Integrating ML and Blockchain for Consumer-Centric Approaches in Securing Data Transmission on IoT Networks

Bo Yuan[1,2,5*],Faguo Wu[3,4,5]

***Abstract*—Data security and privacy are becoming more essential due to the quick expansion of "Internet of Things (IoT)", particularly in consumer-focused applications. To improve the security of data transmission in IoT networks, this study provides a novel architecture that combines Blockchain with Machine Learning (ML) to address critical security threats like data integrity breaches, unauthorised access and cyber-attacks. The suggested solution uses a hybrid blockchain paradigm that combines public and private blockchain capabilities to ensure data integrity and safe access management. Machine learning algorithms, including anomaly detection and classification techniques, are utilised to quickly monitor and analyse network traffic, identify possible risks, and enhance the system's resilience against cyber-attacks. The platform also uses neural networks based on transfer learning for dynamic trust validation and IP rotation using moving target defense (MTD) mechanisms to reduce attacks and strengthen the security. Also, optimised resource management techniques are used to improve stability and reduce computational complexities. Combining these technologies strengthens data security while giving users more control over their data. This method offers a workable solution for the safe implementation of IoT networks in consumer applications by addressing the issues of scalability, latency, and energy efficiency.**

***Index Terms*— Blockchain, data transmission, Internet of Things, anomaly detection, machine learning, security.**

I. INTRODUCTION

The total automation of the communication system without the need for outside engagement has been made possible by technological modernization as a smooth and effective means of enhancing human comfort. IoT technologies also aid in the creation of an enduring urban model and the maintenance of superior quality of life by providing secure and efficient data exchange. [1] These technologies include trackers, actuators, sensors, alarms, and sirens that offer dependable, two-way energy transfer and data sharing between suppliers and customers, creating a more sophisticated, efficient system with higher service quality and financial advantages [2]. As IoT networks get expand, the security and privacy of transmitted data become complex, so it requires effective protection mechanisms to address the cyber threats and unauthorized access. As all of this is going on, artificial intelligence (AI) enables these consumer devices to become increasingly sophisticated and capable of making judgments on their own by learning from the data they gather [3]. Machine Learning (ML), particularly anomaly detection and classification models plays important role in monitoring IoT network traffic and helps to reduce the possible threats in real time. Though these methods have advanced but, they also have disadvantages, particularly in handling large scale security challenges. For instance, traditional centralized security mechanisms struggle with scalability and dynamic access control in IoT networks. To address these concerns blockchain technology acts as an important role [4], which is crucial to consumer electronics because it increases efficiency, security, and transparency. One of its essential applications is making sure Internet of Things (IoT) devices are secure. Manufacturers may use blockchain technology to create tamper-resistant **sys**tems that lower the possibility of unauthorized access or manipulation [5]. Moreover, blockchain provides control over personal data and improves privacy due to decentralized Manufacturers may use blockchain technology to create tamper-resistant identity verification [6]. It reduces processing complexity and communication overhead compared to the traditional centralized method [7]. Hybrid blockchain models combines public and private blockchain abilities which improves both security and computational efficiency. Again, the edge caching considerably enhances end users' overall service experience by utilizing edge nodes' caching and data processing capabilities to deliver lower latency and more robust services [8]. The fundamentals of digital money and the viability analysis of intelligent operating systems are only two sectors in which blockchain technology's three functions have expanded its frontiers. Conversely, safety is ensured by blockchain technology [9]. A communal data structure called a blockchain was created to hold every transaction. The

[1]School of Computer Science and Engineering, Beihang University, Haidian 100191, Beijing, China(e-mail: boyuan@buaa.edu.cn)

[2]State Key Laboratory of Software Development Environmentg, Beihang University, Haidian 100191, Beijing, China

[3]Key laboratory of Mathematics, Informatics and Behavioral Semantics (LMIB), Beihang University, Haidian 100191, Beijing, China(e-mail: faguo@buaa.edu.cn)

[4]Institute of Artificial Intelligence, Beihang University, Haidian 100191, Beijing, China

[5]Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing, Beihang University, Haidian 100191, Beijing, China

Mentions of supplemental materials and animal/human rights statements can be included here.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org

references between the blocks from the chain. We refer to the first blockchain as genesis. The three components of every block are the transaction, block subtitle, and operation counter [10]. It functions as a dispersed structure for data storage. Blockchain security is predicated on the concept of "proof of work (PoW)", whereby communication is deemed valid as long as the system can demonstrate that approved nodes complete sufficient computing tasks. The miner, responsible for creating blocks, continuously uses hash calculations to try and solve cryptographic problems or proof of work [11]. Blockchain requires expensive storage for massive numbers of data. However, it works well to store data hashes in the ledger rather than the actual data [12]. Therefore, we combine Blockchain and Machine Learning to provide Consumer-Centric Solutions for Safe Data Transfer on IoT Networks. By considering the decentralized ability, transparency and secure data transferring ability we chosen the blockchain technology specifically in this study. Apart from the advantage that blockchain is not sufficient individually to fully secure the IoT networks. It requires complementary security strategies to reduce attack surfaces and improve system resilience. Therefore, we integrate the machine learning techniques to address the need for intelligent decision making such as anomaly detection, pattern recognition and adaptive optimization in resource constrained and dynamic IoT environments.

A. Motivation

Despite the significant challenges of implementing blockchain technology, many previous studies have contributed to cloud computing security through various technologies, including "machine learning (ML)" and blockchain. However, the problems associated with cloud computing security have not yet been resolved. The primary issue that these studies have addressed is as follows:

Data Security and Privacy Concerns: Data transmission and storage volumes have risen dramatically with the increase in the Internet of Things strategy. This data is a prominent target for cyberattacks as it frequently contains sensitive personal information. It is tough to ensure the privacy, accuracy, and accessibility of this data.

- **Ineffective and Exposable Access Control Systems:** Because they are frequently centralised and based on pre-established rules, traditional access control solutions do not quickly adapt to the dynamic nature of the Internet of Things settings. These systems lack the flexibility to accommodate a wide range of user needs and responsibilities and may be open to unwanted access.
- **Problems with Scalability in Blockchain-Based Systems:** Blockchain technology presents substantial scaling issues despite its high-security characteristics, such as transparency and immutability. Large-scale IoT networks may find it difficult to use public blockchains because of their high latency and low throughput.
- **Complexity of Identifying and Reacting to Anomalies:** The massive volume of data generated by IoT devices and their diverse nature makes it more challenging to identify irregularities and security concerns. Current machine learning techniques may need a lot of resources and may not function well, particularly in contexts with limited resources.
- **Absence of Consumer Data Control:** Customers' control over their data, including its collection, storage, and sharing, is often restricted in IoT devices. This lack of transparency and control may impact consumer adoption and acceptability of IoT technology, which may give rise to problems with trust and worries about data exploitation.

B. Research Contribution

The innovative points offered for safe cloud computing security services are mentioned. The following are the research's principal contributions:

- The hybrid blockchain architecture presented by this research combines the advantages of private and public blockchains. Cloud Service Providers (CIP) play an important role in the approach, the paradigm addresses scalability challenges and improves data security and integrity, making it appropriate for managing the Internet of Things network's high throughput and low latency strain.
- The paper presents a unique access control approach that dynamically manages policies by leveraging machine learning methods like Fuzzy Inference Systems (FIS), which allows the system to make more accurate and efficient access control decisions based on the fuzzy logic. Role-based and attribute-based access controls are supported by this framework, ensureing flexible and secure data access according to specific user requirements and network roles.
- The application of advanced machine learning methods to track and examine IoT network traffic, such as neural networks and anomaly detection algorithms, is a significant addition. Due to this integration, the system can instantly identify and react to security threats, enhancing the network's overall resilience.
- The proposed model integrates MTD mechanisms of dynamic IP rotation to reduce attack surfaces and prevent adversaries from exploiting static network risks. By utilizing a Domain Name System (DNS) pool, the system continuously rotates the service IP address to avoid potential attackers.
- The study uses optimisation techniques to improve resource management and allocation effectiveness in the Internet of Things environment. Proof of Work (PoW) mechanisms are involved to provide a layer of security. One example is using machine learning-based techniques to minimise computational overhead and energy consumption in feature selection and decision-making.
- By integrating blockchain's immutability and transparency properties, the proposed system improves customer control over their data. Through Cloud Service Providers (CSP) users obtain better control over the collection, storage, and sharing of information. It builds confidence and promotes

the wider use of IoT technology by allowing users to control permissions and monitor how their data is used.

C. Paper Organization

The outstanding section of this work are approved as follows: Section 2 presents an overview of previous research gaps and works on service allocation and intrusion detection in cloud and IoT environments; Section 3 offers a detailed clarification of the suggested work, complete with equations and an appropriate diagram; Section IV describes the simulation setup of the recommended work, the reproduction tool and its simulation parameters; Section V provides an overall summary of the proposed work and compares it to existing works. Finally, section VI concludes the paper.

II. Related Work

This section covers a study of the literature on blockchain-based secure data transfer on IoT networks and machine learning. Blockchain-based IoT cloud platforms are employed for security and privacy in innovative healthcare, according to this article's proposal for a secure architecture supported by federated learning and blockchain [13]. Scalable machine learning applications, such as healthcare, use federated learning technologies. In this paper, they propose to use blockchain technology to defend FL technologies running in the "Internet of Things (IoT)" strategy from assault. Securing the integrity of the trained models is made possible by integrating FL with Blockchain, hence averting model poisoning incidents [14]. With this research, extensive data analytics services that are safe and maintain privacy may be obtained by integrating Blockchain technology with FL. Fuzzy hashing is our suggested method to recognise variation and irregularity in the FL-trained model against poisoning attempts, safeguarding the truthfulness of user data and the qualified model. They tell a wireless sensing framework that supports CIoT devices by utilising semantic capabilities [15, 16]. CIoT devices can reduce energy usage by transmitting just the small-sized retrieved information taken from raw data, allowing for the extraction of semantically meaningful information. They have also created a multi-dimensional contract incentive mechanism that, considering the existence of information asymmetry, provides suitable incentives for various categories of CIoT devices based on their computation and communication costs.

The secure architecture for the DTs' cooperation in consumer electronics is provided in this work [17]. Then, using a consensus model that integrates blockchain, digital twins, and real-time consumer device monitoring, they have developed an access control mechanism. Blockchain technology is employed in the proposed framework to enable consumer electronics products based on digital twins. They specifically developed a cooperative blockchain architecture that prioritises real-time access control and a distributed chain code model based on manufacturer, merchant, and device users. To shield the healthcare sector against phishing attempts, a suggested machine learning (ML) technique was trained on a sizable dataset to identify the traits that separate phishing from non-phishing URLs [18, 19]. The model was trained using the characteristics extracted from the URLs. Individuals and businesses can take proactive steps to safeguard themselves from the harmful impacts of phishing assaults by recognising phishing URLs in real time. This paper suggests [20] BeRout, a unique message-forwarding technique, for consumer-centric IoT opportunistic networks. The proposed system is predicated on nodes' altruistic actions. BeRout, to node's previous behaviour and actions, to achieve a high delivery ratio in IoT opportunistic network scenarios. A buffer management method has been presented to effectively and efficiently use buffer space [21]. In this study, they propose a revolutionary method to ensure transparent and safe communication in consumer electronics. To improve the security and precision of the system, they provide a weighted product model and a multi-criterion decision-making model named TOPSIS. The research [22] presents a novel security architecture for intelligent healthcare that uses blockchain technology to identify and counteract ransomware threats, which we call BSFR-SH. The consequences of the security learning exhibit that the suggested BSFR-SH is secure from ransomware assaults.

In this research [23], they introduce a novel two-level privacy-preserving system. They choose this structure above other approaches like differential privacy and completely homomorphic encryption because it synergises "federated learning" with incompletely homomorphic encryption. They suggested the AI-enabled deep learning model-based zero trust security (AIDL-XTS) architecture for device, user, and application authentication and verification at each access request stage. They employ a Deep CNN-BiLSTM network to authenticate users based on smartphone sensor data. In addition, they suggested using a trust score based on the Bayes theorem to assess the security of zero trust [24, 25]. All users, devices, and apps are assumed to be untrusted in this proposed architecture, necessitating verification and authentication for each access request, irrespective of the user's device or location. They suggest a methodology called Auditable Privacy-Preserving Federated Learning (AP2FL), specifically designed for medical device use [26]. Data leakage concerns are successfully mitigated by AP2FL, which uses Trusted Execution Environments (TEE) to enable safe preparation and aggregation operations on the consumer and server sides. In the suggested system, batch normalisation (BN) approaches are applied to find data similarities and condense user updates, and the "Active Personalized Federated Learning (ActPerFL)" model is used to manage non-IID data. Furthermore, they provide audit technology in AP2FL that exposes each client's input to the FL procedure, allowing the universal representation to be updated across various data distributions and kinds. They provide a safe fitness framework built on an Internet of Things-enabled blockchain network and machine-learning techniques [27]. The proposed architecture consists of two modules: an enhanced relationship and inference engine enabled by smart contracts to extract meaningful information and hidden insights from IoT and user device network data and an IoT network established by blockchain to provide security and integrity to

sensing data. The upgraded smart contract aims to give consumers practical applications by providing simple access, control, real-time monitoring, and immutable logs of devices dispersed across different domains. The inference engine module looks for important information and underlying patterns in data gathered from IoT settings to provide simple services and enable effective decision-making. They describe intrusion detection estimation-enabled private blockchain-based smart home network architecture for the Fused Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) system model [28]. This research examines the RTS-DELM approach used in blockchain-established elegant homes to look for potentially harmful activities. The decision-level and data fusion techniques are also applied to improve accuracy.

III. PROPOSED METHOD

The most important objective of the suggested study is to secure data transfer on "Internet of Things networks" by integrating blockchain knowledge and "machine learning'. The integration of both these technologies provides a secure and intelligent framework. Where blockchain ensure data integrity, and machine learning helps to enhance the system adaptability in real-time conditions. The planned work's general architecture is seen in Fig. 1 and the integration of blockchain and machine learning is shown Fig 2.

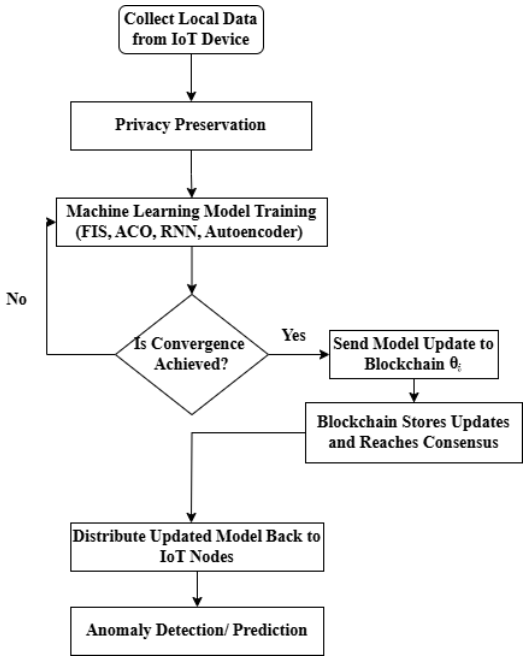

Fig 1. Integration of blockchain and machine learning techniques

A. *Imagine authentication with a password*

The secure agent gives a four-digit number based on a picture for authentication. Every user first registers with the secure agent with their login credentials, which include their user ID, password, role, and fingerprint. Services then register their credentials with the secure agent, providing their service ID, name, location, and service categories. After the registration procedure is finished, the authentication process starts. Throughout the login procedure, users enter their password visually. One hundred pictures are in a 10*10 image grid on the login page. There are three copies of each picture, and users must specify a password consisting of four numbers that they can choose from the photos by clicking on the picture grid. The secure agent identifies the user as valid if the password is accurate; authentication is unsuccessful. The IAES method generates a long-term secret key for examination verification, which the protected representative supplies. The password, secret key, and user and examine recommendations are encrypted and stored in the Cloud Chain to improve security. The exclusive step of the method is similar, but the alteration is occurring, as shown in the following phases.

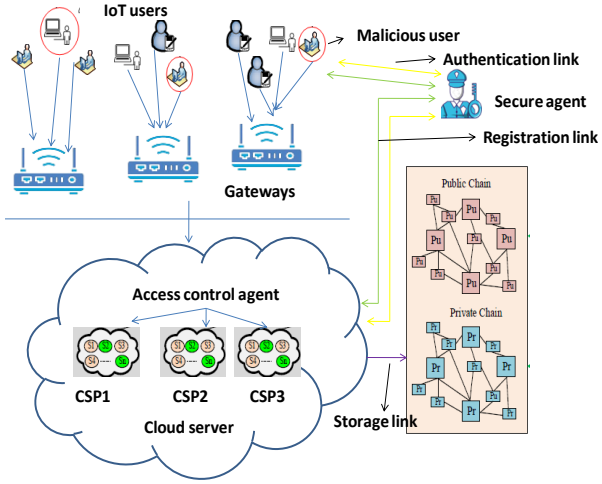

Fig. 2. Overall architecture of the suggested design

The algorithm is connected through supplemental key creation and adds key steps.

Step 1: Using the registered credentials, generate the key.

Step 2: A 256-bit key matrix is produced using an 8-bit LSFR based on registered IDs.

Step 3: 8-bit linear feedback squelch with maximum duration $\mathcal{G}^8 + \mathcal{G}^8 + \mathcal{G}^8 + \mathcal{G}^8 + 1$, that produces $2^8 - 1 =$ 2558-bit FSR is a maximum length feedback polynomial with random outputs.

Step 4: Using LFSR, which indicates the key from the key matrix, create a random integer at each round.

Step 5: The XOR operation processes the registered credentials, m1 and m2, at the addition round key phase.

Step 6: Reduce the number of rounds to half of the initial round. Based on the random number, select one key from the key array.

TABLE I
IAES ALGORITHM PARAMETERS

AES algorithm	192 bits [1]	Proposed 256 bit
Number of rounds	13	15
Size of the key	7	9
Size of the block	5	5

The master key M, which is a 256-bit key in key expansion, is used by the AES algorithm to secure itself as it generates a key schedule using an essential expansion routine. Ti: The first sub-key generated by the key expansion is the initial key, which yields an 11-sub-key array with a 16-length that is functional for the digits. An identically sized sub-key is generated for each encryption round. A substitution table is used as input to carry out a one-by-one byte value replacement process utilizing the nonlinear and invertible S-box. Table I displays the parameters for the AES algorithm.

Pseudocode for encryption
Input: Registered credentials
Output:
Begin
State = Initstate-run (pictxt, secretM)
Add key (state, sk_0)
For j=1 to g^e-1 do
Sub Bytes (state)
Shift Dins (state)
Mix Columns (state)
Add key (state, m_j)
Sub bytes (state)
Shift Rows (state)
Add Key (state, m_{tj-1})
End for
End

B. User Demand Exploration

Following verification, the gateway looks into user-examined requirements to make sure the CSP isn't being hacked. The gateway first verifies whether an incoming request is valid or fraudulent. Based on parameters like examining innovation rate, discussing needs, and time trudge, the suggested work uses a fuzzy presumption organization to validate the arriving packets. The used FIS comprises two self-organized evolving FIS and a conclusion producer that, when combined, provide better accuracy and computational efficiency when making judgments based on user requests. The fraudulent requests are discarded in this step, and only authentic requests are submitted for service classification.

A coarser semi-supervised learning process is necessary for healthy models to perform equally well as supervised and semi-supervised models. However, the optimal configuration may be troublesome in rural areas.

During this step, the supervised and semi-supervised deuce sub-models are certified using the information chunks $\mathcal{N}_1, \mathcal{N}_2, \ldots \mathcal{N}_{\mathcal{T}}$ with the associated tag values $\mathcal{F}_1, \mathcal{F}_1, \ldots, \mathcal{F}_{\mathcal{T}}$ The following stage and twitch to be trained from unlabeled data hunk come after the algorithm process labeled with tagged data.

At this point, the information base is being advanced by quasi-classification of the unlabeled pieces. If we have a new information hunk $\mathcal{N}_t(t > \mathcal{T})$, we may crop the confidence grades to get an example of $\mathcal{N}_t$. $\widehat{\omega}_t = \{\widehat{\omega}(n_{t,1}), \widehat{\omega}(n_{t,2}), \ldots, \widehat{\omega}(n_{t\mathcal{P}_t})\}$ in support of dishonorable supplementary information.

$$if\left(\max_{i=1,2,..,R}\left(\widehat{\omega}(n_{t,m})\right) \geq \psi_0\right) then\left(\widehat{\mathcal{N}}_t \leftarrow \widehat{\mathcal{N}}_t \cup \{n_{t,m}\}; \widehat{\mathcal{F}}_t \leftarrow \widehat{\mathcal{F}}_t \cup \{\hat{n}_{t,m}\}\right) \quad (1)$$

Where ψ_0a threshold for is classifying these examples with strong confidence in their lesson tags; $\hat{n}_{t,m}$ is the predicted label of $n_{t,m}$that results from $\widehat{\omega}(n_{t,1})$ and $\widehat{\mathcal{N}}_t$ is the collection of pseudo-labelled information examples that come from$\mathcal{N}_t$, with $\mathcal{F}_t$ being the conforming quasi labels. Tasters who satisfy disease are not part of or related to the data. The quasi-labels associated with this data are appended to $\widehat{\mathcal{F}}_t$.

Consider using these anticipated labels to tell the database, for instance, about the exceptional tasters of $\mathcal{N}_t$. Thus employing these instances in advance to obtain dishonourable information.

$$\varphi_2^R(n_{t,m}) = \frac{\varrho_2^R(n_{t,m})}{\sum_{j=1}^R \varrho_2^j(n_{t,m})} \quad (2)$$

The sickness 7 score assesses whether the samples match the quasi-code tags based on surety ratings.

$$if\left(\hat{\mathcal{F}}_{t,m} = arg\max_{i=1,2,..,R}\left(\varphi_2^u(n_{t,m})\right)\right) then\left(\left(\widehat{\mathcal{N}}_t \leftarrow \widehat{\mathcal{N}}_t \cup \{n_{t,m}\}; \widehat{\mathcal{F}}_t \leftarrow \widehat{\mathcal{F}}_t \cup \{\hat{n}_{t,m}\}\right)\right) \quad (3)$$

When $n_{t,m}$ is included in complaint number 3, it might be utilised to indicate that the parties involved are unable to agree on the period label for $n_{t,m}$. Because of this, *mmust be handed down and cannot be used to mount embarrassm*
.

The current knowledge series is completed to the method after $\widehat{\mathcal{N}}_t$ and $\widehat{\mathcal{F}}_t$ have been eliminated, and if the location of the mass statistics is available, it is $(t \leftarrow t + 1)$.

This integrates the idea that every unlabelled trial at the policymaking stage should have a fresh, well-read awareness from the unlabeled data into the resolution-making course label t. This accepts the possibility that both copies have been prepared.

$$\hat{\mathcal{F}} = R^*; R^* = \underset{R=1,2,..,R}{\text{argmx}}\left(\frac{\varphi_2^R(n)+\widehat{\omega}^R(n)}{2}\right) \quad (4)$$

The process and customer demand resolution that enabled illogical assumptions about the objective and the development of the most recent wisdom judgment, as well as the assignment of partial tasks along with copies, allowed for route junction and learned reproductions, which in turn started the expectation of the administrative lecture and amenity assortment manner for fulfilling employee wish cares.

The gateway itself additionally categorises the valid requests as responsive and non-sensitive queries. The suggested work uses an improved machine learning technique called SCSVM, which was established in the examiner category to carry out efficient, valid request categorization. Using SCSVM instead of traditional SVM is justified because it reduces undesired computation and does not require a model training procedure.

Examples of standard datasets are allowed to be $\mathcal{L} = [\ell_1, \ell_2, .., \ell_t]^z \in \mathcal{J}^{\mathcal{H}\times\mathcal{F}}$ and the hyperplane for aim resolution be $\mathcal{G}(\ell) = \psi\vartheta(\ell) - \delta = 0$. we make the following assumption and break down the hard optimization:

$$\min_{\psi\in\mathcal{G},\zeta\in\mathcal{J}^{\mathcal{H}},\delta\epsilon\mathcal{J}} \frac{1}{2}\|\psi\|^2 + \frac{1}{\mathcal{H}_{\mathcal{E}}}\sum_{j=1}^{\mathcal{H}}\zeta_j - \delta \;\; s.t.\psi\vartheta\left(\ell_j\right) \geq \delta - \zeta_j, \zeta_j \geq 0 \quad (6)$$

For the overhead equality, $\mathcal{H}$ stands for the keep-fit dataset charity, $\mathcal{E}$ for the regularisation constraint, ζ_j for the floppy flexible agreement to any dataset, δ for the decision flat outside that possibly will be evident by distribution, and ϑ for the way of spatial mapping the statistics. By making known to multipliers $\zeta_j \geq 0$ as well as $\lambda_j \geq 0$ and interpreting the Lagrange balances, the classic is decoded eventually.

$$\mathcal{F}(\psi,\zeta,\varsigma,\lambda) = \frac{1}{2}\|\psi\|^2 + \frac{1}{\mathcal{H}_{\mathcal{E}}}\sum_{j=1}^{\mathcal{H}}\zeta_j - \delta - \sum_{j=1}^{\mathcal{H}}\varsigma_j\left[\psi\vartheta(\mathcal{L}_j - \delta + \zeta_j\right] - \sum_{j=1}^{\mathcal{H}}\lambda_j\zeta_j \quad (7)$$

Utilizing the fractional discrepancy of the variables in the comparison beyond, one may acquire the pairwise custom of the optimization unruly [7]:

$$min_{\varsigma}\varsigma^{z}\mathcal{Y}_{\varsigma} \quad (8)$$

$$s.t. \leq \varsigma_j \leq \frac{1}{\mathcal{H}_{\mathcal{E}}}, \sum_{j=1}^{\mathcal{H}}\varsigma_j = 1 \quad (9)$$

$\mathcal{Y}$ is found inside the kernel matrix of $\mathcal{Y}_{ji}$ and $\mathcal{Y}_{ji}$ can be uttered as:

$$\mathcal{Y}_{ji} = \mathcal{P}\left(\ell_j,\ell_i\right) = \vartheta(\ell_j)\vartheta(i) \quad (10)$$

In this gaussian and genuine kernel principle, $\mathcal{P}\left(\ell_j,\ell_i\right)$ is the kernel collecting. For the RBF essential part purpose, for instance, the organised diagram is presented with the kernel function's adjacent unique parameter, ω, continuously indicating the RBF kernel function's width.

$$\mathcal{P}\left(\ell_j,\ell_i\right) = M^{\frac{-\left\|\ell_j,\ell_i\right\|^2}{2\omega^2}} \quad (11)$$

It is possible to solve ς and multiply ψ and δ separately by figuring out the excessive quadratic indoctrination trick:

$$\psi = \sum_{j=1}^{\mathcal{H}}\varsigma_j\vartheta(\ell_j) \quad (12)$$

$$\delta = \sum_{j=1}^{\mathcal{H}}\varsigma_j\vartheta(\ell_j,\ell_i) \quad (13)$$

From the disentangled ψ and δ, an overexcited resolution plane in the astronomical article may be established.

It is customary to organize the test sample $\mathcal{G}\left(\mathcal{Q}_p\right)(\mathcal{p} = 0,1,..,\mathcal{E})$ in support of the exercise $setQ = [\mathcal{Q}_1,\ldots..,\mathcal{Q}_{\mathcal{E}}]^{z} \in \mathcal{J}^{\mathcal{E}\times\mathcal{F}}$ using an assessment job H(Pq)(q = 0,1,…,F) based on the detachment of Euclid.

$$\mathcal{G}(\mathcal{Q}_p) = sigt(\vartheta\psi\left(\mathcal{Q}_p\right) - \delta) \quad (14)$$

The trial illustration $\mathcal{Q}_p$'s supervisory role $\mathcal{G}(\mathcal{Q}_p)$ is private as a positive session, and it is arranged by arranging the circumstances of $\mathcal{Q}_p$ concerning the pronouncement hyperplane.

C. Secure and Optimal Service Selection

After legitimate requests are classified as sensitive or non-sensitive, the recommended work is to perform the best and safest service selection for the sensitive and non-sensitive requests, respectively. More specifically, a request from a sensitive user in the CSP is matched with the best and safest sensitive service, and a request from a non-sensitive user is matched with the best and safest non-sensitive service. Ant colonies are optimised based on service availability, trust ratings, QoS, and user input to achieve the best and safest possible service allocation. These metrics offer weight values and rankings to collect responsive and non-sensitive services in the CSPs. A sensitive request from the ranking set is assigned to the highest-rated sensitive service, while a non-sensitive request is assigned to the highest-ranked non-sensitive service.

In the end, the suggested work implements the "Moving Target Defence (MTD) mechanism", which involves the MTD representative, a blockchain-deployed agent switching service IP addresses based on gateway data to prevent external attackers' attacks on the services provided by cloud service providers. The MTD agent dynamically rotates the IP addresses of the services from the pool of "IP addresses in the Domain Name Server (DNS). Through MTD, attacker costs can grow without affecting user quality of service (QoS) in CSPs".

Often employed as a metaheuristic to solve combinatorial optimisation issues such as the Optimal Path Problem or the Traveling Salesman Problem (TSP), the "Ant Colony Optimization (ACO)" approach is inspired by the foraging behaviour of ants. Applying ACO typically entails stating the problem, graph-spatializing it, initialising pheromone levels, using virtual ants to build solutions, evaluating the quality of the solution, updating pheromone levels, iterating, coming to an end based on a stopping criterion, and optionally post-processing the work. The ACO algorithm's steps are listed in the following order. Here, we use pheromone trail matrix in ACO denotes the accumulated pheromone levels on the edges of a search space, which guides the ants to reach the better solution. ACO is applied to improve service allocation by simulating the foraging behavior of ants. This can efficiently matching the sensitive and non-sensitive request based on QoS.

Startup: Configure the early pheromone following a template, the number of iterations, and the number of ants. The pheromone trail matrix stores the quantity of pheromone on every border of the grid.

2. Creation of candidate solutions: Using a grouping of the pheromone follow and the reserve between the present node and the subsequent node, each ant repeatedly chooses which node to visit next to generate candidates. The primary goal of probabilistic rules is to assess the chance of occurrences or outcomes established on existing facts and make well-informed predictions or judgments in undecided situations. A probabilistic rule, provided by:, is used to make the selection.

$$\mathcal{Q}_{ji} = \frac{[\tau_{ji}]^{\alpha}.[\eta_{ji}]^{\beta}}{\sum_{m\in\mathcal{V}_{unvisite}}[\tau_{jm}]^{\alpha}.[\eta_{jm}]^{\beta}} \quad (15)$$

The pheromone following on the border (j,i) is represented by τji, and $\mathcal{Q}ji$ is the likelihood of selecting node i, known that the ant is presently at node i. The reserve among nodes i and j is reciprocal and is represented by the η_{ji}. α is the pheromone follow significance feature, β represents the collection of unvisited nodes, where unvisited is the heuristic information significance factor. It refers to the influence of additional problem specific information, which helps ants to make more informed decisions.

3. Pheromone trails are updated based on the efficacy of the remedies found once the ants have finished their journeys. Higher pheromone trails are given to reasonable solutions,

whereas lower pheromone trails are given to wrong solutions. As stated by the updated rule

$$\tau_{ji} = (1-\rho)\tau_{ji} + \Delta\tau_{ji} \quad (16)$$

The measure of pheromone stored on the border (j,i) is represented by $\Delta\tau_{ji}$, whereas ρ represents the evaporation rate.

4. Repeat steps 2 and 3 as needed until the stopping criterion is met. The number of iterations, the longest time restriction, or the calibre of the answers discovered can all be used as the stopping criteria.

5. Pick the optimal course of action: The tour's duration or other objective function is used to determine the best outcome.

The ACO optimisation technique employs a pheromone trail to direct an ant colony toward optimal solutions. The pheromone trail, which is modified by the algorithm according to the calibre of the solutions found, impacts the ants' choice of the subsequent terminal. The applicability of the technique is well suited to large search regions. While they are distinct algorithms used in artificial intelligence and optimisation, Ant Colony Optimization (ACO) techniques have many similarities. These parallels include the capacity to be applied to intricate issues, the ability to balance exploration and exploitation, the potential for distributed and parallel processing, iterative improvement, and stochastic optimisation.

Relatively tiny jumps indicate the tomtit moment. Using a phase scope f, one may achieve this solution by adding numerically. If some people arrange success in terms of education, then the group leader should be positioned at this boundary, and the followers should be placed first to get the best outcome.

D. Adaptive access control and dual revocation

We first allocate the services to the right users and then create a new access control mechanism based on role, trust, and attribute in that sequence. Service type and user roles are taken into account. The user's attributes are displayed, including user ID, role, password, and biometrics. The Recurrent Neural Networks technique may be used to define trust based on the characteristics and roles of the users. The suggested access control system uses RNN to build dynamic access restrictions that take into account the users' current status. RNN are used for detecting anomalies in incoming request. Based on the dynamic policies, we also create an access control map. Illegal access may be quickly identified by creating an access control map, and it can be lessened by reversing two times. Revocation in two flavours: hybrid IDS-based user revocation and attribute revocation.

Because a vast quantity of data comes from many sources, the RNN autoencoder compresses the input data. Therefore, adopting data compression to save hardware storage is crucial. Increased communication bandwidth may also benefit the system's performance.

In addition, the decoder uses the compressed input data to synthesize new data. Assume for the moment that the malicious contents from the link ℓ to be written as follows were extracted ω using the auto-encoder β. $$\ell = \ell^1, \ell^2, \dots, \ell^k!!.

For each link, ℓ^k represents the total amount of harmful materials.

After eliminating the hidden harmful contents from the link ℓ, the auto-encoder βe deduces the malicious contents $\mathcal{D}_k$, which is then formulated as βe: $\ell \to \omega$. Meanwhile, the decoder βc rebuilds the link and writes βe: $\omega \to \ell$ after that. In the case of the auto-encoder and auto-decoder, where ω: content illustration for the connection.

After being taught, the RNN autoencoder βe Fig. out how likely it is to identify harmful connections. The RNN may trigger the link's whole, harmful content and involves the hidden state V_g. Thus, every time step n, computed by equations 17–18, updates the input and output hidden states of the RNN.

$$V_g(n) = f(\beta e)(\mathcal{Z}_j \cdot V_g(n-1) \times \ell^n) \quad (17)$$

$$f(n) = f(o)\left(\mathcal{Z}_o \cdot V_g(n-1) \times \ell^n\right) \quad (18)$$

Once the link has been accessed, the final hidden state of the RNN is applied as a content illustration ω for the link. GRU is used in conjunction with RNN to reduce computational complexity, enhance memory capacity, facilitate successful model training, and provide early observation if a situation arises that calls for early observation in order to make future predictions.

To ascertain the likelihood of harmful information, an automated encoder βe obtains the input link $\mathcal{J}(n)$ from the GRU. The input to the subsequent hidden state, $V_g(n)-1$, is processed using the sigmoid function. Until the output decision $\beta e(n)O$ about the harmful contents from the provided link is achieved, this procedure keeps going. To identify any potentially harmful information in the following URL, the encoder is reset. The encoder has updated features $\mathcal{E}\beta e(n)$that are necessary for updating the subsequent layer. Furthermore, $\mathcal{B}\beta e(n)$ the process can be activated by the encoder.

The following is the formula for content detection using automated encoding with the GRU: In this case, at first for $n = 0$ and $\beta e(n)O = 0$, Therefore, it may be ascertained as:

$$\mathcal{E}\beta e(n) = \sigma_{sigmoid}\{(\forall\rho.\mathcal{E}\beta e(n,\ell) + (\forall \cup .\mathcal{E}\beta e(n, V_g(n-1)) + \forall a.\mathcal{E}\beta e(n)\} \quad (19)$$

$$\mathcal{R}\beta e(n) = \sigma_{sigmoid}\{(\forall\rho.\mathcal{R}\beta e(n).\ell) + (\forall \cup .\mathcal{R}\beta e(n).V_g(n-1) + \forall a.\mathcal{R}\beta e(n)\} \quad (20)$$

$$\mathcal{B}\beta e(n) = \varphi g\{(\beta e(n)O.\ell)(\forall\mathcal{B} \cup .\mathcal{B}\beta e(n) \times (\mathcal{R}\beta e(n) \oplus V_g(n-1)) + \forall a.V_g\} \quad (21)$$

$$\beta e(n)O = \{(1-\mathcal{E}\beta e(n)) \oplus (\beta e(n)O - 1) + (\mathcal{E}\beta e(n) \oplus \mathcal{B}\beta e(n))\} \quad (22)$$

Where $V_g(n)\varphi g$ is the hyperbolic tangent and $\sigma_{sigmoid}$is the sigmoid

The auto-encoder's parameters, $\forall\rho$, $\forall \cup$, and $\forall a$, are utilized to aid in the detection of malicious data.

$$\omega = \beta e(n, \forall\rho) \quad (23)$$

One crucial component that takes the ω as an input to start the construction process is the decoder. To generate the malicious output content sequence, another RNN is utilized in the construction of the decoder βc. $\{j = j^1, j^2, \dots, j^k\}$With every time step n, the decoder's concealed state is triggered.

$$V_g(n) = f(\beta e)\left(\mathcal{Z}_j \cdot V_g - 1, j^n\right) \quad (24)$$

The total likelihood of creating the malicious output

sequence that generates the input link ℓ is

$$q_{\!}(j(|\ell;\theta_c|) = \prod_{j=1}^{k} q_{\!}(j_n|j_n-1|, j_n-2, \ldots j_1, \omega, \theta_c) \quad (25)$$

Whereθ_c: the decoder's argument

To lessen the negative impact of the probability p for all of the malicious contents of the connection, the auto-encoder's components mutually train with each other.

$$\ell^k(\forall\rho, \forall \cup, \forall a, \theta_c) = -\sum_{n=1}^{k} log q_{\!}(j_n|\ell_n; \rho, \forall \cup, \forall a, \theta_c) \quad (26)$$

The trust model may forecast each node's trust if the normalized trust complies with the input data for the LSTM architecture-based trust modeling.

A recurrent neural structure makes up the LSTM model. Cell states, which preserve context from previous observations to more accurately forecast future states, compose its fundamental structure. Give the input and output data at time n, y_n and g_n, respectively. Three gating mechanisms make up the model: j, f, and o stand for contribution gateway, not remember gate, and output gate, correspondingly. $\mathcal{D}_n$ represents the memory cell's state value at time n. The following steps comprise the updating process of an LSTM unit:

The forget gate is utilized by the LSTM layer to ascertain the information required to discard the input $\mathcal{Y}t_n$ at the current step, as well as g_{n-1} from the previous iteration. The impact of past data on the current memory unit's state value is managed by the forget gate. The procedure's purpose is:

$$f_n = \sigma(\mathcal{Z}_f.[g_{n-1}, y_n] + a_f) \quad (27)$$

Where the forget gate's bias vector is denoted by a_f and its weight matrix is represented by $\mathcal{Z}_f$. With a range of 0 to 1, $\sigma(\cdot)$ represents the logistic sigmoid commencement purpose. Total memory is represent by a value of 1, and zero signifies that all data should be discarded.

$$\sigma(w) = \frac{1}{1+e^{-w}} \quad (28)$$

Using the input gate, which regulates how the current input affects the memory unit's state value, the LSTM chooses what input data is added to the memory information stream at each iteration. This is how the procedure is expressed:

$$j = \sigma(\mathcal{Z}_n.[g_{n-1}, y_n] + a_j) \quad (29)$$

A potential value for the memory unit in the present $\overline{\mathcal{D}}_n$ is determined by:

$$\overline{\mathcal{D}}_n = tang(\mathcal{Z}_d.[g_{n-1}, y_n] + a_d) \quad (30)$$

Where in $tang\,(\cdot)$, the hyperbolic tangent function, has values between −1 and 1.

$$tang\,(w) = \frac{e^{w}-e^{-w}}{e^{w}+e^{-w}} \quad (31)$$

To manage the material transferred to the following iteration, or the memory unit's output state value, the LSTM model employs an output gate. An output gate's calculation is as follows:

$$o_n = \sigma(\mathcal{Z}_o.[g_{n-1}, y_n] + a_o) \quad (32)$$

The corresponding bias vector of the affine transformation is a_o, and $\mathcal{Z}_o$ is the output gate's weight matrix. When $\odot$ is used as the point multiplication operation, the memory unit's state value is modified as follows:

$$\mathcal{D}_n = f_n \odot \mathcal{D}_{n-1} + j_n \odot \overline{\mathcal{D}}_n \quad (33)$$

Ultimately, the value of the output is computed by:

$$g_n = o_n.tang(\mathcal{D}_n) \quad (34)$$

Furthermore, infectious strictures were excisioned covertly. Consequently, the contrastive model's knowledge route becomes less necessary to accomplish firm mining, causing the exercise duration to slow down.

IV. Experimental Results

In this part, we offer the suggested consumer-centric approaches to data transmission security on IoT networks, which integrate blockchain technology and machine learning. There are three subsections in this experimental study: comparative analysis, simulation setup, and explicit. As may be seen from the results section, the suggested work performs better than earlier efforts.

A. Simulation Setup

The NS-3.26 network simulator is used to implement the simulation result of this suggested work with IoT simulation, which enhances the performance of this study. Our approach produces higher performance, as demonstrated by comparing the suggested framework with other performance indicators. The setup of the system is shown in Table (II).

TABLE II
System Parameter

Hardware configuration	Hard disk	62 GB
	RAM	4GB
	Processor	CPU: Intel(R) Core(TM) i5-4590S @ 3.00 GHz
Software configuration	Network simulator	NS-3.26
	Operating system	Ubuntu 14.04 LTS

B. Comparative analysis

In this segment, we presented the comparative study of two current works, AP2FL and Cloud-IoT, with the suggested ML and Blockchain for Consumer-Centric Approaches in safeguarding Data transmission over IoT Networks. The most important objective of this research is to develop an access control organization based on safe cloud security services. In terms of attack detection rate, overhead, unauthorized access, throughput, traffic rate, and latency, the suggested work performed better.

Impact of attack detection rate

The rate at which attacks are detected in cloud security services is estimated using this KPI. This may be described as follows: the ratio of detected attacks to the growing number of users is commonly used to depict this.

$$U_o = \frac{\varphi_h}{G\prime} \quad (35)$$

Where U_o indicates how often the assault is detected. This indicates the ever-increasing number of users that the system with a high detection rate may reach to obtain a safe cloud security service. It also explains the assaults detected $\mathcal{G}'$. The assessment of the uncovering rate and numeral of requirements

for both the suggested and current mechanism is shown in Fig (3). Compared to previous work on AP2FL and Cloud-IoT, the evaluation result shows that the suggested has a higher recognition rate. Our approach involves photo verification of the pictures by the protected agent to verify that together, the consumer and the examiner are real. This helps to decrease harmful traffic in the network by excluding illegitimate users. In addition to avoiding traffic in the network, which raises transfer masses and results in inefficient load balancing, the current approach pays little attention to legitimate users. However, some environment users may be sending fraudulent traffic over the network.

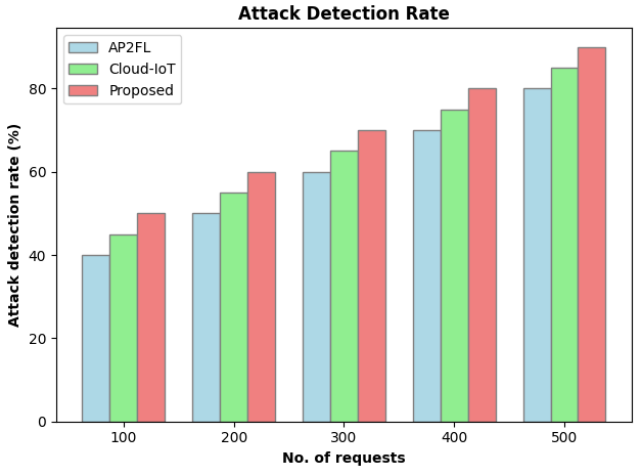

Fig. 3. Attack detection rate

When comparing the suggested Integrating ML and Blockchain approach to the shortened 52, where the performance of the outgoing works is 40, and the AP2FL is 35, the show aggression recognition rate is raised. The suggested work's average attack detection rate for 500 requests is 96, indicating that it outperforms previous work like AP2FL's 85 and Cloud-IoT's 70. The numerical data displayed in the graph suggest that our suggested approach outperforms the current work.

Impact of overhead

The overhead refers to the ratio of lost bandwidth needed to transfer the payload. The extra information given to the packet header above the payload ensures that a packet reaches its intended recipient.

$$OG = \frac{x_{eu}}{JW_h} \tag{36}$$

Where $\mathcal{JW}_{\hbar}$ represents the sent packet, and x_{eu} shows the overhead packets that are sent during overhead. Fig. (4) compares the number of requests and overhead for the proposed and completed works. The comparative analysis reveals that the proposed approach has achieved lower overhead compared to the ongoing work on AP2FL and Cloud-IoT. We carry out the optimum service selection by the secure choice for the sensitive and non-sensitive services in the CSP for a non-sensitive user request to obtain the optimal secure service allocation using those metrics. We assign weight values and rank the set of sensitive and non-sensitive items. While determining the cloud service allocation characteristic, the current work assigns services by considering less the service selection values of the ideal metrics that may be allocated to low features of determinants of the optimal features allocation.

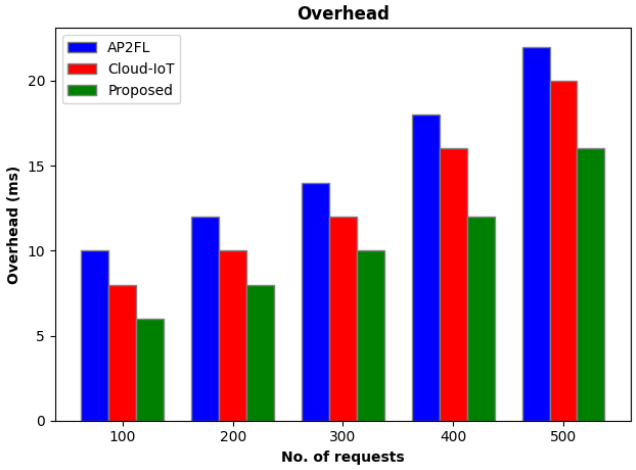

Fig. 4. Overhead

When comparing the suggested technique to the shortened 7, where the existing work performs 12 and Cloud-IoT does 14, the overhead is decreased. The average overhead of the proposed work for 500 requests is 15, indicating that we outperform existing work, with scores of 23 for AP2FL and 28 for Cloud-IoT. The graph's numerical results show that our recommended task performs better than the existing endeavour.

Impact of throughput

The quantity of data packets that are successfully transferred during a specific amount of time is known as throughput, and it may be expressed as,

$$\mathrm{NQ} = \frac{\Gamma_{\mathrm{suc_x}*\mathrm{avg_{xe}}}}{o} \times 100\% \tag{37}$$

Where $\mathrm{suc_x}$the packet stands for the successful packets, o for the average packet size, and t for the entire amount of time was transmitted. The throughput and number of requests for both the proposed and current works are compared in Fig (5). The comparative result shows that, when compared to the previous work on Cloud-IoT and AP2FL, the suggested has achieved reduced overhead. To effectively decide, we utilize FIS, composed of two self-organised developed FIS and a decision maker, based on user demands, which offer enhanced accuracy and computing efficiency, respectively. Genuine requests are submitted for service categorisation in this phase, with the fraudulent requests being rejected. Valid requests are also divided into sensitive and non-sensitive categories by the gateway. The current method investigates user requests with less attention to user requests. It makes decisions on user requests that consider limited features, which offers less accuracy and throughput while using a basic machine learning algorithm that varies slightly from the user-assigned process of that work. It is not yet possible to classify a user who may be inadequately supplying packet services based on their valid requests to get the users' access to the resources.

The throughput of the suggested technique is higher than the existing works' 32 and 28 when compared to the truncated 50. We surpass the present work, which is 290 for Cloud-IoT and 310 for AP2FL, with an average throughput of 342 for 500 requests in the proposed work. The numerical data displayed in

the graph suggest that our suggested approach outperforms the current work.

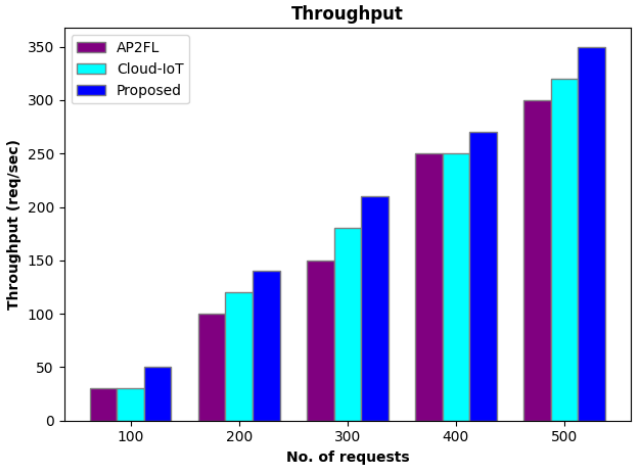

Fig. 5. Throughputs

Impact of delay

The stoppage indicates how long it took for the suggested employment to upload and download the services, respectively, and the user request. The delay time needs to be reduced as much as feasible to enhance the data rate.

$$D = \frac{\sum_{i=1}^{N}(T_{received,i} - T_{sent,i})}{N} \quad (38)$$

The comparison between the number of requirements for both planned and accessible mechanisms and the delay is shown in Fig. 6. The comparative result shows that the suggested has reduced overhead compared to the current work on Cloud-IoT and AP2FL. Our approach involves thwarting external attackers' attacks on cloud service providers' services. The system we propose to implement does this by randomly assigning service IP addresses based on gateway information. The IP addresses of the services are dynamically rearranged by the agents from the DNS pool of IP addresses. By using CSP services, the attacker's expenses rise without compromising the users' quality of service. Attacks on the services that were provided, as well as the providers' disregard for the network attacker, cloud service comparison, and the attackers' provided quantity of the environment's structural and functional capabilities of the delay procedures of the identified attackers' cloud services, were conducted in the work that has already been done.

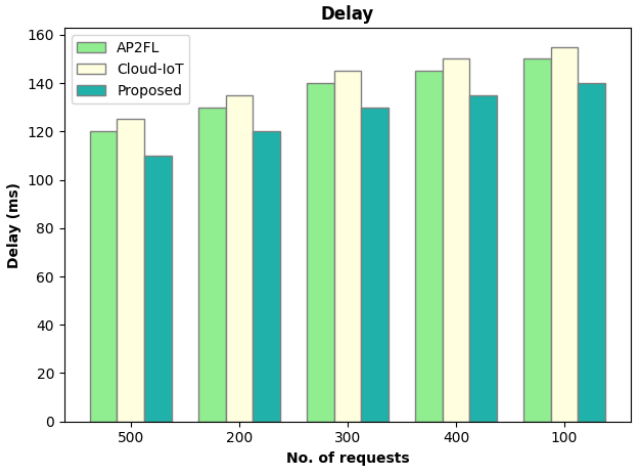

Fig .6. Delay

In contrast to the shorter 110, where the current works do 125 and 135 jobs, the proposed approach reduces delay in task completion. Based on the average delay of the proposed work for ten requests, which is 150, we surpass existing work, such as AP2FL, which is 180, and Cloud-IoT, which is 192. The numerical results shown in the graph indicate that our proposed method performs better than past efforts.

Impact of unauthorized access

Processing a storage request involves using technology to compute and store data. A computer's storage system allows it to store data for a temporary or permanent period.

The contrast between the amount of requests for both proposed and current works and illegal access is shown in Fig (7). The comparative result shows that the suggested has reduced overhead compared to the current work on Cloud-IoT and AP2FL. At work, we employ an access control map that shows odd versions for a given value if a user's attribute expires before the time stamp that is set. Rather than penalizing, the proposed work informed that attribute variation performs attribute updating. Furthermore, a virtual firewall, a hybrid intrusion detection system, is installed in the cloud environment to monitor user storage request traffic and differentiate between safe and dangerous requests. The suggested work's qualities and distribution are used for user identification in the current work, which improves power distribution and preserves the work's determinacies.

When compared to the shortened 15, wherever the exit mechanism performs 25 and 35, the proposed technique performs illegal access lowered. Our work outperforms prior work such as AP2FL, which has an attack detection rate of 65, and Cloud-IoT, which has an attack detection rate of 85, with an average of 35 for 250 storage requests. Our suggested work outperforms previous work, according to the numerical findings displayed in the graph.

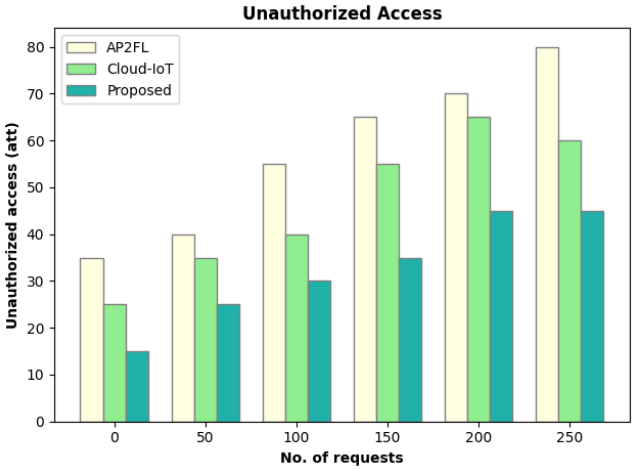

Fig. 7. Unauthorized access

Figure 8 shows trust score based on the changes in user behavior. Initially, the trust score is set at the base level,finally it fluctuates based on the user interactions.

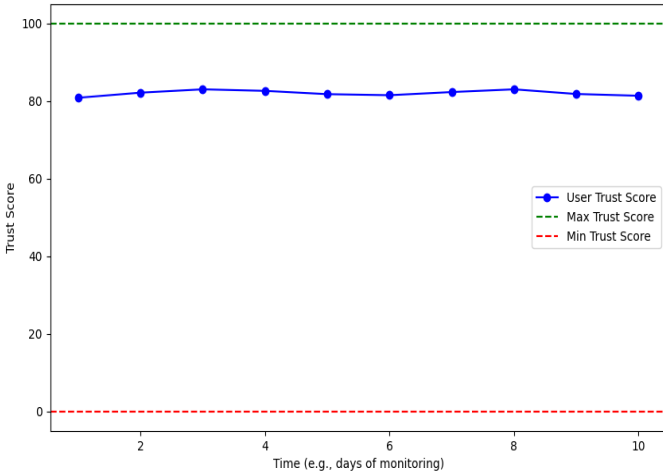

Fig 8: RNN based trust mechanism

Figure 9 shows the overall comparison analysis with the state of art methods of Ant Colony optimization with Multi Kernel Support Vector (ACOMKSVM) [29], Ant colony optimization (ACO) [30], miner revenue optimization algorithm (MROA) [31], Genetic Algorithm based ant Lion Optimization Energy Efficient Multipath routing protocol (GALOEEM) [32]. When compared with these models the suggested model outperforms with the existing model in terms of security, QoS, and resource efficiency.

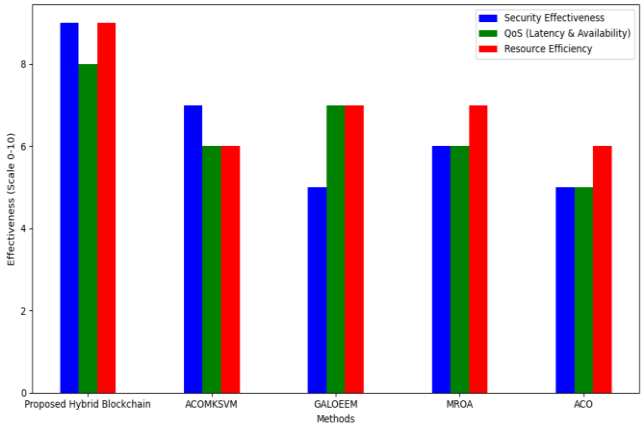

Fig 9: Comparative analysis with state of art methods

Figure 10 shows the service selection process based on ACO algorithm which illustrates the selection frequency and attractiveness of services like A) authentication service, B) Encryption service C) Request verification service D) Service classification service E) MTD service over 100 iterations.

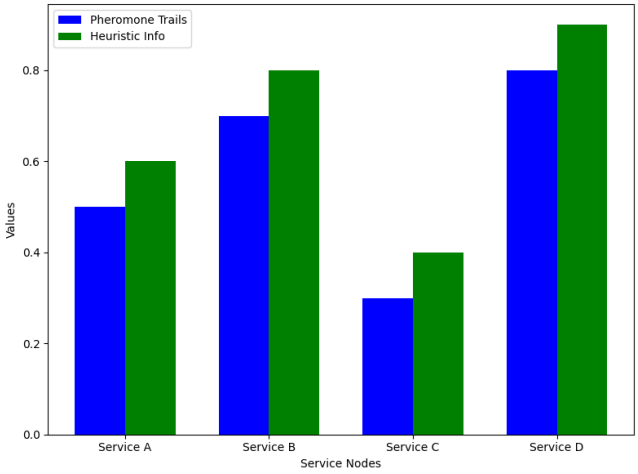

Fig 10: Comparison of pheromone trails and heuristic information in service selection using ACO algorithm

V. CONCLUSION

This study presents a comprehensive approach to enhance data security and privacy in Internet of Things networks through the combination of Blockchain and Machine Learning technologies. Key issues with data integrity and safe access control are addressed by the suggested hybrid blockchain approach, which combines public and private blockchain functionality. The system can promptly identify and address possible security risks by utilizing machine learning algorithms that incorporate sophisticated anomaly detection and classification methods. To further ensure that the system adjusts to changing security situations and offers strong defense against cyberattacks, neural networks based on transfer learning are used for dynamic trust validation. The integration of hybrid blockchain models ensures that the security mechanisms scale efficiently when the IoT networks expand. With the ability to handle large volumes of data and devices, the system can maintain high throughput by reducing latency. Also, the use of machine learning algorithms, allows the system to continuously

respond to user behavior and attack patterns, which ensures continuous security in a changing environment. Incorporating advanced optimization methods for resource management balances scalability, latency, and energy consumption concerns while simultaneously increasing system performance. Also, proposed model effectively protects against DDoS, man-in-the middle and data manipulation issues.

All things considered, this research provides a workable and novel approach to IoT network security, especially for consumer-focused applications. It increases the overall reliability of IoT devices and gives consumers more control over their data. The results of this study open the door for a wider acceptance and implementation of IoT technologies in numerous consumer and industrial applications by supporting the continuous efforts to create more secure, effective, and user-friendly IoT environments. Future research could focus on enhancing these technologies and investigating their potential integration into intricate and expansive IoT networks.

VI. Acknowledgment

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks ...” In most cases, sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page, not here.

References

[1] G. Rathee, C. A. Kerrache, C. T. Calafate, and M. S. Halimi, "SecureBlock: An ML-blockchain consumer-centric sustainable solution for industry 5.0," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 556-564, 2023.

[2] M. F. Ayub, X. Li, K. Mahmood, S. Shamshad, M. A. Saleem, and M. Omar, "Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 3, pp. 445-453, 2023.

[3] Y. Li, J. Shen, P. Vijayakumar, C.-F. Lai, A. Sivaraman, and P. K. Sharma, "Next-Generation Consumer Electronics Data Auditing Scheme Towards Cloud-Edge Distributed and Resilient Machine Learning," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 88-97, 2024.

[4] S. Bhardwaj, S. Harit, and A. Yadav, "Towards a software-defined networking model for consumer-centric content delivery network for IoT," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 1, p. e4903, 2024.

[5] P. Tiwari, A. Lakhan, R. H. Jhaveri, and T.-M. Grønli, "Consumer-centric internet of medical things for cyborg applications based on federated reinforcement learning," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 756-764, 2023.

[6] J. K. Mudhar, J. Malhotra, and S. Rani, "Blockchain-Based Decentralized Access Control Framework for Enhanced Security and Privacy for Consumer Electronic Devices," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 123-134, 2024.

[7] S. I. Popoola, A. L. Imoize, M. Hammoudeh, B. Adebisi, O. Jogunola, and A. M. Aibinu, "Federated deep learning for intrusion detection in Consumer-Centric Internet of Things," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 234-245, 2023.

[8] G. Liu, G. Bao, M. Bilal, A. Jones, Z. Jing, and X. Xu, "Edge data caching with consumer-centric service prediction in resilient industry 5.0," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 5, pp. 301-312, 2023.

[9] A. Shankar and C. Maple, "Securing the Internet of Things-enabled smart city infrastructure using a hybrid framework," *Computer Communications*, vol. 205, pp. 127-135, 2023.

[10] O. A. Alzubi, J. A. Alzubi, K. Shankar, and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, p. e4360, 2021.

[11] H. Vargas, C. Lozano-Garzon, G. A. Montoya, and Y. Donoso, "Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach," *Electronics*, vol. 10, no. 21, p. 2662, 2021.

[12] P. Kumar *et al.*, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326-2341, 2021.

[13] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," *Future Generation Computer Systems*, vol. 129, pp. 380-388, 2022.

[14] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Computers & Security*, vol. 109, p. 102393, 2021.

[15] D. Ye, X. Huang, G. Cheng, and M. S. Hossain, "Multi-Dimensional Contract Design for Energy-Efficient Wireless Sensing in Consumer-Centric E-Commerce Systems," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 235-247, 2024.

[16] S. Sathesh, S. Maheswaran, P. Mohanavenkatesan, M. Mohammed Azarudeen, K. Sowmitha, and S. Subash, "Allowance of driving based on drowsiness detection using audio and video processing," in *International Conference on Computational*

Intelligence in Data Science, 2022: Springer International Publishing Cham, pp. 235-250.

[17] A. Sasikumar, L. Ravi, M. Devarajan, S. Vairavasundaram, K. Kotecha, and N. Herencsar, "Sustainable Electronics: A Blockchain-Empowered Digital Twin Based Governance System for Consumer Electronic Products," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 112-124, 2024.

[18] P. K. Roy, A. Kumar, and A. Singh, "Advanced Learning for Phishing URLs Detection to Secure Consumer-Centric Applications," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 2, pp. 145-156, 2024.

[19] S. Sathesh *et al.*, "Smart Medicine Kit using Embedded IoT for Visually and Hearing-Impaired Patients," *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, vol. 8, no. 5, pp. 127-138, 2021.

[20] P. Kumar, N. Chauhan, N. Chaurasia, K. K. Agarwal, A. Vidyarthi, and D. Gupta, "Benevolence Behavior Based Message Forwarding Scheme for Consumer-Centric IoT Opportunistic Networks," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 6, pp. 675-688, 2024.

[21] Kumar, A., Rathee, G., Kerrache, C.A., Bilal, M. and Gadekallu, T.R., 2023. A secure architectural model using blockchain and estimated trust mechanism in electronic consumers. *IEEE Transactions on Consumer Electronics*, *69*(4), pp.996-1004.

[22] M. Wazid, A. K. Das, and S. Shetty, "BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 18-28, 2022.

[23] Rabieinejad, E., Yazdinejad, A., Dehghantanha, A. and Srivastava, G., 2024. Two-level privacy-preserving framework: Federated learning for attack detection in the consumer internet of things. *IEEE Transactions on Consumer Electronics*, *70*(1), pp.4258-4265.

[24] Nagarajan, S.M., Devarajan, G.G., Ramana, T.V., Bashir, A.K. and AlZubi, A.A., 2024. Artificial intelligence based zero trust security approach for consumer industry. *IEEE Transactions on Consumer Electronics*.

[25] M. Shanmugam, I. Natarajan, V. Balasubramaniam, R. D. Gomathi, and S. Shanmugam, "Smart Lights for Smart City," in *Smart Cities: Concepts, Practices, and Applications (1st ed.)*: CRC Press, 2022, pp. 223-243.

[26] A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "AP2FL: Auditable privacy-preserving federated learning framework for electronics in healthcare," *IEEE Transactions on Consumer Electronics*, 2023.

[27] F. Jamil, H. K. Kahng, S. Kim, and D.-H. Kim, "Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms," *Sensors*, vol. 21, no. 5, p. 1640, 2021.

[28] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, and S. O. Hwang, "Blockchain-based smart home networks security empowered with fused machine learning," *Sensors*, vol. 22, no. 12, p. 4522, 2022.

[29] Le Nguyen, B., Lydia, E.L., Elhoseny, M., Pustokhina, I., Pustokhin, D.A., Selim, M.M., Nguyen, G.N. and Shankar, K., 2020. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. *Computers, Materials & Continua*, *65*(1), pp.87-107.

[30] Zhou, C. and Jiang, Z., 2023. Computer network communication security encryption system based on ant colony optimization algorithm. *Procedia Computer Science*, *228*, pp.38-46.

[31] Chen, Y., Chen, H., Han, M., Liu, B., Chen, Q., Ma, Z. and Wang, Z., 2021. Miner revenue optimization algorithm based on Pareto artificial bee colony in blockchain network. *EURASIP Journal on Wireless Communications and Networking*, *2021*, pp.1-28.

[32] Ponjothi, A.R. and Parwekar, P., 2023. Bidirectional blockchainbased secure data transfer using galoeem routing protocol in wsn. *Journal of Computer Science, 19 (8), 964-976. Journal of Computer Science*, pp.964-976.

Bo Yuan male, Han nationality, native of Shouxian County, Anhui Province, is a senior engineer and doctoral candidate at the Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing. His research interests include: blockchain, information security, and computing network.

Faguo Wu, male, Han nationality, Anqing, Anhui, PhD, associate professor, research direction: anti quantum computing, artificial intelligence, blockchain, information security.