A Web 3.0 Integrated Blockchain Enabled Access System Augmented by Meta-Heuristic Cognitive Learning Framework for Mitigating Threats in IoT Enabled Consumer Electronic Devices

***Abstract*— Consumer Electronic Devices have become an open network model because of the infusion of the Internet of Things (IoT) and other communication technologies such as 5G/6G. Though these devices have provided the high-end sophistication even to common person, but it has proved its darker side by triggering more security breaches and privacy problems. Hence, securing and authenticating these Internet enabled consumer devices has become a probable issue to be solved for safer and secured communication. Therefore, this paper presents a novel fusion of Web 3.0- based Blockchain (WBC) and Deep learning (DL) technique for securing consumer electronic devices in an IoT ecosystem. The proposed framework k(MTD-BCAM) is devised into two components: Multiple-Threat Detection(MTD) and Access Management Mechanism(AMM). In the first component, a DL model is applied for threat detection, whereas WBC is meant for an efficient authentication process. Furthermore, a novel residual fast-gated recurrent neural network is proposed. To reduce the complexity, the komodo Mlipir optimization (KMO) approach is used to tune the hyper-parameters of the network. The comprehensive experimental outcome study of the proposed approach employs NSL-KDD datasets in which the distinct metrics of both DL and Blockchain (BC) are measured and analyzed. Results demonstrated the superior accuracy of the model by achieving 99.78% with less computational time and higher transaction speed. Additionally, the statistical validation and security strength of the model are also analyzed and examined with the varied state-of-art models.**

***Index Terms*—Artificial Intelligence, Block chain, Komodo Mlipir Optimization, Multi-threat detection, Web 3.0**

I. INTRODUCTION

The IoT-enabled Consumer Electronic Gadgets are rapidly increasing the spectrum of interests from a wide range of sectors [1]. These devices span a broad spectrum of intelligent technologies, including voice-controlled home assistants (like Alexa), smart door locks, connected televisions, and internet-enabled cameras. The adaptability of these gadgets allows them to be applied in a variety of evolving real-world scenarios. Increased number of smart phones, cloud-based infrastructures and advancements in IoT systems are all act as catalysts for the increased demand in the consumer electronics market. According to an in-depth study by Market Research Future (MRFR), titled "IoT in Consumer Electronics Market" – which analyzes data by product type, vehicle category, materials, and region, and provides projections up to 2030 – the market is expected to reach USD 172 billion, expanding at a compound annual growth rate (CAGR) of 18% by the year 2030[2]. These methods offer numerous advantages for both consumers and businesses, such as enhanced convenience, greater efficiency, improved workflows and output, better service quality, and higher levels of customer satisfaction [3]. The merits of IoT are unavoidable. Data security is a primary concern in which these devices are exploited by intruders and growing vulnerabilities that lead way to the privacy breaches and security problems, even leading to the customer's fatal end [4, 5]. A cyber-attack on an intelligent consumer gadget can significantly control the generation of false information and practical failures. Cyber specialists are now facing huge streams of hurdles to identify and detect all the possible threats and attacks.

In recent times, DL techniques are providing promising results in handling multiple and heterogeneous data from different domains [6]. This is carried out to support analysis and decision-making across different fields. These networks have become unavoidable for maintaining the security in the consumer device environment and maintaining the huge datasets provided through the intelligent networks [7]. The DL evoked intrusion detection has been used to discover and categorize the attack vectors [8]. Numerous possible threats have been verified with recognition, repudiation, tampering, data leakage, extended privilege (EoP), and denial of service (DoS). In present times, BC technology plays an important role in safeguarding consumer electronic devices owing to their absolute and tamper-resistant information. BC delivers a distributed and decentralized ledger that can stock IoT-Consumer devices data immutable and transparently [9]. By keeping data in blocks and connecting them with cryptographic hashes, the immutability and reliability of the data can be certified [10]. This helps in preventing data varying and illegal changes.

A. Motivation and Contribution

In recent times, DL and BC are considered twin approaches implemented across various domains that encounter threats related to scalability and privacy. However, existing systems often struggle with mysterious security breaches, poor resource optimization, and the inability to effectively counter diverse cyber threats, which hinder the seamless integration of DL and BC in IoT-enabled consumer electronic gadgets. Additionally, these systems suffer from high computational overhead, inefficient threat detection, and limited scalability, making them less effective in ensuring security and performance in large-scale IoT ecosystems. Motivated by this aforementioned problem, this research proposes a BC-Enabled Security Management with Optimized DL Threat Detection (BCESM-ODLTD) for safeguarding consumer electronic gadgets in the IoT ecosystems. The proposed method consists of two components which include BC management systems and a threat detection mechanism. In this approach, the BC model can manage access to consumer electronic gadgets whereas an optimized DL approach is used for proficiently identifying multiple attacks. To enhance the recognition results and reduce the computational overhead, Chaotic Komodo Mlipir Optimization has been utilized to improve parameters for the residual fast gated recurrent networks. In summary, the primary contribution of the research paper pursues

1. This proposed system demonstrates the application of the novel BCESM-ODLTD model that transforms consumer electronics devices by utilizing Web 3.0 and BC to improve access control and safety. This combination provides a decentralized and immutable credential management system to provide a more secured device access system.
2. The proposed technique proposes the novel fast gated recurrent networks(RFGN), which are used to utilize the different patterns of attacks and to protect consumer devices against privacy issues, thereby stabilizing the integrity and safety of consumer devices.
3. The study presents the Komodo Mlipir optimized hyperparameters to enhance performance while reducing computational costs.
4. Extensive testing has been conducted on the recommended system using the well-known NSL-KDD dataset, where key metrics such as accuracy, and varied metrics are examined and examined against other leading models in the field. Additionally, statistical analysis is performed to assess the performance further.
5. The complete model was integrated with the Ethereum BC environment using Web 3.0 interfaces and analyzed the security defense characteristics against the multiple attacks.

The remainder of the paper is structured as: Section-2 depicts a detailed survey of different authors, illustrating the BC and DL techniques for counterfeiting the different attacks on consumer electronic gadgets. The proposed framework with BC implementation and DL technique is represented in Section-3. The experimentation outcomes, performance validation and comparative assessment are demonstrated in Section-4. Finally, the paper is concluded up with the future direction in Section-5.

II. LITERATURE REVIEWS

Das et.al [11] proposed B-ERAC system, which aims at addressing security challenges in IoT device communication, particularly in supply chain ecosystems. This system advocates for BC technology as a solution due to its decentralized and distributed nature. By employing Elliptic Curve Cryptography (ECC), smart contracts, ES256 encryption standards, and Infura API integration, the framework ensures robust security, stringent access controls, data integrity, and transparency. Khandekar et al. [12] presented a BC-enabled IoT data-sharing framework leveraging the interplanetary file system (IPFS) to address critical issues in IoT-based systems, including data security, transparency, and scalability. The proposed framework in this study employs smart contracts developed in Solidity, deployed on a local Ethereum test network, for access control in IoT data sensing. By eliminating TTPs, the approach enhances data immutability and trustworthiness while addressing the computational and storage limitations of IoT devices. Katib et al. [13] proposed a BC-based cyber-security threat intelligence (CTI) and situational awareness system for intrusion alert prediction, addressing the challenges of network security assessment in the context of evolving technologies such as 5G, cloud computing, and the IoT. The system employs a CTI model where collected data undergo linear normalization. Yang et al. [14] proposed a Hybrid BC-Based Approach for IoT identity management, addressing the challenges of secure and efficient device identity management in IoT ecosystems. Their innovative framework strategically combines direct and indirect BC connections, achieving reduced latency, optimized network utilization, and enhanced energy efficiency. By employing local cluster interactions for routine tasks and utilizing indirect BC. Wang et al. [15] proposed a framework for enhancing security in IoT networks, addressing the limited focus of existing decentralized IoT solutions on privacy and

BC that optimizes data storage and provides a lightweight authentication mechanism for massive IoT systems. Additionally, homomorphic encryption is integrated for secure data encryption at the user's end before uploading to the cloud, ensuring privacy. Zhuang et al. [16] proposed a novel framework for detecting Advanced Persistent Threats (APTs) using a Conditional Dingo Optimization Algorithm (CDOA) integrated with Deep Residual Networks (DRN).

The study highlights the significance of APTs, which encompass data alteration, destruction, or Denial of Service attacks, often facilitated by exposed hardware and software vulnerabilities. Yang et al. [17] recommended a BC-based hybrid intrusion detection system (BC-HyIDS) to address the critical challenges of data security and confidentiality in modern networks, emphasizing the growing issue of intruder access to sensitive data through compromised networks. The BC-HyIDS leverages BC technology for secure signature sharing across distributed intrusion detection systems (IDS) and operates in three phases, combining anomaly and signature-based detection methods with BC in the third phase. The system incorporates cryptographic techniques to enhance data security in BC blocks and utilizes Hyperledger Fabric v2.0 and Hyperledger Sawtooth for implementation. Deng et al. [18] explore the integration of BC technology into intrusion detection systems (IDSs), highlighting its potential to elevate the security, accuracy, and reliability of IDSs. BC, a decentralized architecture that employs cryptographic validation through hashing functions, ensures the integrity of data by linking blocks in a secure and transparent manner. This technology guarantees immutable and verified records, crucial for monitoring malicious activities in network systems.

III. METHODOLOGY

Figure 1 depicts the system model for the recommended architectures. Here the IoT-based consumer electronic gadgets are considered. These devices are grouped into ordinary users and owning devices. These devices are interconnected to the cloud through which the owner can access the devices to achieve the intelligent control system. The owners can access the devices using their mobile applications which are stored in the cloud. Meanwhile, one of the intruders intended malicious activity on this infrastructure and attacked the consumer devices, which resulted in the hacking of the data of the specific owners. All the data from the devices and cloud will be tampered with. As shown in Figure1, BCESM-ODLTD model consists of two components which are as follows.

1.Threat Detection Component

2.Block Chain Component

The detailed description of each and every component is presented as follows:

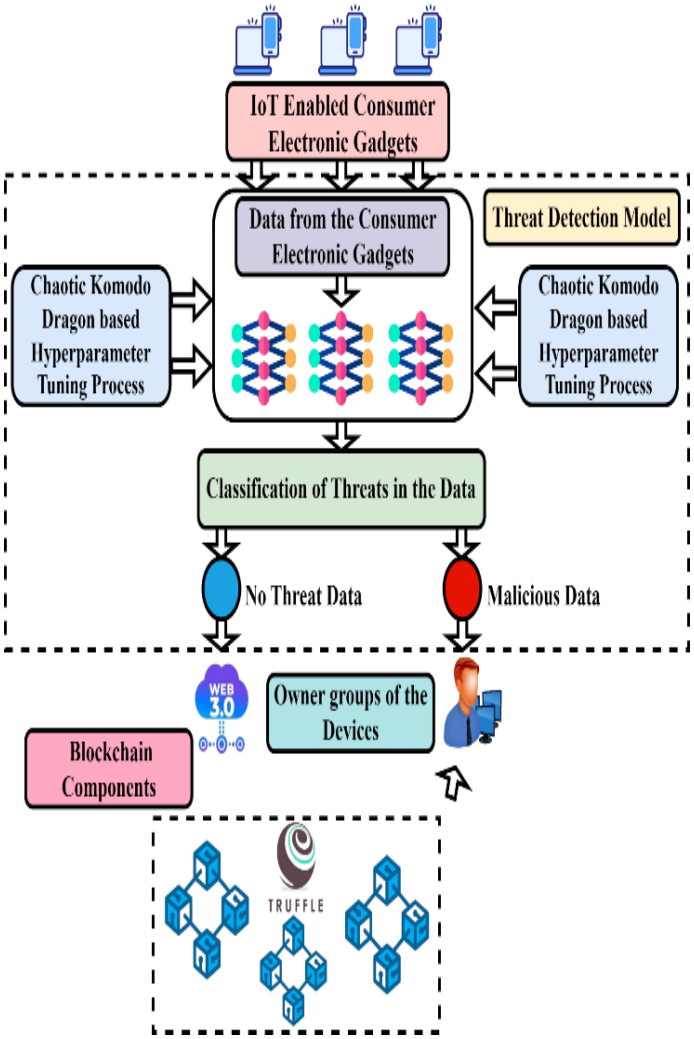

Fig. 1: Overall Framework for the BCESM-ODLTD model

A. Threat Detection Model

The proposed model effectively implements the residual gated recurrent fasts neural network(RGRFNN) method to classify the multiple threats. These network consist of residual gated recurrent units integrated with the deep fast neural networks with the hyper-parameters tuned by the komodo Mlipir optimization model. The elaborated description of the each and every module is presented

a) Gated Recurrent Neural Networks

The GRU (Gated Recurrent Unit) is widely regarded as one of the most intriguing alternatives to the Long Short-Term Memory (LSTM) network. It merges the forget gate and input vector into a single entity [19]. This architecture efficiently handles long-term dependencies and retains extensive memory. Compared to LSTM, the GRU significantly reduces the model's complexity.

Chung coined characteristics of GRU

$$h_t = (1 - x_t) \odot h_{t-1} + x_t \odot h_t \quad (1)$$

$$\widetilde{h_t} = g(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h \quad (2)$$

$$z_t = \sigma(W_h x_t + U_z h_{t-1} + b_z) \quad (3)$$

$$r_t = \sigma(W_h x_t + U_r h_{t-1} + b_r) \quad (4)$$

$$P = GRU(\sum_{t=1}^{n}[x_{t,} h_{t,} z_{t,} r_t(W(t), B(t), \eta(tannh))] \quad (5)$$

At the present time step, x_t depicts the input feature, while y_t denotes the output state. The output of the module at this specific moment is given by ht. The variables z_t and r_t correspond to the update and reset gates, respectively. W(t) stands for the weight parameters, and B(t)B(t) refers to the bias values at the current step.

To achieve the high accurate classification of multiple threats, traditional networks has replaced with the deep fast neural networks. The detailed description of these networks are as follows.

b) Deep Fast Neural Networks

The proposed model uses the principle of extreme learning machines (ELM) suggested in [20] for the high speed and high accurate classification of different grades. The features extracted from the different GRU cells are then fed into the deep fast neural networks. This type of neural network utilizes a single hidden layer where tuning the hidden layer parameters is not mandatory. These networks employ a kernel function to attain high accuracy and improve performance. One of the key benefits ELM is their ability to minimize training errors and provide better approximation. Since ELM automatically adjusts the weights and biases using non-zero activation functions, it is highly effective in classification tasks. A detailed explanation of how ELM works is provided in [21].

In this architecture, the neurons in the hidden layer, denoted as 'L', are activated by a differentiable function, such as the sigmoid function, while the output layer typically uses a linear activation. In ELM, it is not necessary to fine-tune the parameters of the hidden layer. While hidden nodes are still relevant, their parameters can be generated arbitrarily, even prior to training with the data set. For a single-hidden layer ELM, the system output is expressed in equation (6).

$$f_L(x) = \sum_{i=1}^{L} \beta_i h_i(x) = h(x)\beta \quad (6)$$

Where x → input features from encoder-decoder

β → output weight vector

$$\beta = [\beta_1, \beta_2, \dots\dots\dots\dots \beta_L]^T \quad (7)$$

H(x)→ output hidden layer

$$h(x) = [h_1(x), h_2(x), \dots\dots\dots\dots .. h_L(x) \quad (8)$$

To compute the Output vector O, the hidden layers are denoted by equation (9).

$$H = \begin{bmatrix} h(x_1) \\ h(x_2) \\ \vdots \\ h(x_N) \end{bmatrix} \quad (9)$$

$$\beta' = H^* O = H^T (HH^T)^{-1} O \quad (10)$$

$$\beta' = H^T (\frac{1}{C} HH^T)^{-1} O \quad (11)$$

Output function can be find by utilizing the above equation

$$f_L(x) = h(x)\beta = h(x)\, H^T (\frac{1}{C} HH^T)^{-1} O \quad (12)$$

The input feature maps are represented by h(x), while β denotes the temporal matrix, which is H computed using the Moore-Penrose generalized inverse, symbolized by HT. C is a constant, and B and O are the weight and bias parameters of the network. Ultimately, the probability for each category's occurrence is determined through the softmax function.

$$Y' = Softmax(S) \quad (13)$$

The output Y' is used to forecast the mechanism of DFU based on known datasets. To compute the loss, the cross-entropy function is employed, and its mathematical expression as

$$Loss = (\frac{1}{K}) \sum_{i=1}^{K} (Y(i) * Log\ Y' + \eta ||\theta||^2 \quad (14)$$

B. Hyperparameter Tuning

Hyperparameter tuning is done to recognize the optimal hyperparameters for the recommended approach, aiming to minimize its complexity. This process takes place before model training. The primary hyperparameters that need to be tuned in this research are the quantity of hidden layers, the count of hidden units, the dropout rate, the total number of epochs, and the batch size. In this research, the Chaotic Komodo Dragon Mlipir Optimization (CKDMO) algorithm is utilized to fine-tune the parameters of the networks for improved classification performance. The operational principles of the CKDMO algorithm are outlined below.

a) Komodo Dragon Mlipir Optimization Model

The Komodo dragon (Varanus komodoensis), a species of monitor lizard belonging to the family Varanidae, inhabits Komodo Island and neighboring islands in the Lesser Sunda region near Flores, East Nusa Tenggara, Indonesia. This reptile can grow up to 3 meters in length and weigh approximately 135 kilograms. Its distinct behaviors in feeding and reproduction make it a fascinating species. Female Komodo dragons exhibit unique reproductive strategies. They can yield offspring either by mating with dominant adult males or through parthenogenesis, a form of asexual reproduction. Intense battles often occur among large males competing for access to food or a mate. The victorious male typically gains the right to consume the prey or court a female. However, if the female rejects mating, she may opt for parthenogenesis instead. Smaller male Komodo dragons adopt a different approach to survival. They rely on scavenging leftovers from larger males but must maintain a safe distance to avoid being cannibalized. These smaller males cautiously wait for the dominant ones to move away before approaching the remnants of a meal. The term “mlipir” originates from the Japanese language, describing a cautious movement along the side of a road to avoid potential hazards. It conveys the act of discreetly navigating the roadside, remaining unnoticed, and successfully reaching a destination without incident. This distinctive style of walking is a reflection of careful strategy to ensure safety. In the context of foraging strategies, smaller male Komodo dragons adopt a behavior similar to that of mlipir. They carefully navigate around more dominant males, steering clear of direct conflict and the threat of being cannibalized. By remaining inconspicuous, these smaller individuals take advantage of chances to scavenge leftover food discarded by the more powerful males, using stealth and precise timing to ensure their survival.

The concept of the Komodo Mlipir Algorithm (KMA) can be illustrated through a simple optimization problem. Consider a two-dimensional function f(x1, x2)=x12+x22 where x1 and x2 correspond to the horizontal and vertical axes. The global optimum solution, or target, is f=0, which occurs at x1=0 and x2=0. Initially, a population of six Komodo individuals (potential solutions), denoted as k1,k2,…,k6, is randomly generated. Each Komodo is represented solely by its position vector within the solution space, without incorporating velocity.

The top-performing big male mimics the dominant Komodo that captures the sole prey, representing the best solution so far.

The interaction is modeled as an attraction-distract mechanism**.** A lower-ranking big male moves towards the superior one, while the stronger big male may move closer to or away from the weaker one, with a probability of 0.5. This simulates the behavior of dominant Komodos competing for prey. K2 is attracted to k1 (indicated by w21), moving closer to the global optimum. Meanwhile, k1 moves randomly, simulating distraction (w12) and exploration. This ensures that some big males focus on intensification around the best solution, while others explore more diverse regions. In this model, the dynamics between two dominant Komodo dragons, labeled k1 and k2, are framed as a process of attraction and distraction governed by specific rules.

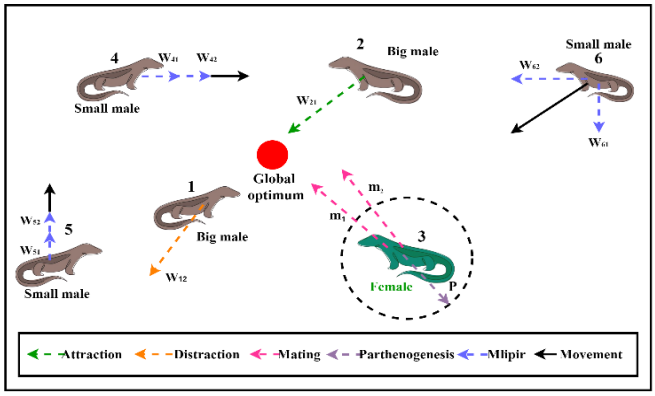

Fig. 2: Working mechanism of Komodo Mlipir Algorithm

The lower-quality dominant male (k1) is inclined

The lower-quality dominant male (k1) is inclined to approach the higher-quality male (k2). This duality results in some dominant males engaging in high-exploitation while others adopt a low-exploration strategy over a broader range.

K2 is drawn towards k1 (denoted by w21), driving it for the global optimum (exploitation), resembling the Komodo dragon’s trait when fighting to claim prey held by another dominant male. On the other hand, k1 is randomly diverted from k2 (indicated by w12) with a probability of 0.5, promoting exploration. This represents the Komodo dragon’s instinct to defend its prey from rivals. Additionally, similar to other metaheuristic approaches, the Komodo Dragon Algorithm (KMA) is structured to retain the highest-quality dominant males at all times.

The female either mates with the top-performing Komodo individual (the one with the highest fitness) to produce two offspring (represented as g1 and g2), or undergoes parthenogenesis through a random movement (denoted by h). Therefore, she seeks a solution in a moderately exploitative and moderately explorative manner.

In the novel metaheuristic optimization approach, small male Komodo dragons (k4, k5, and k6) employ a unique movement strategy called "mlipir" to bypass the larger males. This movement is characterized by a random selection of certain dimensions. This is referred to as the "mlipir rate." In Figure 2, where the "mlipir rate" is 0.5, it implies that the smaller males pursue the larger males in only half of the available dimensions.

For instance, k4 sidesteps the positions of k1 and k2 along just the first dimension (x1, horizontal), as shown by vectors w41 and w42. By adding these vectors together, the result is a new position for k4 that is closer to k2. On the other hand, k5 bypasses k1 and k2 by moving along the second dimension (x2, vertical), represented by vectors w51 and w52. When these vectors are summed, they push k5 upward, exploring the surrounding search space. Lastly, k6 follows both the vertical direction from k1 and the horizontal direction from k2, as depicted by vectors w61 and w62, resulting in a diagonal movement that brings k6 closer to the global optimum. This "mlipir" movement offers a combination of high exploration and potentially low exploitation. It is a key feature of the proposed Komodo Dragon Algorithm (KMA). In the initial stages of the algorithm, the population is highly diverse, and the small males, through the mlipir strategy, engage in extensive exploration of the search space. As the iterations progress, this exploration becomes more focused, and exploitation increases. The large males interact in all m dimensions, whereas the small males perform the mlipir movement in only a subset of d dimensions, where d is determined by the mlipir rate, a real number between 0 and 1, which defines the fraction of dimensions (1, 2, ..., m−1) selected for their movement. Additionally, no survivor selection process is applied to the new locations of the small males, as the larger males have already performed their actions.

1. Komodo individual representation

In the KMA, an individual Komodo is represented as a real-valued vector kk consisting of mm dimensions, defining its location within the problem domain. The population is composed of six Komodos, denoted as k1,k2,…,k6, where the dimensionality is m=2m = 2. Similar to the firefly mechanism in the Firefly Algorithm (FA), each Komodo in KMA is characterized solely by its position without any associated velocity. This absence of velocity contributes to its more dynamic movement throughout the search space, as the lack of inertia simplifies its motion.

2.Three groups of individuals

A proportion pp, typically set to 0.5 but adjustable within the range (0,1) determines the distribution.

$$q = \lfloor (p-1)n \rfloor, \quad (15)$$

$$s = n - q, \quad (16)$$

If the value of pp is either excessively low or overly high, it can result in q or ss equating to zero. Therefore, a straightforward method is employed to ensure that both large and small males engage in at least two interactions with Komodo dragons.

3. Movements of Big Males

The interaction between dominant males is governed by a straightforward principle proposed in this study. A low-quality dominant male is inclined to approach a higher-quality counterpart. Conversely, a high-quality dominant male may either be drawn towards or diverted by lower-quality counterparts, with a 50% likelihood of either outcome, allowing it to acquire a new location. This approach ensures that the opportunities for exploitation consistently surpass those for exploration. As a result, this innovative movement strategy is termed high-exploitation low-exploration (HILE). The positional update for a dominant male ki to determine its new location ki is expressed through the following two equations (17) and (18)

$$w_{ij} = \begin{cases} r_1(k_j - k_i), \text{ if } f(k_j) < f(k_i) \text{ or } r_2 < 0.5 \\ r_1(k_i - k_j), \text{ otherwise,} \end{cases} \quad (17)$$

$$k_i' = k_i + \sum_{j=1}^{q} * w_{ij}, \text{ where } j \neq i, \quad (18)$$

When considering the fitness (or quality) of the i-th and j-th big males, denoted as f(ki) and f(kj), respectively, and where ki and kj represent the i-th and j-th big males (j≠i), r1and r2 are random variables drawn from a normal distribution within the interval [0,1] and q denotes the total count of big males. In the first scenario, both males carry out an exploitative search in areas close to the global solution. Conversely, in the second scenario, the lower-quality Big Male 2 performs exploitation by being drawn toward the higher-quality Big Male 1. The probability of exploitation surpasses that of exploration. In the first scenario, all three males engage in exploitation near the global optimum. Scenarios 2, 3, 4, and 5 involve two males exploiting while the third explores. Scenarios 6, 7, and 8 feature one male

exploiting, while the others explore. Notably, there are no scenarios where all three big males perform exploration simultaneously. The optimal number of dominant males for interaction must be determined. In theory, two or three large males provide the best balance between exploration and exploitation. For unimodal functions, two large males are sufficient to achieve the optimal interaction. However, for multimodal functions, three large males are more effective. This hypothesis has been supported by various preliminary experiments. This approach to interaction contrasts with the method used in EO.

4. Reproduction of female

A female of moderate quality is designed to either focus on exploitation or exploration, with each option having an equal probability of 0.5. On the other hand, if exploration is selected, the female spreads out her search by reproducing through parthenogenesis, thus exploring a broader section of the search space. Finally, the female is upgraded with the best offspring produced. Additionally, the mating process between 2 Komodo dragons is structured as follows

$$k'_{il} = r_l \cdot k_{il} + (1 - r_l) \cdot k_{jl} \quad (19)$$

Meanwhile, kil′ and kjl′ refer to the k-th dimension of the two offspring produced through mating. Additionally, rk is a random variable drawn from a normal distribution within the interval [0, 1] for the l-th dimension. Since mating is carried out independently for each dimension, a variety of possible offspring can result from the process. In parallel, the parthenogenesis method is utilized, where a limited value is added to every dimension of the female.

$$(k_{i1}, k_{i2}, \dots, k_{im}) \rightarrow (k'_{i1}, k'_{i2}, \dots, k'_{im}), \quad (20)$$

$$k'_{ij} = k_{ij} + (2r - 1)\alpha|ub_j - lb_j|, \quad (21)$$

5. Movements of Small Males

In the wild, a smaller male Komodo dragon has 2 main tasks: (1) searching for leftover food from the larger males, and (2) avoiding being cannibalized by them by moving out of their way, a behavior known as mlipir. This specific behavior is modeled in the Komodo Movement Algorithm (KMA) through a unique action referred to as mlipir. Due to their lower status, the smaller males are designed to search a larger area for resources but may occasionally engage in some focused exploration. Each small male Komodo moves out of the way (mlipir) to avoid larger ones, which is represented by randomly selecting a portion of their dimensions with a specific likelihood, called the mlipir rate. This movement, denoted by a rate d within the range (0, 1), is mathematically defined as the mlipir action of the i-th Komodo dragon when it follows the j-th one.

$$w_{ij} = \begin{cases} \sum_{l=1}^{m} r_1(k_{jl} - k_{il}), \text{ if } r_2 < d \\ 0, \text{ otherwise} \end{cases} \quad (22)$$

$$k'_i = k_i + \sum_{j=1}^{q} w_{ij}, \text{ where } j \neq i, \quad (23)$$

In this context, r1 and r2 are randomly generated numbers within the range [0, 1] using a normal distribution. Here, r1 determines the velocity of the movement, while r2 specifies the dimension to move in. The value mmm represents the total number of dimensions, and kil and kjl denote the lth dimension of the ith small male and the jth big male. The lth dimension is selected randomly, with the probability determined by the multiplication rate d, which influences the choice of one or more dimensions (from 1 to m−1) of the big male. The variable q stands for the big males in presence.

Among these combinations, movements 1, 2, 4, and 5 are considered exploration, where both small males move horizontally and vertically around the big males, covering positions above, below, to the left, and to the right. At least one small male moves diagonally toward the big male.

6. Population adaptation scheme

As outlined earlier, the KMA algorithm involves three key parameters: population size n, portion pp, and mutation rate dd. Hypothetically, n is considered more impactful than pp and dd, as it plays a significant role in balancing exploration and exploitation strategies. In contrast, pp and dd can be set to fixed values, such as 0.5, since the problem specifics are not known in advance. Consequently, a dynamic adjustment method is proposed to modify n during the evolutionary process. When two consecutive improvements in the best-so-far fitness are observed, the population size n is reduced by removing five individuals. If stagnation is observed, the value of n is incremented by adding five new individuals. Each new individual is generated by randomly altering the position of the most successful male thus far. The updated population size n′ is then calculated

$$n' = \begin{cases} n - a, \text{ if } \delta f_1 > 0 \text{ and } \delta f_2 > 0 \\ n + a, \text{ if } \delta f_1 = 0 \text{ and } \delta f_2 = 0 \end{cases} \quad (24)$$

C. KMO Tuned DFNN Model

The weights in the dense networks employed for the classification layers are optimized by utilizing the simple MSSO method. At the start, the training network acquires hyperparameters that are selected at random. The fitness score for the suggested approach is calculated using equation (25).

$$Fitness\ Function = \{Max(Accuracy, Precision, Recall, F1 - score) \quad (25)$$

The proposed classification layer is designed to swiftly identify normal and heart disease conditions with minimal

computational effort. To achieve this, fast-learning networks utilizing GRU (Gated Recurrent Units) are employed to capture temporal features. These are followed by dense networks, tuned with the KMO (Kaiser-Meyer-Olkin) method, to effectively classify multiple types of attacks. The model parameters include 130 hidden nodes, a momentum value of 0.01, and 231 epochs for training, selected based on empirical evaluations to balance accuracy and computational efficiency.

D. BC Layers

BC technology can be applied to access management of consumer electronic gadgets and offers the intelligent system to generate the consensus systems against the multiple attacks. Depending on the BC, every device can manage without any physical activity. In this component, BC plays an important role for providing the safe access management system for consumer electronic devices. The BC network consist of four components such as Initialization Phase, Registration Phase, Transaction and Block generation phase. The detailed description of each and every phase is explained as follows:

a) Initialization Phase

Consumers are sub-categorized into ordinary consumers and device owners. To connect the consumers and device owners, BC produces public secret key pairs of every consumer. These keys are produced by the chaotic principles which is based on the combination of Henon maps, Multi-scroll maps and logistic maps. After the formation of chaotic keys Ck, digital generation process is executed between the consumers and device owners.

b) Device Registration Phase

Consumers include their gadgets in to the BC component. By executing the chaotic hashes on the owner's public key, every device is allocated an exclusive value g=hash(keys). IN this method every device is identified and signified as (Ck, D) where D denotes the devices and Ck keys illustrates the public chaotic keys.

c) Transaction generation

The owners with rights to these smart gadgets can handle and function then over the system confirmation by their secret and public chaotic keys. For an effective transaction generation, Web 3.0 is utilized in this component which exhibits the strong performance to handle the block chain networks. The secret chaotic key Csk is utilized for producing the signature e and creating the transaction Tx. Hence the access demand will be loaded into the real time distributed databases as a transaction. In the upcoming transaction, the ownership of a particular record is transferred to a different user within the BC.

d) Verification

Miners acquire this transaction tx and validate the signature by consistent owner's keys. If the signature is accurate, it indicates that this gadget's holder has produced it. Otherwise, this transaction tx is prohibited.

e) Block generation

Miners contain an accessible transaction tx into a novel block. Over the consensus device, like PoW, miners contest for the right to include this novel block in the chain. Miners approve a general set of authenticated dealings in the ledger. Also, the miner who acquires the right to create a novel block will be prized. After that, the block has been decided by complete system nodes, transaction will be broad, and the consumer can access this gadget. The public keys from the consumers creates the confidentiality and it is employed for both data encryption and confirmation process.

IV. IMPLEMENTATION

The full algorithm was implemented on an Intel Workstation featuring an i7 processor, an NVIDIA GPU, 16GB of RAM, and a 3.2 GHz clock speed. To examine the performance of the system within an Ethereum BC setting, Web 3.0 Python libraries were utilized. The development of decentralized applications (DApps) was carried out, with Infura APIs leveraged to establish connectivity to the Ethereum network.

A. Performance Evaluation

Performance metrics such as accuracy, precision, recall, specificity, and F1-score are assessed [22] and examined with state-of-the-art DL models in the context of Fog computing, highlighting the advantages of the proposed approach. Accuracy measures the overall correctness of threat detection in IoT security. Recall assesses the model's ability to detect actual threats, while specificity evaluates how well normal traffic is identified. Precision determines the proportion of correctly detected threats, and the F1-score balances precision and recall for a comprehensive performance measure.

Additionally, these metrics, along with the latency overhead, are examined to depict that the recommended approach is both more super and incurs lower overheads. To address issues of overfitting and generalization, the early stopping method is employed. This methodology halts the training process when the model's validation performance ceases to improve over time.

B. Results and Discussion

The experimental validation of the proposed framework is verified by employing the NSL-KDD Datasets, which consists multiple class of attacks such as DoS, Normal,

Probe, r2L and u2R. The dataset's adaptability enables effective benchmarking of Web 3.0-integrated security frameworks, ensuring their robustness against evolving cyber threats in decentralized IoT environments. Table 1 illustrates the number of instances utilized for training (70%) and testing (30%) process.

TABLE. 1
DATASET DESCRIPTION FOR NSL-KDD DATASETS (NSL_KDD 99) DATASETS

SL.NO	Dataset Descriptions	No of Data in the Dataset
1	Total number of Data records	5.1 Million
2	Training Datasets	4,898,431
3	Testing Datasets	311,029
4	Number of Features	42

The classification outcome of the recommended model under 70% training data was shown in Table 2 and Figure 3. It is apparent that the, recommended approach has yielded average performance of 99.78%, precision of 99.65%, recall of 99.6%, specificity of 99.7% and F1-score of 99.7% respectively. The similar fashion of the performance is evident for the testing data (30%) which is illustrated in Table 3 and Figure 4.

TABLE. 2
PERFORMANCE METRICS OF THE RECOMMENDED MODEL IN DETECTING THE DIFFERENT ATTACKS UNDER 70% TRAINING DATA.

Attacks	Performance Metrics				
	Accuracy	Precision	Recall	Specificity	F1-score
DoS	99.77%	99.73%	99.65%	99.67%	99.7%
Normal	99.74%	99.64%	99.59%	99.67%	99.65%
Probe	99.76%	99.67%	99.64%	99.73%	99.65%
U2R	99.7%	99.70%	99.69%	99.72%	99.70%
R2L	99.79%	99.72%	99.70%	99.70%	99.72%
Average Performance	99.78%	99.69%	99.65%	99.7%	99.70%

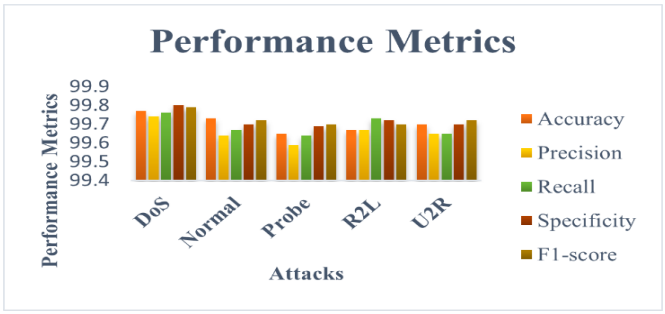

Fig. 3: Performance metrics of the recommended approach in detecting the different attacks under 70% training data.

Table. 3
PERFORMANCE METRICS OF THE RECOMMENDED APPROACH IN DETECTING THE DIFFERENT ATTACKS UNDER 30% TESTING DATA.

Attacks	Performance Metrics				
	Accuracy	Precision	Recall	Specificity	F1-score
DoS	99.78%	99.71%	99.64%	99.66%	99.7%
Normal	99.73%	99.63%	99.60%	99.68%	99.65%
Probe	99.74%	99.66%	99.65%	99.70%	99.65%
U2R	99.79%	99.68%	99.65%	99.71%	99.70%
R2L	99.80%	99.70%	99.69%	99.72%	99.72%
Average Performance	99.774%	99.68%	99.64%	99.69%	99.70%

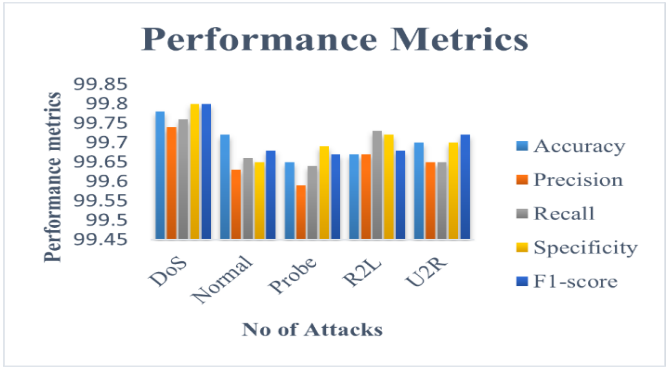

Fig. 4: Performance metrics of the recommended model in recognizing the varied attacks under 30% testing data.

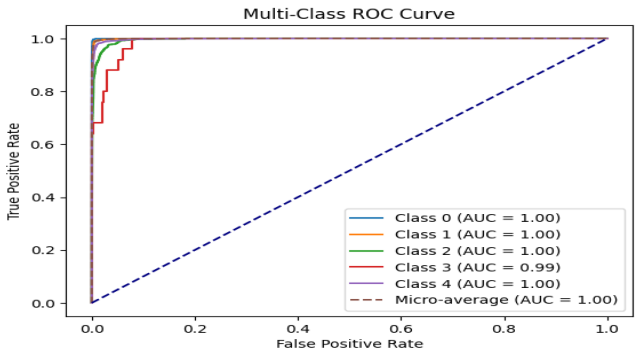

Fig. 5: Multi-Class ROC Curves for the recommended approach in Detecting the Multiple –Attacks

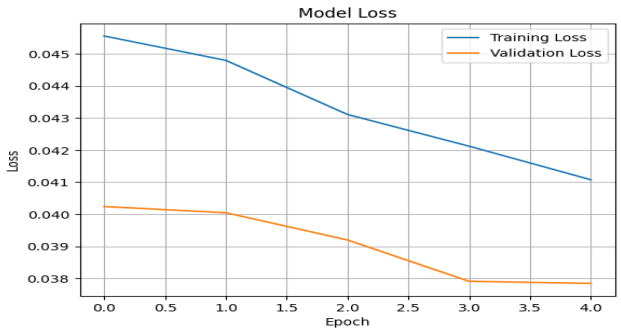

Fig. 6: Validation-Loss Curves for the recommended approach in Detecting the Multiple-Attacks

Figure 5 depicts the ROC curves produced by the proposed framework, proving its ability to differentiate multiple classes of attacks. This depicts the capability of the recommended approach to classify the different attacks. This highlights the model's efficiency in assorting the misclassification of the several classes. Figure 6 summarizes the loss-validation curves for the proposed framework. As shown in Figure 6, loss values are readily reducing as the model optimizes its weights to reduce the false alarm rates to produce an efficient classification of multiple attacks.

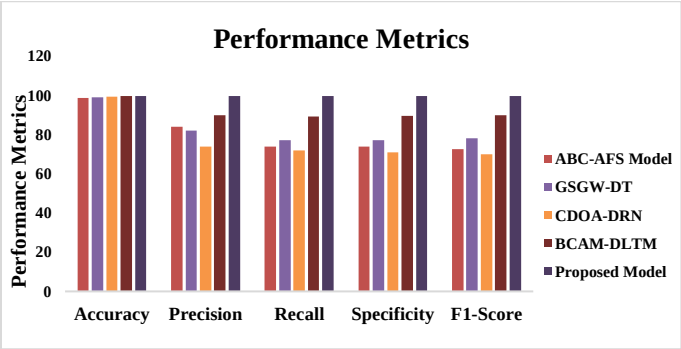

Fig. 7: Comparative Analysis of Performance Metrics Across Different Models

Figure 7 examines a comparative analysis of the recommended approach model with the other hybrid existing model. In terms of accuracy, ABC-AFS model has produced the accuracy of 98.60%, GSGW-DT has given the accuracy of 99.02%, CDOA-DRN has produced the 99.25%, BCAM-DLTM has outcome 99.6% and recommended model has yielded the accuracy of 99.78% respectively. In terms of accuracy, similar fashion of performance is illustrated but the recommended approach has outperformed the varied hybrid learning models. In the terms of precision and recall, the recommended approach has produced the maximum performance in recognizing the attacks and proves its superiority over the other models. From the Figure 7, CDOA-DRN model has produced the least precision and recall whereas the recommended approach has produced the better performance than the varied approaches. Finally based on the specificity and F1-score, recommended approach gained the higher specificity and f1-score of 99.6% and 99.7% respectively. BCAM-DLTM has produced the precision of 95.36%, recall of 94.5% in detecting the multiple attacks using NSL-KDD datasets. The proposed model has shown the performance improvement of 5.77% over the BCAM-DLTM model. In contrast, CDOA-DRN model has produced the least precision of 75.16% and recall of 74.23% respectively.

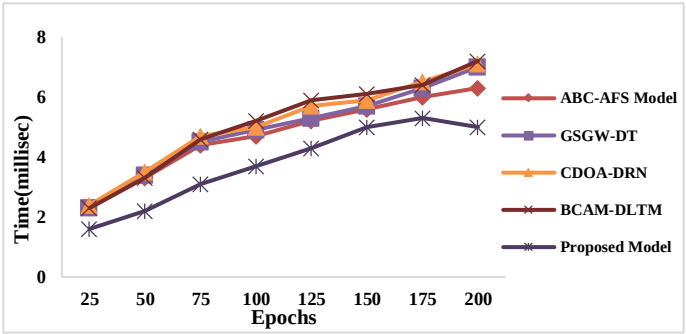

Fig. 8: Computational Complexity Comparison Across Existing Security Models

Figure 8 illustrates the computational complexity comparison across existing security models over increasing epochs. The proposed model consistently exhibits lower computational time than ABC-AFS, GSGW-DT, CDOA-DRN, and BCAM-DLTM, demonstrating its efficiency. This reduction in time highlights the model's ability to enhance security performance while maintaining lower processing overhead.

Table 4 shows the statistical validation of the recommended approach over the other meta-heuristic algorithms. The recent meta-heuristic algorithms like Conditional Dingo Optimization(CDO) algorithm, Reptile Search Algorithm(RSA), Scalp Swarm Optimization Model (SSO) and Enhanced Particle Swarm Optimization(E-PSO) which are used for tuning the hyper-parameters of the learning model.

TABLE. 4
FITNESS FUNCTION BASED OUTCOMES FOR THE VARIED COMBINATIONS OF OPTIMIZERS

Algorithm	Best	Worst	Mean	Median	SD	Variance
CDO	0.7470	0.6445	0.72210	0.022839	0.06540	$7.4x10^{-6}$
RSA	0.730330	0.63525	0.69034	0.020202	0.07033	$6.39x10^{-6}$
SSO	0.7523	0.6763	0.65372	0.027820	0.068903	$5.89x10^{-5}$
E-PSO	0.80234	0.64389	0.73402	0.0302-2	0.059034	3.90x10-4
Proposed Model	0.99763	0.81202	0.85640	0.06344	0.037630	$2.28930 x10^{-4}$

From the table 4, it is very apparent that the recommended KMO algorithm has yielded the best performance with the least median, standard deviation(SD) and variance when examined with the other learning models. Table 5 Shows the transaction time of the recommended DL model when integrated with the Block chain network. As shown in table 5, the recommended BCESM-ODLTD has produced the least transaction time when compared with other existing DL based block chain network, thereby significantly reducing latency in the system.

TABLE. 5

TRANSACTION TIME ANALYSIS

Algorithm	Transaction Time(Secs)
Ref[23]	45.9
Ref[24]	34.89
Ref[25]	19.90
Ref[26]	14.89
Proposed Model	10.89

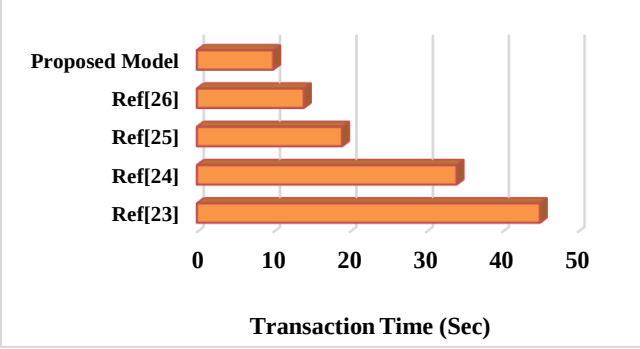

Fig. 9: Comparative analysis of the transaction Time analysis with distinct models

The experimental value obtained in Table 5 stated that the BCESM-ODLTD has produced the optimum transaction time and outperformed the other existing block chain models. Based the table 5 and figure 9, it is evident that the recommended model has achieved the excellent transaction time which is 25% less than Ref [23], 40% less than ref [24], 47% less than ref [25] and even 55% less than [26] respectively.

V. CONCLUSION

This study presents a technique for securing consumer electronics devices in the IoT ecosystems. The BCESM-ODLTD technique mainly monitors a two-phase procedure: access management and threat detection. In the BCESM-ODLTD technique, BC technology can be applied to manage access to consumer electronics devices USING Web 3.0. Besides, the BCESM-ODLTD technique uses the FGRU method proficiently to classify threats. To enhance the recognition outcomes of the FGRU technique, the hyperparameter tuning process takes place using KMO. The extensive experimentation has been conducted using NSK-KDD datasets to produce a 99.78%performance and statistically proving its stability in providing the defense characteristics against the growing cyber-attacks. Furthermore, the model is deployed in Ethereum BC and examined with varied learning models. Evaluation outcomes demonstrate that the proposed KMO-tuned DL training networks have surpassed the varied residing DL models that encounter the different attacks. The research proves the ensemble DL framework has demonstrated its capability to mitigate the privacy and security concerns in the consumer electronic network. A future study should focus on the development of privacy-preserving DL models for real-time IoT-enabled devices in order to maintain the scalability, robustness and effectiveness of the model. Additionally, the proposed approach can be extended to smart cities and autonomous vehicles to enhance security, real-time data processing, and threat mitigation in these evolving IoT domains.

REFERENCES

[1] Saif, S., Das, P., Biswas, S., Khan, S., Haq, M. A., & Kovtun, V. (2024). A secure data transmission framework for IoT enabled healthcare. Heliyon, 10(16), e36269. https://doi.org/10.1016/j.heliyon.2024.e36269

[2] L. Arya and G. P. Gupta, ‘‘Ensemble filter-based feature selection model for cyber attack detection in industrial Internet of Things,’’ in Proc. 9th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), vol. 1, Coimbatore, India, Mar. 2023, pp. 834–840.

[3] G. C. Sekhar and R. Aruna, ‘‘A novel Blockchain-assisted deep learning model for secure edge intelligence in IoT networks,’’ J. Inst. Eng. India, Ser. C, pp. 1–14, Apr. 2024.

[4] Luo, H., Zhang, Q., Sun, G., Yu, H., & Niyato, D. (2024). Symbiotic Blockchain Consensus: Cognitive Backscatter Communications-Enabled Wireless Blockchain Consensus. IEEE/ACM Transactions on Networking, 32(6), 5372-5387. doi: 10.1109/TNET.2024.3462539

[5] Saurabh, et al. ‘Lightweight Security for IoT’. 1 Jan. 2023 : 5423 – 5439.

[6] M. Nasir, A. R. Javed, M. A. Tariq, M. Asim, and T. Baker, ‘‘Feature engineering and deep learning-based intrusion detection framework for securing edge IoT,’’ J. Supercomput., vol. 78, no. 6, pp. 8852–8866, Apr. 2022.
[7] Gupta, D., Rani, S., & Gadekallu, T. R. (2025). Blockchain-Based Semantic Exchange Framework for Summarized Video Contents in Wireless Edge Intelligence Network Enabled Web 3.0. IT Professional, 26(6), 70-76.
[8] H. Alkahtani and T. H. H. Aldhyani, ‘‘Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms,’’ Complexity, vol. 2021, pp. 1–18, Jul. 2021.
[9] S. Anbalagan, G. Raja, S. Gurumoorthy, D. Suresh R and K. Ayyakannu, " Blockchain Assisted Hybrid Intrusion Detection System in Autonomous Vehicles for Industry 5.0," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 881-889, Nov. 2023, doi: 10.1109/TCE.2023.3320282
[10] Han, F., Yang, P., Du, H., & Li, X. (2024). Accuth+: Accelerometer-Based Anti-Spoofing Voice Authentication on Wrist-Worn Wearables. IEEE Transactions on Mobile Computing, 23(5), 5571-5588. doi: 10.1109/TMC.2023.3314837.
[11] S. Das, Y. Manchala, S. K. Rout, and S. K. Panda, ‘‘Deep learning and metaheuristics based cyber threat detection in Internet of Things enabled smart city environment,’’ Researchsquare, Jan. 2023.
[12] A. Khandekar and S. F. Ahmad, ‘‘Secured IoT architecture for personalized marketing using Blockchain framework with deep learning technology,’’ Cluster Comput., pp. 1–16, May 2024.
[13] I. Katib and M. Ragab, ‘‘Blockchain-assisted hybrid Harris hawks optimization based deep DDoS attack detection in the IoT environment,’’ Mathematics, vol. 11, no. 8, p. 1887, Apr. 2023.
[14] X. Yang, T. Li, W. Xi, A. Chen, C. Wang, A Blockchain -assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud, IEEE Access 8 (2020) 170713–170731, https://doi.org/10.1109/ACCESS.2020.3025060.
[15] Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium Blockchain, in: IEEE Access, vol. 7, 2019, pp. 136704–136719, https://doi.org/10.1109/ACCESS.2019.2943153.
[16] Y. Zhuang, L.R. Sheets, Y.-W. Chen, Z.-Y. Shae, J.J.P. Tsai, C.-R. Shyu, A patientcentric health information exchange framework using Blockchain technology, IEEE J. Biomed. Health Inf.cs 24 (8) (Aug. 2020) 2169–2176, https://doi.org/ 10.1109/JBHI.2020.2993072.
[17] Y. Yang, et al., Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers, IEEE Access 6 (2018) 46949–46961, https:// doi.org/10.1109/ACCESS.2018.2865535.
[18] F. Deng, Y. Wang, L. Peng, H. Xiong, J. Geng, Z. Qin, Ciphertext-policy attributebased signcryption with verifiable outsourced designcryption for sharing personal health records, in: IEEE Access, vol. 6, 2018, pp. 39473–39486, https://doi.org/ 10.1109/ACCESS.2018.2843778.
[19] Kurochkin, Ilya & Volkov, S. (2020). Using GRU based deep neural network for intrusion detection in software-defined networks. IOP Conference Series: Materials Science and Engineering. 927. 012035. 10.1088/1757-899X/927/1/012035.
[20] Huang, G.-B., Zhu, Q.-Y., & Siew, C.-K. (2006). Extreme learning machine: Theory and applications. *Neurocomputing*, *70*(1–3), 489–501. https://doi.org/10.1016/j.neucom.2005.12.126
[21] Wu, Y., Guo, G. & Gao, H. ELM: a novel ensemble learning method for multi-target regression and multi-label classification problems. *Appl Intell* **54**, 7674–7695 (2024). https://doi.org/10.1007/s10489-024-05570-3
[22] Ahmad, I., Ul Haq, Q. E., Imran, M., Alassafi, M. O., & AlGhamdi, R. A. (2022). An Efficient Network Intrusion Detection and Classification System. *Mathematics*, *10*(3), 530. https://doi.org/10.3390/math10030530
[23] Razaque, A., Jararweh, Y., Alotaibi, A., Amsaad, F., Alotaibi, B., & Alotaibi, M. (2022). A blockchain-enabled framework for securing connected consumer electronics against wireless attacks. Simulation Modelling Practice and Theory, 121, 102652. https://doi.org/10.1016/j.simpat.2022.102652
[24] Kharche, A., Badholia, S., & Upadhyay, R. K. (2024). Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India. Blockchain: Research and Applications, 5(2), 100188. https://doi.org/10.1016/j.bcra.2024.100188
[25] W. Fan, Y. Park, S. Kumar, P. Ganta, X. Zhou and S. -Y. Chang, "Blockchain-Enabled Collaborative Intrusion Detection in Software Defined Networks," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, 2020, pp. 967-974, doi: 10.1109/TrustCom50675.2020.00129.
[26] Abubakar, A.A., Liu, J. and Gilliard, E. (2023), An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. Electron. Lett., 59: e12888. https://doi.org/10.1049/ell2.12888