected data then moves on to SDN architecture's control layer. The data plane is also in charge of gathering all data in cloud. environment.

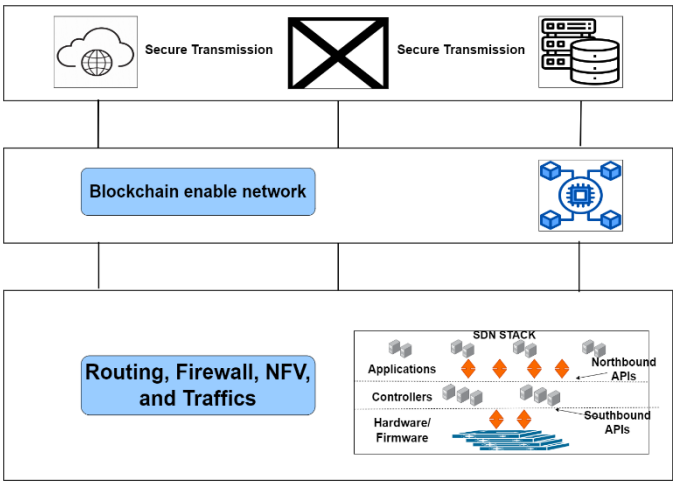

Fig.2. Secure cloud network analysis

Markov sparse Bayesian neural networks:

Structural learning strategy can be used to reduce the maximum in-degree. In real-world applications, we examine outcome of following optimization to shorten several class-to-feature arcs in Gi: Where sets of graphs should be designed to include one another in the arcs space, then by eq. (1), $G_i^* = arg\ max_{G_i \subset G \subset G_i} log\ P(G \mid D)$

$$log\ P(G \mid D) = \sum_{i=1}^{n} \psi_\alpha[C_i, Pa(C_i)] + \sum_{j=1}^{m} \psi_\alpha[F_j, Pa(F_j)] \quad (1)$$

$$\sum_{i=1}^{|Pa\,(F_j)|} \left[log\ \frac{\Gamma(\alpha_j)}{\Gamma(\alpha_j + N_{ji})} + \sum_{k=1}^{|F_j|} log\ \frac{\Gamma(\alpha_{ji} + N_{jik})}{\Gamma(\alpha_{ji})} \right]$$

where the first sum is made up of all of its parents' states combined and the second sum is made up of all of Fj's potential states. Finally, whileα j = P I ji, αji is equal to divided by sum of (joint) states of parents of Fj and number of states of Fj.

Consider a network that is linked to a particular class event. Since linkages between class events are fixed, class variables in all graphs in search space have the same parents.As a result, the optimization in (3) can be finished by just taking the

features into account. Any subset of C may be the parents set of a feature, which simplifies issue to m different local optimizations by eq. (2)

$$C_{F_j} = arg\ max_{Pa\,(F_j)\subseteq C}\psi_a[F_j, Pa(F_j)] \quad (2)$$

For every $j = 1$ instance, m. Bipartite separation of class events and features makes this conceivable. Assume that X is collection of query variables, Z is set of additional variables, and k is number of mixture components. We can determine marginal distribution of X by eq. (3) by summing up C and Z:

$$P(X = x) = \sum_{c=1}^{l}\sum_z P(C = c, X = x, Z = z)$$

$$= \sum_{c=1}^{k}\sum_z P(c)\prod_{i=1}^{|x} P(x_i \mid c)\prod_{j=1}^{|4} P(z_j \mid c) \quad (3)$$

$$P(A_i \mid B) = \frac{P(B|A_i)P(A_i)}{\sum_{j=1}^{n} P(B|A_j)P(A_j)} \quad (4)$$

Feedback on backward errors: Initial weights are either random or empirical values. These weight values are modified using the backward error feedback method, which involves providing feedback on the classification accuracy to enhance accuracy of learning system's final output. Then lower layer connection error derivative by eq (5)

$$\frac{\partial E}{\partial z_{Nj}} = \frac{\partial E}{\partial y_{Nj}}\frac{\partial y_{Nj}}{\partial z_{Nj}} \quad (5)$$

where$\partial E/\partial y_{Nj} = y_{Nj} - t_{Nj}$ and $j = 1,2,\cdots,L_N$. For j-th node of layer $i(i = 1,2,\cdots,N-1)$, denoted as $\partial E/\partial y_{ij}$. Next, lower layer connection's error derivative by eq (6)

$$\frac{\partial E}{\partial z_{ij}} = \frac{\partial E}{\partial y_{ij}}\frac{\partial y_{ij}}{\partial z_{ij}}, \quad (6)$$

where $\frac{\partial E}{\partial y_{jj}} = \sum_{k=1}^{L_{i+1}} w_{jk}^{i+1}\frac{\partial E}{\partial z=1,l}, i = 1,2,\cdots,N-1,$ and $j = 1,2,\cdots,L_i,$

The agent's objective is to maximise the total reward Qt via eq (7)

$$\max_{\pi} Q_t = maxE_{\pi}\,(r_t + \gamma r_{t+1} + \gamma^2 r_{t+2} + \cdots \mid s_t = s, a_t = a, \pi) \quad (7)$$

Agent's experience, et = (st, at, rt, st+1), is recorded in experience pool U and can be replayed at any time (D). The agent randomly selects a sample of stored experience each time it needs to take an action throughout learning method. So, by eq (8),

$$L_i(\theta_i) = E_{(s,a,r,s')\in U(D)}\left(\left(r + \gamma \max_{a} Q(s', a', \theta_i^-) - Q(s, a, \theta_i)\right)^2\right) \quad (8)$$

One-point connection capability k(1) t (x) measures anticipated specialist thickness at area x, so normal number of specialists inside an area L is registered by eq. (9,10)

$$E(|\gamma_t \cap A|) = \int_A k_t^{(1)}(x)dx. \quad (9)$$

$$E(|\gamma_t \cap A_1 \parallel \gamma_t \cap A_2|) = \int_{A_1}\int_{A_2} k_t^{(2)}(x_1, x_2)dx_2dx_1 + \int_{A_1\cap A_2} k_t^{(1)}(x)dx \quad (10)$$

Thespatio-transient connection capability of the essential model as eq. (11)

$$k_{t,\Delta t}(x, y) = k_{\Delta t}^{OO}(x, y) + k_{\Delta t}^{O+}(x, y) + k_{\Delta t}^{-O}(x, y) + k_{\Delta t}^{-+}(x, y)$$

$$k_{t,\Delta t}(x) = k_{\Delta t}^{O}(x) \quad (11)$$

the following Markovianity property is also satisfied by eq. (12,13):

$$p(X_{st} = x_{st} \mid X_{qr} = x_{qr}, s \neq q, t \neq r, \forall(s,t), (q,r) \in V) \quad (12)$$

$$= p(X_{st} = x_{st} \mid X_{qr} = x_{qr}, s \neq q, t \neq r, (q,r) \in \eta_{sr}) \quad (13)$$

The term $z^g\langle k^g\rangle f(n_i^{eff}/s_i)$in Eq. (14) addresses the general number of contacts, which increments with the thickness of fix I following capability f, and furthermore represents the standardization factor z g , which is determined as eq. (14):

$$z^g = \frac{N^g}{\sum_{i=1}^{N} f\left(\frac{n_i^{eff}}{s_i}\right)(n_i^g)^{eff}} \quad (14)$$

where the effective population at patch i is given by eq. (15)

$$z^g = \frac{N^g}{\sum_{i=1}^{N} f\left(\frac{n_i^{eff}}{s_i}\right)(n_i^g)^{eff}} \quad (15)$$

Let$X_i = \{0,1,\ldots,r_i - 1\}\ forall\ i \in [n]\ and\ Y_j = \{0,1,\ldots,s_j - 1\}$ The graphical model with full bipartite interactions $\{\{i,j\}: i \in [n], j \in [m]\}\ on\ X \times Y$ is the exponential family as shown in eq. (16), (17)

$$E_{X,Y} := \left\{\frac{1}{Z(\theta)}exp\left(\langle\theta, A^{(X,Y)}\rangle\right): \theta \in R^{d_X d_Y}\right\} \quad (16)$$

$$p(V, h) = \frac{1}{Z}exp\,(-E(V, h)) \quad (17)$$

with adequate insights lattice equivalent to the Kronecker item A^((X,Y))=A^((X))⊗A^((Y)) of the adequate measurements frameworks A^((X)) and A^((Y)) of the autonomy models EX and EY . The lattice A(X,Y) has $d_X d_Y = \left(\sum_{i\in[n]}(|X_i| - 1) + 1\right)\left(\sum_{j\in[m]}(|Y_i| - 1) + 1\right)$straightly free lines and |X × Y| segments, every section comparing to a joint state (x, y) all things considered. Dismissing the passage of θ that is duplicated with the consistent column of A(X,Y) , which counteracts with the standardization capability Z(θ), this definition of EX,Y is balanced. Specifically, this model has aspect$dim\,(E_{X,Y}) = d_X d_Y - 1$ as shown in eq. (18)

$$RBM_{X,Y} := \{q(x) = \sum_{y\in Y} p(x, y)\text{for all } x \in X: p \in E_{X,y}\}$$

$$Z = \sum_{V,h} exp\,(-E(V, h)) \quad (18)$$

RBMs are energy-based models, with most extreme probability as the learning objective. The energy of the arrangement of its apparent factors v and secret factors h working together is given by eq. (19), eq. (20)

$$E(v, h; \theta) = -\sum_{ij} W_{ij} v_i h_j - \sum_i b_i v_i - \sum_j a_j h_j \quad (19)$$

$$p(V) = \frac{1}{Z}\sum_h exp\,(-E(V, h)) \quad (20)$$

IV. Performance analysis

A mobile blockchain network is considered in our simulation, along with one IoT device and mining activities, one MEC server, and one MCC server. IoT device, MEC server, and MCC server each have computation capabilities set to fIoT = 500 MHz, fedge = 3 GHz, and fcloud = 5 GHz, which satisfy equation fIoT<fedge<fcloud[6]. As an illustration, let's assume that there are N = 5 jobs in application on IoT device. According to measurements, we assume that ptr>pex>pidle and that transmission power, processing power, and idle power of IoT device are fixed at 1.3 W, 0.9 W, and 0.3 W. MATLAB is used as simulation tool to assess the performance

of proposed research work.

Dataset description:

Our methodology was validated using five representative event-based classification datasets, namelyN-MNIST (N-M), NCaltech101 (N-Cal), CIFAR10-DVS (CIF10), N-CARS (N-C), and ASL-DVS(ASL)[23,24,25].

Table-1 gives analysis for various secure healthcare dataset. the dataset compared are N-MNIST (N-M), NCaltech101 (N-Cal), CIFAR10-DVS (CIF10), N-CARS (N-C) and ASL-DVS (ASL) in terms of data transmission ratio, specificity, training accuracy, validation accuracy, security analysis.

TABLE1

COMPARATIVE ANALYSIS BASED ON VARIOUS SECURE HEALTHCARE DATASET

Dataset	Techniques	Data transmission ratio	Specificity	Training accuracy	Validation accuracy	Security analysis
N-MNIST (N-M)	DBN	71	65	77	62	69
	IPFIX	73	68	79	64	72
	CA_SE_IoT_ MSL_SH	75	71	81	68	73
NCaltech101 (N-Cal)	DBN	72	69	79	64	73
	IPFIX	74	72	82	68	75
	CA_SE_IoT_ MSL_SH	76	73	83	69	77
CIFAR10-DVS (CIF10)	DBN	77	73	82	66	79
	IPFIX	79	75	86	69	82
	CA_SE_IoT_ MSL_SH	81	77	88	72	83
N-CARS (N-C)	DBN	79	75	83	69	81
	IPFIX	82	79	85	73	83
	CA_SE_IoT_ MSL_SH	83	81	86	75	85
ASL-DVS (ASL)	DBN	82	81	85	72	82
	IPFIX	84	83	89	74	86
	CA_SE_IoT_ MSL_SH	86	85	92	76	89

A privacy-isolation zone is established at the source to capture non-speech body sounds and data. The security of cloud-based storage and data transfer is further guaranteed by this. These guarantees start to finish security assurance for clinical information. In order to estimate the system's performance, privacy leakage and data tampering attacks are tested.SMBNNs is a special neural network that attains efficiency through multilayer architecture. It uses a multivariate Gaussian with a diagonal covariance matrix as the proposed approximation distribution.

The user's identity and gait information are often combined with other health-related data, gestures, and movements collected by the wearable device. In the event of a data breach from the cloud, a malicious user could separate the gait information from the data and compromise the user's privacy.

Therefore, it is essential to analyze and divide the data in the privacy-isolation zone prior to uploading it to the cloud. A smooth window function is used to make the signal zero outside the boundary and keep it there. Duplication is performed between the assembled signal and the sign inside the limit. Within the boundary, the signal can be extracted using a predetermined threshold value. In addition to the gait data, the collected data also contains information about gravity. The gravity's fixed downward force is 9.8 m/s2. Because the gravity projection will change on each axis, it is difficult to establish a fixed threshold given the user's motion. Fig.3 gives analysis based on N-MNIST (N-M), NCaltech101 (N-Cal) dataset.

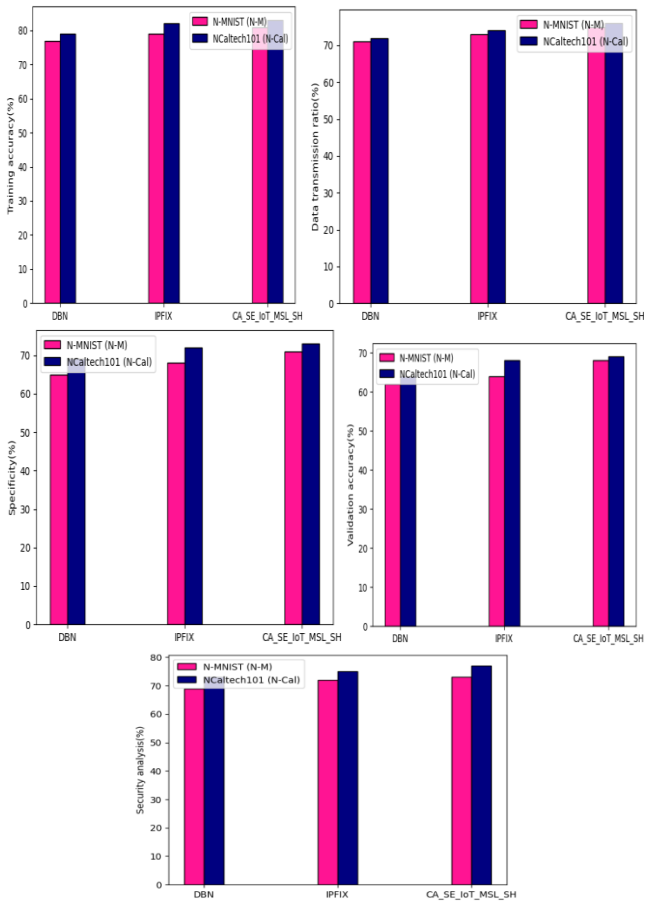

Fig.3. Analysis for N-MNIST (N-M), NCaltech101 (N-Cal) dataset

The proposed technique attained data transmission ratio of 75%, specificity of 65%, training accuracy of 85%, validation accuracy of 75%, security analysis of 81%, existing DBN attained data transmission ratio of 71%, specificity of 65%, training accuracy of 77%, validation accuracy of 62%, security analysis of 69%, IPFIX attained data transmission ratio of 73%, specificity of 68%, training accuracy of 79%, validation accuracy of 64%, security analysis of 72% for N-MNIST (N-M) dataset, for NCaltech101 (N-Cal) dataset proposed technique attained data transmission ratio of 79%, specificity of 69%, training accuracy of 89%, validation accuracy of 79%, security analysis of 85%, existing DBN attained data transmission ratio of 72%, specificity of 69%, training accuracy of 79%, validation accuracy of 64%, security analysis of 73%, IPFIX attained data transmission ratio of 74%, specificity of 72%, training accuracy of 82%, validation accuracy of 68%, security analysis of 75%.

Fig.4 analysis for CIFAR10-DVS (CIF10), N-CARS (N-C) and ASL-DVS (ASL) dataset is shown. Proposed technique attained data transmission ratio of 81%, specificity of 77%, training accuracy of 88%, validation accuracy of 72%, security analysis of 83%, existing DBN attained data transmission ratio of 77%, specificity of 73%, training

accuracy of 82%, validation accuracy of 66%, security analysis of 79%, IPFIX attained data transmission ratio of 79%, specificity of 75%, training accuracy of 86%, validation accuracy of 69%, security analysis of 82% for CIFAR10-DVS (CIF10) dataset.

For N-CARS (N-C) dataset proposed technique attained data transmission ratio of 83%, specificity of 81%, training accuracy of 86%, validation accuracy of 75%, security analysis of 85%, existing DBN attained data transmission ratio of 79%, specificity of 75%, training accuracy of 83%, validation accuracy of 69%, security analysis of 81%, IPFIX attained data transmission ratio of 82%, specificity of 79%, training accuracy of 85%, validation accuracy of 73%, security analysis of 83%; proposed technique attained data transmission ratio of 86%, specificity of 85%, training accuracy of 92%, validation accuracy of 76%, security analysis of 89%, existing DBN attained data transmission ratio of 82%, specificity of 81%, training accuracy of 85%, validation accuracy of 72%, security analysis of 82%, IPFIX attained data transmission ratio of 84%, specificity of 83%, training accuracy of 89%, validation accuracy of 74%, security analysis of 86% for ASL-DVS (ASL) dataset.

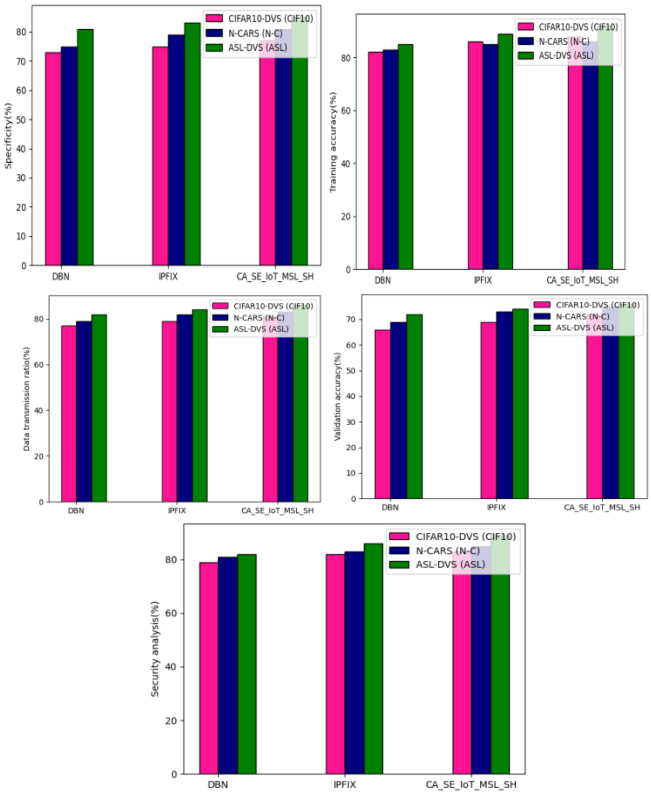

Fig.4. Analysis for CIFAR10-DVS (CIF10), N-CARS (N-C) and ASL-DVS (ASL) dataset

Spotting malicious hotspots, gaining access to malicious terminals, monitoring abnormal traffic, and other issues affect IoT devices and the transmission of data over the network. Identity authentication is among the issues associated with IoT devices and the cloud, necessitating the use of trusted third parties in traditional security measures, which can be resource-intensive. Blockchain technology can address these issues by enabling the implementation of security policies without the need for a third party. For example, the identity authentication mechanism between IoT devices and the cloud may require the distribution of keys by third parties. However, blockchain technology can enable authentication without involving third parties, reduce user authentication time, and provide high Quality of Experience (QoE) to the user. As a result, the main focus of this paper on using blockchain technology to develop a security system for IoT terminals throughout their entire life cycles. Specifically, the platform layer comprises an IoT asset database that supports full life-cycle management of massive devices using blockchain technology as the primary method. The key components of IoT devices, device operations, working conditions, software version upgrades, and other aspects are monitored and managed throughout the entire course. The security situation detection framework detects and reports threats promptly and effectively.

Although earlier works had a healthcare-related focus, it is still necessary to create new optimization algorithms for IoT devices to achieve energy efficiency. When sending patient data to a cloud server, IoT devices use a lot of energy. Therefore, the clustering method is used to increase energy efficiency. To achieve optimal resource utilization and meet workload deadlines in fog computing environments, an efficient healthcare application based on IoT is needed. The application should be capable of processing a significant amount of data from heart patients while consuming minimal energy and providing a quick response time. Furthermore, an ensemble deep learning-based fog computing model is necessary for real-time diagnosis of the severity of heart disease in patients.

V. Conclusion

Many sectors like academia, industry, healthcare, and defense have adopted the services of cloud computing, but security is a major issue with cloud computing. This research proposes a novel method in cloud security enhancement based on consumer IoT utilizing the AML technique for smart healthcare. In a smart healthcare system, individual IoT devices may be susceptible to different types of attacks, and Adversarial ML helps in identifying these threats at real time including emergencies with flexibility in handling the diversity. The security of cloud network is improved using trust encryption cryptographic technique and analyzed using structure based markov sparse Bayesian neural networks. The proposed model and algorithm can offer secure services to IoT applications, especially healthcare sector. The acquisition data of the IoT device, identity authentication information of the IoT device, and the security sensitivity of the IoT device are all essential ledger information when the IoT device interacts with the distant cloud. Several types of modern attacks are possible to breach the stored data over the cloud and need a trustable approach to cope with these challenges. The proposed approach tackles these issues using an ML-based structure-based Markov sparse Bayesian neural networks approach that provides secure authentication and authorization, allowing only legitimate users for the services.

The proposed approach performance is examined over the standard dataset and improved the data transmission ratio of 86%, specificity of 85%, training accuracy of 92%, validation accuracy of 76%, and security analysis of 89%. The proposed AI-based adversarial machine learning is a block box approach that lacks transparency, and explain ability. In future work, authors will use explainable AI to enhance cloud security for the healthcare area. Authors can use adversarial ML-based algorithms to predict the IoT workload in the future so that utilization of resources can be improved.

REFERENCES

[1] Singh, P. D., Dhiman, G., & Sharma, R. (2022). Internet of things for sustaining a smart and secure healthcare system. Sustainable computing: informatics and systems, 33, 100622.

[2] Haseeb, K., Saba, T., Rehman, A., Ahmed, I., &Lloret, J. (2021). Efficient data uncertainty management for health industrial internet of things using machine learning. International Journal of Communication Systems, 34(16), e4948.

[3] Guo, B., Ma, Y., Yang, J., & Wang, Z. (2021). Smart Healthcare System Based on Cloud-Internet of Things and Deep Learning. Journal of Healthcare Engineering, 2021.

[4] Riley, A., &Nica, E. (2021). Internet of Things-based smart healthcare systems and wireless biomedical sensing devices in monitoring, detection, and prevention of COVID-19. American Journal of Medical Research, 8(2), 51-64.

[5] Chinmay C, Senthil MN, Ganesh GD, RAMANA TV, Rajanikanta M, Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method, ACM Transactions on Sensor Networks, 1-16, 2023, doi.acm.org?doi=3597210

[6] Zahra, F., Jhanjhi, N. Z., Brohi, S. N., Khan, N. A., Masud, M., &AlZain, M. A. (2022). Rank and wormhole attack detection model for RPL-based internet of things using machine learning. Sensors, 22(18), 6765.

[7] Amit K., Chinmay C., Wilson J., Intelligent Healthcare Data Segregation using Fog Computing with Internet of Things and Machine Learning, Int. J. of Engineering Systems Modelling and Simulation, 12(2/3), 2021, 10.1504/IJESMS.2021.10036745

[8] Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-based internet of things and industrial IoT: a comprehensive survey. Security and Communication Networks, 2021.

[9] Unal, D., Bennbaia, S., &Catak, F. O. (2022). Machine learning for the security of healthcare systems based on Internet of Things and edge computing. In Cybersecurity and Cognitive Science (pp. 299-320). Academic Press.

[10] Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., &Biamba, C. (2022). Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring. Sensors, 22(3), 1076.

[11] Liang S, Zhu W., C. Chinmay C., Du J.. Yu K., "The IMU augment SLAM on Unmanned Vehicle for detection of protective measures in COVID-19," in IEEE Sensors Journal, 2022, doi: 10.1109/JSEN.2022.3189033

[12] Mistry, M., Pandey, R., &Kalita, A. (2021). Softwarization of the infrastructure of Internet of Things for secure and smart healthcare. Annals of the Romanian Society for Cell Biology, 25(6), 6680-6701.

[13] Lalithadevi, B., &Krishnaveni, S. (2022). Analysis of (IoT)-Based Healthcare Framework System Using Machine Learning. In Intelligent Data Communication Technologies and Internet of Things (pp. 219-237). Springer, Singapore.

[14] Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., &Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, 77(9), 9576-9596.

[15] Rath, M., Satpathy, J., &Oreku, G. S. (2021). Artificial intelligence and machine learning applications in cloud computing and internet of things. In Artificial intelligence to solve pervasive internet of things issues (pp. 103-123). Academic Press.

[16] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., &Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11(2), 198.

[17] Wu, X., Liu, C., Wang, L., & Bilal, M. (2021). Internet of things-enabled real-time health monitoring system using deep learning. Neural Computing and Applications, 1-12.

[18] Stone, D., Michalkova, L., &Machova, V. (2022). Machine and Deep Learning Techniques, Body Sensor Networks, and Internet of Things-based Smart Healthcare Systems in COVID-19 Remote Patient Monitoring. American Journal of Medical Research, 9(1), 97-112.

[19] Kondaka, L. S., Thenmozhi, M., Vijayakumar, K., &Kohli, R. (2022). An intensive healthcare monitoring paradigm by using IoT based machine learning strategies. Multimedia Tools and Applications, 81(26), 36891-36905.

[20] Hurley, D., &Popescu, G. H. (2021). Medical big data and wearable Internet of Things healthcare systems in remotely monitoring and caring for confirmed or suspected COVID-19 patients. American Journal of Medical Research, 8(2), 78-90.

[21] Chaudhary, A., Peddoju, S.K. & Chouhan, V. Secure Authentication and Reliable Cloud Storage Scheme for IoT-Edge-Cloud Integration. J Grid Computing 21, 35 (2023). https://doi.org/10.1007/s10723-023-09672-z

[22] S. Pandey et al., "Do-It-Yourself Recommender System: Reusing and Recycling with Blockchain and Deep Learning," in IEEE Access, vol. 10, pp. 90056-90067, 2022, DOI: 10.1109/ACCESS.2022.3199661.

[23] Orchard, G.; Cohen, G.; Jayawant, A.; and Thakor, N. "Converting Static Image Datasets to Spiking Neuromorphic Datasets Using Saccades", Frontiers in Neuroscience, vol.9, no.437, Oct. 2015

[24] Li H, Liu H, Ji X, Li G and Shi L (2017) CIFAR10-DVS: An Event-Stream Dataset for Object Classification. Front. Neurosci. 11:309. doi: 10.3389/fnins.2017.00309

[25] Yin Bi, Aaron Chadha, Alhabib Abbas, EirinaBourtsoulatze and Yiannis Andreopoulos, 'Graph-based Object Classification for Neuromorphic Vision Sensing', IEEE Conference on Computer Vision (ICCV), Oct.17 - Nov,2, 2019, Seoul, Korea

Jitendra Kumar Samriya (Member, IEEE), working as an Assistant Professor in Department of CSE,Indian Institute of Information Technology,Sonepat. His research interest is Cloud computing, Artificial Intelligence and Multi-objective Evolutionary optimization Techniques.

Chinmay Chakraborty (Senior Member, IEEE) is currently working as an Assistant Professor with the Department of Electronics and Communication Engineering, Birla Institute of Technology at Mesra, India. He has published 200+ articles in reputed international journals, conferences, book chapters, and books. His current research interests include the Internet of Medical Things, m-health/e-health, and medical imaging.

Aditi Sharma, (Senior Member, IEEE) worked as Post Doctoral Fellow in School of Engineering and Digital Sciences at Nazarbayev University Kazakhstan in the area of Intelligent Cryptosystems, IoT and cloud in Robotics in 2022. She is working as Associate Professor in the Department of CSE Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune.

Mohit Kumar (Member, IEEE), is currently working as an Assistant Professor in the Department of Information Technology, NIT Jalandhar, India. He has received his Ph.D. from IIT Roorkee, India. His research activity is mainly focus at Cloud computing, internet of Things, Fog computing andSoft Computing.

Savanth Kumar R is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, VNR Vignanajyothi Institute of Engineering and Technology, Hyderabad, India. His research interest includes Brain Computer Interface, Signal Processing, Machine Learning, and Bio Medical Signal Processing.