Date available online: 20-09-2024
Vol. 2, Issue 1 (January – June 2024)

SecureNet: A Convergence of ML, Blockchain and Federated Learning for IoT Protection

Abeera Malik[1*], Hafiz Muhammad Talha[1], Muhammad Zunnurain Hussain[2], Muzammil Mustafa[3], Basit Sattar[3], Jibran Ali[4], Jawad Altaf[5]

[1]The Punjab University Lahore, Pakistan
[2]Assistant Professor, Department of Computer Science Bahria University Lahore Campus Lahore, Pakistan
[3]University of Management & Technology, Lahore, Pakistan
[4]Multinet Pakistan Pvt Ltd Lahore, Pakistan
[5]National College of Ireland, Ireland

[*]Corresponding author: Abeera Malik (e-mail: abeeramalik108@gmail.com)

***Abstract*—**The Internet of Things (IoT) has become a foundational element of the digital infrastructure, extending its connectivity across various sectors and embedding intelligence in everyday devices. This article introduces SecureNet, a pioneering approach that integrates Machine Learning (ML), Blockchain, and Federated Learning (FL) to enhance IoT security. To navigate this challenging train, an innovative framework that synergizes Machine Learning (ML), Blockchain technology, and Federated Learning (FL) to fortify IoT security. SecureNet is architected to deliver a robust defense mechanism for IoT ecosystems, providing resilience against increasingly sophisticated cyber threats, and ensuring the preservation of data integrity, privacy, and unwavering system reliability. This study explores the application of advanced ML techniques NSL-KDD dataset, implementing two highly effective classifiers: Random Forest and Logistic Regression. The Random Forest classifier exhibited an exceptional accuracy of 99.85%, while the Logistic Regression model demonstrated a near-perfect accuracy of 99.03%. These compelling results highlight the efficacy of ML in identifying and mitigating activities within network traffic. SecureNet leverages ML's profound analytical capabilities for intelligent threat discernment, Blockchain's immutable ledgers for unassailable data verification, and FL's privacy-centric approach to distribute model training. These outcomes underscore the potential of ML models to enhance IoT security by accurately identifying malicious patterns and anomalies within network traffic.

Index Terms—Internet of Things (IOT), Machine Learning, Blockchain, Federated Learning, Data Integrity, Privacy, SecureNet, Network Traffic Analysis

I. INTRODUCTION

Today's digital fabrics of our ever more interconnected world depend more than ever on the Internet of Things. However, the Internet of Things (IoT) is now much more than just smart appliances and gadgets; it is a broad and extremely specialized network of functions and devices that cover every industry, enabling unprecedented levels of automation and data collection and analysis capabilities. [1] Regrettably, the increased requirement for these features indicates that more advanced security measures are required, which is why developments like IoT SecureNet are crucial. With the help of IoT SecureNet, which builds on the advantages of federated learning, blockchain, and machine learning, the IoT environment will be more resilient to various attacks and guarantee data privacy, integrity, and system dependability.

[2] From the understanding of the base principles of SecureNet, it is then necessary to ascertain the individual dynamics and intersectional benefits of Machine Learning, Blockchain, and Federated Learning where the trio are considered. One of the major benefits of Machine Learning is that the system is designed to adopt varied analytics and has adaptable abilities to realize dynamic and unpredictable assaults and also provide predictive risk intelligence [3]. This implication is particularly necessary in IoT considering the huge amount of data volume produced which makes monitoring and malware or breach detection processes humanly impossible. Consequently, ML embeds tracking systems which assess and monitor the behavior changes which flag off unusual patterns and predict potential malicious alterations [4].

Because blockchain technology is transparent and unchangeable, it adds another level of security and confidence to SecureNet. Blockchain reduces the danger of data tampering and ensures network integrity by decentralizing data management and eliminating single points of failure [5]. For Internet of Things applications like supply chain management or smart contracts, where trust and data authenticity are critical, this feature is essential. SecureNet's combination of Blockchain innovation guarantees information sent between IoT gadgets is secure, irrefutable, and impervious to unapproved adjustments. [6].

Combined learning, then again, resolves the basic

issue of information protection in Web of Things organizations. Using AI models that are prepared across a few gadgets and don't need incorporated information, [7] SecureNet can use aggregate insight. This strategy jelly touchy information security while empowering versatile and effective model preparation over broadly scattered IoT gadgets. Combined learning has permitted SecureNet to completely use AI (ML) for security purposes without compromising client protection or information [8]. These innovations cooperating to frame SecureNet implies a change in outlook in the way that IoT security is drawn nearer.

This underscores the need of cutting-edge security solutions like SecureNet [9]. As IoT continues to spread throughout many industries, from smart homes to industrial IoT, the need for cutting-edge security solutions like SecureNet is growing, signaling the beginning of a new era of IoT ecosystems that are safe, intelligent, and self-sufficient [10].

Examining case studies and actual applications of these technologies in use is advised to gain a fuller understanding of how SecureNet may be put into practice and the potential impact it holds for IoT security. Keeping up with the most recent findings and innovations in the nexus of ML, Blockchain, and Federated Learning will offer insightful perspectives on how IoT security will grow in the future [11].

The advanced age gives the premise to the Web of Things' execution. IoT might be summarized as a wide expression that portrays how devices are associated with the web by means of sensors without the requirement for human contribution.

Any contraption, including telephones, lights, PCs, espresso creators, and other ordinary things with sensors, can be associated with it. The most common way of integrating this present reality into a computerized climate brings about expanded financial open doors, diminished work costs, and different human efficiencies. Since there are many risks related to the Web of Things, state of the art innovations like IoT SecureNet

[12] — which incorporates blockchain, united learning, and AI to convey a complete IoT security arrangement — are expected to counter different complex dangers [13].

Furthermore, with the ongoing expansion of the IoT ecosystem, the number of affected areas, including infrastructure, healthcare, and production, expands as well, exacerbating the potential impact of malicious activities]. The unique and intricate structure of the IoT system consisting of millions of nodes makes it nearly impossible to fully secure the network and the data it produces. It calls for a multi-level approach to security, which could fulfil the protection of the existing IoT network from the majority of threats and guarantee the inviolability of the structure and its integrity.

II. Literature Review

The literature review SecureNet: A Convergence of ML, Blockchain, and Federated Learning for IoT Protection explores a novel strategy for protecting IoT ecosystems that centers on ML, FL, and Blockchain. The essential focal point from this exploration is that the decentralization of Blockchain guarantees straightforwardness and sealed procedures, which are basic for safeguarding information and gadget associations and proposition a strong starting point for Web of Things security. This investigates a state-of-the-art technique for safeguarding IoT organization's blockchain, ML, and FL biological systems [14]. The principal end to be drawn from this study is that the decentralized idea of Blockchain ensures straightforwardness and carefully designed techniques, which are fundamental for shielding information and associations among gadgets and give major areas of strength for a to Web of Things security. It additionally takes a gander at how significant Unified Learning is to working on the security of IoT gadgets. Its capacity to prepare AI models on decentralized information while safeguarding protection is featured by the Web of Things in situations where information security and protection are critical.

In addition, it digs into Combined Learning's basic job in expanding IoT security, featuring its ability to prepare AI models on decentralized information while keeping up with protection. This is particularly significant in Web of Things settings where information security and protection are basic [15].

The evaluation additionally explains how ML models are utilized to really recognize and balance IoT security chances. It features the challenges in integrating complex AI calculations into IoT gadgets with restricted assets and proposes a few potential fixes, for example, utilizing edge registering for constant examination and creating lightweight models. The novel part of SecureNet is the way these three innovations — ML, Blockchain, and FL — are completely incorporated to make a synergistic arrangement that reinforces IoT security by tending to its weaknesses and using its benefits [16]. This union not just addresses a significant leap forward in IoT security yet additionally lays out another line of request for AI research from now on.

At the point when Blockchain innovation is incorporated into Web of Things security structures, the decentralized idea of the insurance it offers enormously works on the trustworthiness and secrecy of information moved between IoT organizations. Blockchain diminishes potential marks of weakness by empowering programmed, secure, and direct associations between IoT gadgets without the requirement for mediators through shrewd agreements. Besides, the organization is reinforced against unapproved access by Blockchain's ability to empower protected, decentralized gadget confirmation, making it truly challenging for agitators to think twice about the framework.

[17] On the other hand, unified learning (FL) presents a change in outlook in information handling for Web of Things (IoT) security by permitting information

to remain on the gadget, safeguarding protection and bringing down the probability of concentrated information breaks decisively. With FL, ML models might be mutually prepared on a few gadgets; just model changes are shipped off a focal server for solidification. [18] Guaranteeing that private or delicate information doesn't get away from the gadget is one of the fundamental security worries in IoT environments that this procedure addresses. Besides, by gaining from a wide assortment of information sources, FL can work on the viability and productivity of ML models utilized for IoT security, bringing about more dependable location and relief strategies against changing security dangers. When joined, Blockchain and FL give a powerful blend to protecting IoT gadgets, ensuring client security and information security. Moreover, FL can improve the viability and productivity of AI models utilized for IoT security by consolidating information from a great many information sources.

A. Contributions

From the article (Machine Learning in IoT Security: Current Solutions and Future Challenges) by Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain, We contribute specifically enhance the understanding and application of machine learning (ML) and Blockchain and Federated Learning approaches within the domain of IoT security. The main contributions of this paper can be summarized as follows:

1) We proposed Algorithm for explanation on how Blockchain will be helpful for IoT Protection.
2) We proposed a solution in-depth review to Implement explanation of how Federated Learning (FL) used for IoT Protection.
3) Applying 2 ML Models for IoT Protection on dataset.

III.Related Work

Yunlong Lu et al. (2019) made a fundamental commitment with their work on (Blockchain and United Learning for Protection saved Information Partaking in Modern IoT), distributed in 2019. This article presents a pivotal system that consistently mixes the strength of blockchain with the security saving nature of combined learning. By architecting a solid information sharing improvement grounded in permissioned blockchain improvement, Lu and his get-together location the sincere difficulties of shielding information security and constancy inside the IIoT circle. [19] The article is seen by its reasonable evaluation, showing the game plan's substantial quality and abundancy through genuine world dataset assessments. Their appraisal not just plans for additional assessment concerning secure information sharing structures inside IIoT yet moreover addresses the limit of blockchain and joined learning in chipping away at the possibility of association in arising applications [20].

Likewise, Zhang et al's. (2019) examination concerning combined learning applications in IoT, with an emphasis on brilliant home conditions, is a brilliant illustration of development. This study presents a one of a kind engineering that joins the strength of blockchain with the security safeguarding characteristics of united learning. Lu and his associates have organized a permissioned blockchain-based safe information-sharing planning to address the immense difficulties of information security and uprightness security in the IoT region. The article is conspicuous for its sensible examination, which shows the plan's help and application through dataset evaluation utilizing genuine world datasets [21].

Sabita Maharjan et al. have made a wonderful commitment by exploring the mix of blockchain innovation and combined figuring out how to protect security issues. Their careful examination looks at the numerous strategies and learning ideal models utilized in the combination of these two advancements, catching the best in class draws near. Crafted by Maharjan et al. is urgent in accentuating the range of purposes and upgraded execution that come from consolidating blockchain innovation with unified learning. Their paper is a significant asset for scientists and professionals who need to carry out protected and successful IoT frameworks since it presents a scientific perspective on the turns of events and conceivable execution increments.

[22] Xiaohong Huang and Yueyue Dai's work is indispensable for the movement of the conversation around brought together learning for IoT contraptions enabled by blockchain. They give a flexible and safe designing that settle the chief issues of data security in Snare of Things networks through their comprehensive assessment and structure plan. Their strategy incredibly builds the viability of information utilization among scattered IoT gadgets while at the same time reinforcing security shields. Huang and Dai's work offers viable experiences into the organization of blockchain and united learning advances in true Web of Things applications by stressing the commonsense execution and surveying the framework's presentation across numerous circumstances.

By and large, these academic works enlighten the way towards bridling the consolidated force of blockchain and united learning for getting and streamlining information sharing and handling in the IIoT space. Every commitment, with its one of a kind concentration and technique, improves the more extensive story of progressing IoT security and productivity through mechanical development. The essence of these examinations lies in their bound together position on the need of complex, layered security systems to safeguard the prospering organizations of IoT gadgets. The coming of combined learning and blockchain innovation presents a clever worldview where security doesn't exclusively depend on customary encryption or disconnected protection components. All things considered, it advocates for a conveyed at this point strong way to

deal with shielding information, utilizing the qualities of blockchain's changelessness and combined learning's decentralized nature.

IV. Blockchain for IoT

Blockchain lays out a decentralized structure that improves Web of Things security by definition, making it an essential device chasing a protected IoT climate. Blockchain innovation essentially lessens the assault surface of concentrated frameworks by scattering information all through an organization of hubs. Concentrates by Lu et al. (2019) exhibit the flexibility of a decentralized system in frustrating breaks and unapproved access inside the IIoT worldview. [23] These examinations affirm that decentralization ensures that the general trustworthiness of the IoT network is safeguarded even in the case of a compromised hub.

Refer to Figure 1 Blockchain Innovation Application in IoT systems by empowering shared correspondence among IoT gadgets, blockchain innovation could further develop information integrity in IoT biological systems by strengthening information trades against outside dangers. Relevant investigations given by Lu et al. (2019) show how blockchain advancement has been successfully applied in a collection of IoT security circumstances, showing its ability to safeguard data uprightness and keep a reliable record of all trades and data exchanges inside an IoT association [24].

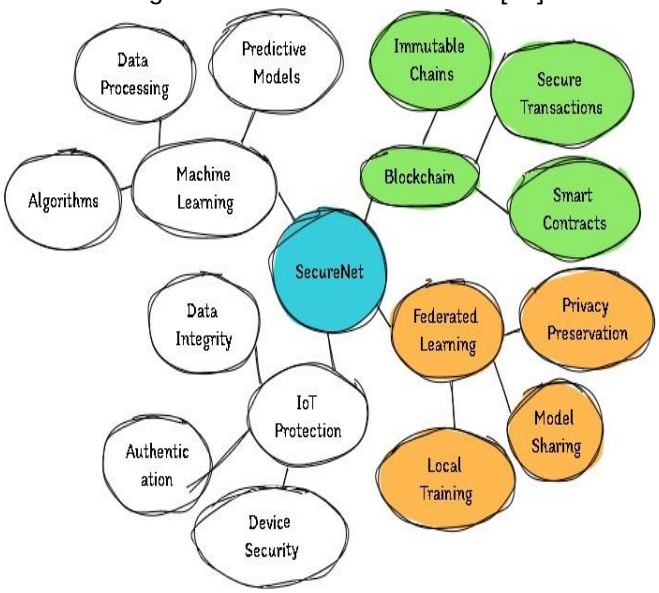

FIGURE 1. Components Related to Blockchain, FL, and ML concepts of SecureNet.

Adding IoT gadgets to a blockchain is a fast and simple method for expanding their security. The arrangement use the powerful properties of blockchain, explicitly its unchanging nature and decentralization, to safeguard the tremendous and different information climate created by Web of Things gadgets. Transparency, integrity, and tamper-proof security are guaranteed for the data transferred between devices using this mechanism [25].

The Internet of Things devices begin gathering and sending data after registering. This information could be anything from human interactions in smart homes to environmental readings in applications for smart agriculture. In addition, the information is divided into safe chunks prior to being kept on the blockchain. This method assures the data's confidentiality and integrity while also keeping it impervious to tampering. After the information is recorded on the blockchain, it is nearly impossible to change it later on without the approval of most network users. This protects the data from unwanted changes and online attacks.

[26] Blockchain technology offers a safe and effective framework for handling the data from Internet of Things devices through these processes. Because blockchain is decentralized, it removes central points of failure, making the Internet of Things ecosystem more resilient to attacks and guaranteeing that operations will continue even in the worst of circumstances. This IoT device and blockchain technology integration represents a major step forward for digital security, providing a strong answer to the intricate problems associated with safeguarding the ever-growing universe of linked devices. Algorithm 1, (Enhanced Verification for Secure IoT Blockchain Transactions) is essential to the security of IoT transactions utilizing blockchain technology.

Algorithm 1 Enhanced Verification for Secure IoT Blockchain Transactions

procedure AdvVerTxIoT(M, T, D)
  for each $m \in M$ **do**
    if ¬VerifyMiner(m) **then**
      return $\perp$ ▷ Miner verification failed
    end if
  end for
  if ¬AuthDevice($T.DID$) **then**
    return $\perp$ ▷ Device authentication failed
  end if
  if ExceedsRateLimit($T.DID$) **then**
    return $\perp$ ▷ Transaction rate limit exceeded
  end if
  if VerifySig(T) = 1 $\wedge$ ¬IsDup(T) **then**
    return 1 ▷ Approve transaction for blockchain
  else
    return 0 ▷ Reject transaction
  end if
end procedure

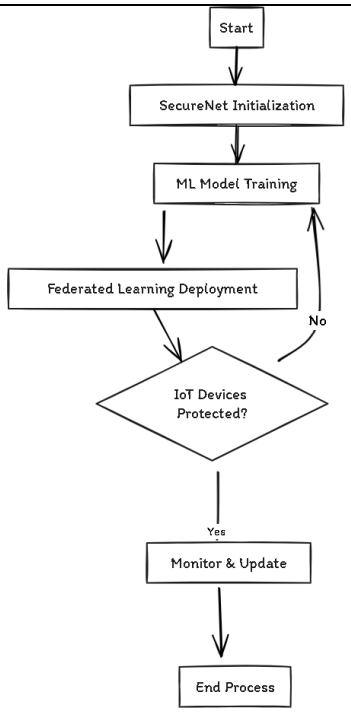

FIGURE 2. Detail Flowchart of SecureNet.

The strategy begins by guaranteeing that every excavator (*M*) is approved through the VERIFYMINER capability, moderating the gamble of pernicious elements taking part in the blockchain. This step is critical for keeping up with the trustworthiness of the blockchain, as it keeps unapproved excavators from affixing misleading exchanges. The calculation further improves security by confirming IoT gadgets (*D*) engaged with the exchange (*T*). It really takes a look at the gadget's extraordinary identifier (*T .DID*) against a library of approved gadgets, guaranteeing that the main checked gadgets can contribute information to the blockchain. This confirmation step is crucial in an IoT setting, where gadgets are omnipresent and possibly more powerless to think twice about.

Moreover, the methodology utilizes the EXCEEDSRATE- LIMIT capability to add a method for halting exchange flooding by diminishing the potential for a solitary gadget to overpower the organization with an inordinate number of exchanges, this restricts the risk of refusal of administration (DoS) assaults. It does this by observing on the off chance that a gadget finishes more exchanges in a predefined measure of time. Ultimately, it affirms the mark of the exchange (VERIFYSIG(*T*)) and searches for duplication (ISDUP(*T*)) to ensure its credibility and uniqueness. By using the decentralized and permanent nature of blockchain innovation, this layered security technique helps defend the Web of Things Above Algorithm explains verification approach leverages the immutable and decentralized nature of blockchain technology to enhance IoT security. By ensuring that only verified miners participate, authenticating devices, limiting transaction rates, and verifying transaction integrity, the algorithm provides a robust framework for securing IoT transactions against various attacks, thereby protecting the IoT ecosystem biological system against different assaults, thus ensuring the trustworthiness and steadfastness of IoT information ex- changes on the blockchain.

V. Federated Learning for IOT Protection

Figure 2 represents Federated learning (FL) is a progressive AI approach intended to prepare calculations across numerous decentralized gadgets or servers holding nearby information tests, without trading them [12]. This creative technique is especially powerful in situations where information protection, security, and access privileges present critical worries. All things being equal of expecting information to be transferred to a solitary focal server for examination, FL takes into account the actual model to travel, gaining from information where it is created and living.

[27] Federated learning (FL) progresses are turning out to be progressively critical for safeguarding Web of Things (IoT) environments from rising dangers. By exploiting the distributed idea of IoT gadgets to cooperatively construct a common expectation model while saving the restriction of all preparing information, this original methodology essentially improves information protection and security. This procedure offers a versatile, decentralized learning methodology that adjusts to the different handling and stockpiling limits of Web of Things gadgets, from actuators in modern control frameworks to sensors in savvy homes, by exploiting the innate assortment of these gadgets.

[28] This strategy's dynamic, complex combined learning structure, which runs in two separate stages — limited preparing and model conglomeration — is its major part. Each IoT gadget first forms a nearby model on its own information, utilizing its own insight and perceptions to learn without unveiling private data. These nearby models catch the unmistakable elements and conceivable security gambles with specific to the setting of every gadget. The updates from these nearby models are then specifically joined utilizing a security-protecting convention to make a protected, collected model. By utilizing refined cryptographic strategies like safe multi-party figuring and homomorphic encryption, this convention guarantees that singular commitments are kept hidden while using aggregate knowledge.

[29] Furthermore, this method presents an adaptive learning rate optimization solution designed for IoT environments' extremely changeable network conditions. Through the dynamic adjustment of learning rates in response to real-time network performance data, the technique balances computational efficiency and model convergence speed throughout the federation. By doing this, it is made possible for devices with constrained resources to take part in federated learning without experiencing bottlenecks. With the help of this creative approach, IoT safety becomes intrinsically proactive rather than merely reactive since the federated model is always changing to anticipate and neutralize new threats, guaranteeing a safe and robust IoT environment.

In the academic exploration of IoT protection, understanding the interaction between components within a system is essential. In Fig. 3, the illustration outlines a security-focused network architecture employing Federated Learning and Blockchain technologies. The diagram demonstrates how IoT devices transmit data through encrypted channels to Federated Learning nodes. These nodes function collaboratively, yet independently, analyzing data without centralizing it [30]. Data is then safely moved to a Blockchain node, which offers a further degree of protection via decentralized ledger systems and permits frequent upgrades and model deployment to protect the network. An alternative method is shown in Figure 4, where data is delivered straight to a central server from a variety of IoT devices located in different client firms. In this case, the server is essential for gathering data, developing machine learning models, and doing predictive analysis. This model's centralization of data highlights the trade-offs between centralized and decentralized data processing systems and offers an alternative viewpoint on security and efficiency [31].

Both diagrams serve as visual representations of two distinct methodologies in IoT security management. Fig. 3 emphasizes the importance of preserving data privacy at each node, leveraging the strengths of Blockchain technology. In contrast, Fig. 4 focuses on the central server's capacity to integrate diverse data sources for comprehensive analysis. The juxtaposition of these two figures in an academic discourse facilitates a deeper understanding of the potential and versatility of IoT protection strategies.

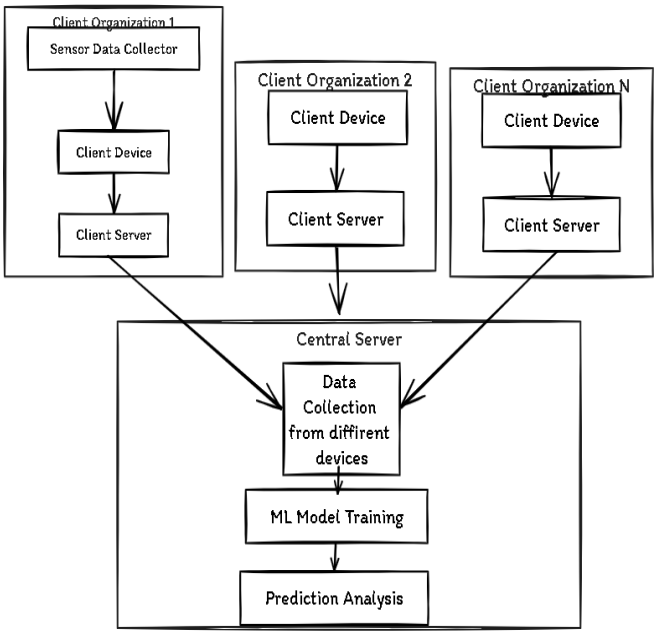

FIGURE 3. Distributed Data Training Work process across numerous Organizations.

Refer to Fig. 3 Blockchain technology, Federated Learning, and Machine Learning (ML) are pivotal in fortifying the security framework of Internet of Things (IoT) systems. Blockchain acts as a decentralized ledger that records transactions across a network of devices, ensuring data integrity and traceability.

Its immutable nature prevents data tampering, making it a cornerstone of trustworthy communications in IoT ecosystems.

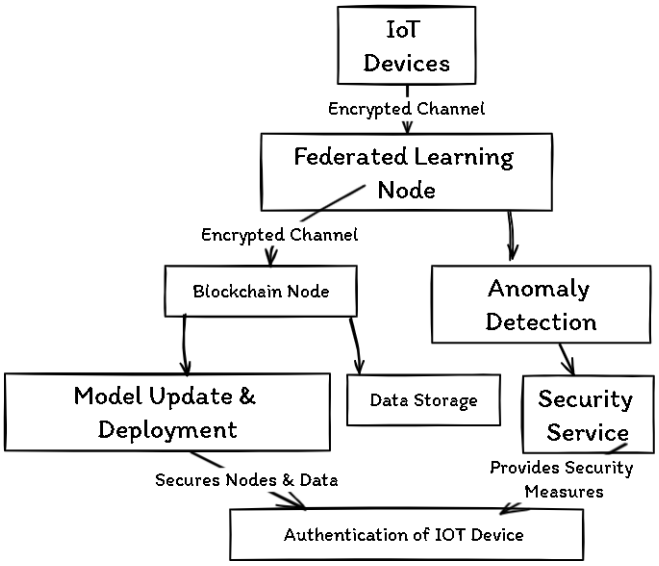

FIGURE 4. Decentralized Federated Learning ML Model Flowchart

Refer to figure 4 Combined Learning and ML, when applied to IoT, empower gadgets to gain and settle on choices from information while keeping up with security. United Learning permits various IoT gadgets to add to a common ML model without uncovering their information, saving client security. This model is consistently further developed through ML calculations that foresee and adjust to potential security dangers, upgrading the general strength of the IoT organization. Together, these technologies provide a robust defense mechanism, mitigating risks and protecting against unauthorized access in connected device environments.

VI. Machine Learning Models

[32] IoT networks are therefore a prime target for assaults because of the numerous vulnerabilities that this integration also exposes. Machine Learning (ML) presents a ray of hope for strengthening IoT ecosystem defenses against such threats because of its capacity to learn from data and make intelligent judgments. Using the complex "NSL-KDD" dataset as a fundamental tool, this introduction examines the critical role that machine learning (ML) plays in improving Internet of Things (IoT) protection, namely through network and traffic attack detection.

[33] Imagine your IoT devices, like smart fridges, security cameras, or fitness trackers, as a bustling city full of people and activities. Now, just as a city might face issues with unwanted visitors causing trouble, your

IoT devices can encounter cyberattacks trying to sneak in and cause harm.

[34] Machine Learning (ML) acts like the city's most advanced security system. It learns by watching and remembering the patterns of daily life in the city - how people normally come and go, the usual traffic flow, and when the lights turn on and off. So, when something out of the ordinary happens, like a cyberattack trying to disrupt normal activities, ML can spot this unusual pattern because it doesn't match the daily routine it has learned. Using the NSL-KDD dataset, which is like a detailed guidebook containing records of both the city's regular activities (normal samples) and the time's troublemakers (attacks) tried to cause problems, ML models train themselves. They read through this guidebook over and over, learning to recognize what's normal and what's not. Once trained, these ML models can quickly identify when an unwanted visitor is trying to enter the IoT city, even if they're trying to blend in or sneak in unnoticed.

[35] In this manner, our machine learning models can learn from and adjust to new techniques used by attackers, ensuring the security of our Internet of Things devices.

[36] ML, like a highly intelligent security system that constantly learns and adapts to keep the city secure, essentially helps protect IoT devices by figuring out what's normal and alerting us to anything questionable. This dataset is extremely important when discussing IoT security because a variety of attack types frequently target networks where IoT devices are used. The NSL-KDD dataset can be used to train machine learning models like Random Forest and Logistic Regression, which can be used to create complex systems that can recognize and react to possible threats. These models are able to pick up on the minute differences between malicious and benign.

The use of machine learning (ML) in this field goes beyond simple detection and involves ongoing security protocol improvement to keep up with evolving cyberthreats. Because machine learning is dynamic, models may adapt to new attack techniques, making Internet of Things networks adaptable to a constantly shifting threat landscape.

TABLE 1. Mean and Median of Duration by Attack Type

Attack Type	Mean	Median
back	0.480376	0.429223
buffer_overflow	0.559406	0.705779
guess_password	0.344615	0.539310
neptune	0.197373	0.327421

The table titled: Mean and Median of Duration by Attack Type, presents data from the NSL-KDD dataset. This table is instrumental in understanding the typical behavior patterns of different attack types in terms of duration, which can be a significant feature for models to detect attacks. In the context of the table, (duration) likely refers to the length of time for which each type of attack lasts or the time taken for the attack to be completed.

In the table, two key descriptive statistics are provided for each attack type: the mean and the median duration. The mean duration offers an average value which suggests the general tendency or the central tendency of the duration of each attack, while the median provides a midpoint value, indicating that half of the attacks last longer than the median value and half are shorter. For example, back attacks have a mean duration of 0.480376 and a median of 0.429223, which are relatively low, indicating that such attacks are of short duration. Buffer overflow attacks present a higher mean and median duration of 0.559406 and 0.705779 respectively, suggesting that these attacks tend to last longer than back attacks. It is interesting to note that for buffer overflow, the median is higher than the mean, indicating a skewed distribution where a significant number of longer-lasting incidents push the median up.

A. Type of Attacks in Dataset

The bar chart titled: Distribution of Attack Types in the Dataset, illustrates the frequency of various categories of network interactions – labeled as: normal, and several types of attacks – within a dataset presumably used for network intrusion detection. The normal category, representing benign traffic, dominates the dataset with the highest count, suggesting that the majority of the network activity is legitimate. This prevalence reflects typical network conditions where ordinary activities are more common than malicious ones. Following normal, the neptune category, which likely represents a type of Denial of Service (DoS) attack, shows a significant occurrence, indicating that such attacks are also commonly represented in the dataset.

This distribution has important implications for IoT security. IoT devices are vulnerable to several types of assaults since they are frequently always connected to networks. When applied to such datasets, machine learning models like Random Forest and Logistic Regression need to be skilled at identifying the minute patterns that distinguish apart normal interactions from attack vectors, regardless of how common the attack is. As a result, the distribution of attacks in the dataset offers important insight into the kinds of risks that an Internet of Things system might face, guaranteeing that the defenses put in place are comprehensive and successful against the real threats to the network.

ML models as highly intuitive detectives in the world of IoT security. They're trained using vast amounts of data from past events, learning to distinguish between normal device behavior and signs of cyber threats, much like a detective learns to spot clues that something's wrong. As cyber attackers evolve their tactics, these ML detectives aren't fooled easily; they continuously learn from new data, adapting their understanding to predict and prevent future attacks.

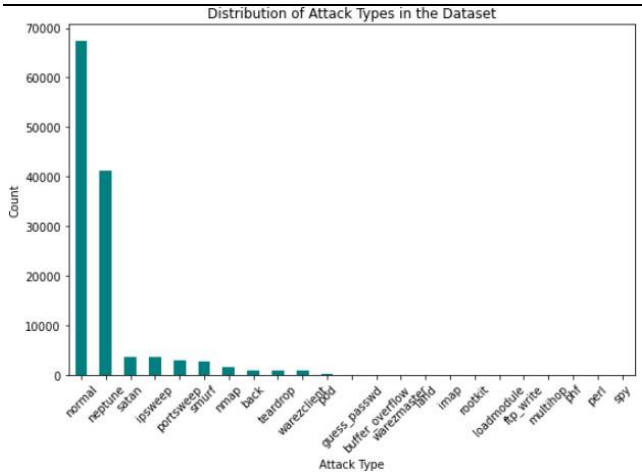

FIGURE 5. Different Types of Attacks.

B. ML Models Metric Performance Table

Table II presents represent performance metrics of two different machine learning classification models applied within the context of IoT (Internet of Things) protection. The first table showcases the performance of a Logistic Regression model. This model has achieved a high accuracy of 90.03%, suggesting that it correctly predicts whether an IoT device is at risk or not in 90.03% of the cases. The precision metrics, which indicate the number of true positive predictions out of all positive predictions, are 79% for Macro Average Precision and 99% for Weighted Average Precision. The F1-score, which balances precision and recall, is 77% for the Macro Average and 99% for the Weighted Average. Although the weighted measures are high, indicating good performance on possibly imbalanced classes weighted by their size, the macro averages suggest that there may be a variance in performance across different classes.

TABLE 2 Comparison of Machine Learning Model Performance

Model	Accuracy (%)	Precision (%)	F1 Score (%)
Logistic Regression	99.03	79.0	77.0
Random Forest	99.85	86.0	80.0

The performance of a Random Forest classifier, another machine learning model, in an IoT security context. This model has an even higher accuracy of 98.85%, implying it is very effective at classifying the security status of IoT devices. The F1-scores are 80% for the Macro Average and 100% for the Weighted Average, while the precision scores are 86% and 100% respectively. The perfect Weighted Average Precision and F1-score suggest that when the model predicts an IoT device is secure or not, it is extremely reliable, particularly in classes with more instances. The Large-scale Midpoints are somewhat lower than the weighted ones, demonstrating some fluctuation in execution among the different classes, yet they are still sensibly high, mirroring a decent presentation by and large. These models can be essential in frameworks intended to recognize vulnerabilities or expected breaks in IoT gadgets, a critical viewpoint of keeping up with security in interconnected gadgets.

C. Measurement of Dataset

In the Domain of IoT security, artificial intelligence (ML) models emerge as cautious guardians, utilizing genuine encounters like the association among mean and vacillation in network traffic to safeguard devices. These models, ready on datasets determining normal and bizarre IoT traffic plans, are capable of perceiving unpretentious hints of advanced risks.

At the point when the fluctuation in network traffic digresses fundamentally based on what's generally anticipated in view of the mean — similar as seeing an unexpected, unique change in the way of behaving of a group — ML models can hail this as expected pernicious movement. This limit is compared to a painstakingly pre-arranged examiner figuring out signs to foil a plot before it spreads out. By understanding the conventional check spread out by estimations, for instance, the mean and center of association features, ML models can rapidly recognize peculiarities. This early revelation is essential, as it considers fast movement to alleviate risks, holding expected attacks back from compromising the IoT climate.

[37] The dataset's creation, as demonstrated by the bar graph, likewise takes into consideration the adjustment of prescient models by giving a rich setting of ordinary versus assault situations. In the domain of IoT, where gadgets range from family contraptions to modern sensors, a model prepared on such a dataset can turn out to be profoundly capable at hailing deviations from the standard, in this way shielding against misleading up-sides which could somehow prompt superfluous cautions or personal time. Furthermore, the presence of various assault types, including the unmistakable Neptune, DoS class, guarantees that models are presented to an assortment of assault marks.

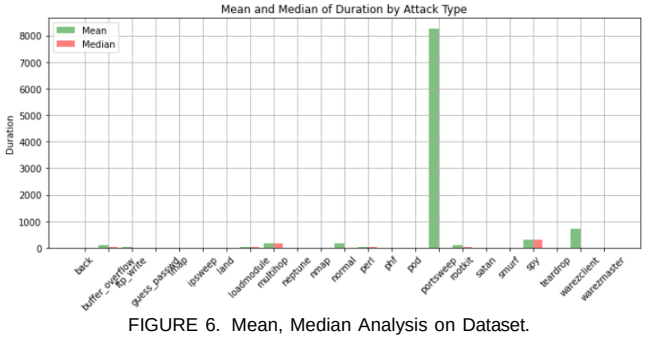

FIGURE 6. Mean, Median Analysis on Dataset.

[38] The importance of PC-based knowledge (ML) in safeguarding our coordinated contraptions basically makes as we travel through the advanced age. As well as guaranteeing the security of the Snare of Things regular system, it correspondingly moves innovative trust, which is key for the new development and propelling breaker of IoT contraptions into our standard ordinary existences. This mix of prosperity and progression makes the way for when IoT can sort out its most prominent breaking point.

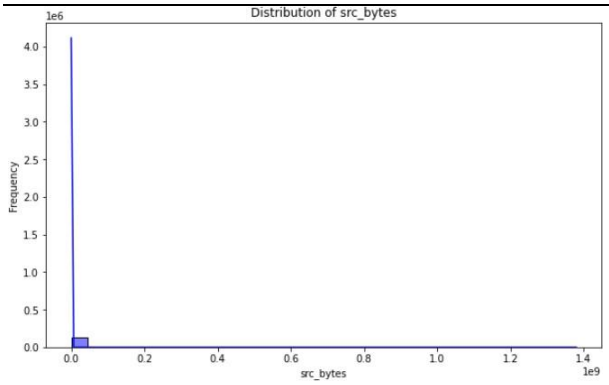

FIGURE 7. Graph of predictions on Dataset.

Figure 6 illustrates the mean and median duration of various types of cyber-attacks, potentially against IoT devices. A significant disparity between the mean and median values for one particular attack type suggests that there are outliers or anomalous events that drastically extend the duration of such attacks, skewing the average. In contrast, most other attack types have similar mean and median durations, indicating a more uniform distribution of attack durations. [39] This information can be critical in IoT protection as it helps to identify and prioritize the defense against the types of attacks that tend to last longer, as prolonged attacks may provide more opportunities for exploitation and can indicate more sophisticated threats.

Figure 7 shows the distribution of src bytes, which likely represents the volume of data sent from the source in an IoT network environment. Understanding this distribution is crucial for IoT protection because it can help in setting thresh- olds for anomaly detection systems. If an IoT device suddenly starts to send data in volumes that are inconsistent with this distribution, it could be flagged for further investigation. This kind of analysis assists in the early detection of security incidents, protecting IoT networks from potential breaches or disruptions.

[40] In the context of IoT protection, the scatter plot displaying the relationship between mean and variance of network traffic features is instrumental. The pattern observed—where variance initially increases with the mean and then stabilizes—can indicate normal traffic patterns and their deviations, which are crucial for detecting anomalies. When a device behaves unusually, resulting in a significant increase in variance not consistent with the mean, it could signal a cybersecurity threat like a DDoS attack or system compromise [41].

VII. Future Work

Future research should focus on optimizing Blockchain technology for IoT applications, ensuring scalability and reduced latency in transaction verification processes. Further Machine Learning models that can run efficiently on IoT devices will also be critical. Furthermore, advancing Combined Learning techniques to focus on model accuracy and productivity in decentralized environments would bolster SecureNet's sustainability. Examining the integration of SecureNet in genuine Internet of Things applications across several domains will yield valuable insights into its practical implementation and opportunities for enhancement.

VIII. Limitations

SecureNet offers an IoT protection arrangement that shows guarantee, however, it isn't without limits. Blockchain's flexibility in dealing with various exchanges without encountering huge inaction is as yet being tried. In addition, to guarantee viability, IoT gadgets should be improved to satisfy the registering needs of AI calculations on resources. Regardless of whether Joined Learning shows guarantee for safeguarding the climate, more examination is expected to increment model exactness while using decentralized information sources.

The paper" SecureNet: A Combination of ML, Blockchain, and United Learning for IoT Insurance" features a few promising headways yet additionally uncovers a few basic restrictions. One significant shortcoming is the adaptability and inertness of Blockchain innovation when applied to IoT biological systems. The paper recommends that Blockchain's capacity to deal with enormous scope IoT exchanges productively is as yet dubious, which could prevent true execution. Furthermore, while the mix of Combined Learning (FL) is an inventive step for security insurance, the review recognizes that more examination is expected to further develop model exactness while utilizing decentralized information sources. This constraint could affect the viability of the proposed structure in assorted and dynamic IoT conditions.

One more critical shortcoming lies in the computational requests of executing AI calculations on IoT gadgets. Numerous IoT gadgets have restricted handling power, which might battle to meet the figuring necessities of cutting-edge calculations, raising worries about the possibility of SecureNet across different IoT frameworks. Moreover, while SecureNet shows guarantee in coordinating ML, Blockchain, and FL, it doesn't completely investigate possible weaknesses, for example, those presented by antagonistic assaults or how these advancements will deal with developing dangers in the IoT space. These holes highlight the requirement for additional examination to upgrade and get the framework for far-reaching use

IX. Conclusion

SecureNet controls the joined properties of ML, Blockchain, and FL, tending to a urgent move toward bracing IoT security. This bound together methodology tends to the continuous security issues and establishes the groundwork for hearty IoT organic frameworks that are ready for continually developing computerized

dangers. As IoT keeps on spreading all through numerous businesses, it is basic to convey powerful security conventions like as SecureNet, proclaiming another period of shrewd, secure, and independent IoT tasks.

SecureNet gives a shrewd viewpoint on IoT protection by embracing the conversion of these innovations, guaranteeing a reliable and secure computerized future. The exploration of SecureNet's implementation and the potential impact on IoT security opens new avenues for research and practical applications, promising a more secure IoT landscape.

References

[1] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, "Ml-ddos: A blockchain-based multilevel ddos mitigation mechanism for iot environments," *IEEE Transactions on Engineering Management*, 2022.

[2] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale internet of things data storage and protection," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 762–771, 2018.

[3] M. U. Nasir, O. K. Khalil, K. Ateeq, A. Almogadwy, B. Saleem, M. Khan, and K. M. Adnan, "Cervical cancer prediction empowered with federated machine learning." *Computers, Materials & Continua*, vol. 79, no. 1, 2024.

[4] N. Naz, S. Abbas, M. Khan, Z. Hasan, M. Bukhari, and T. Ghazal, "Optimizing semantic error detection through weighted federated machine learning: A comprehensive approach," *International Journal of Advanced and Applied Sciences*, vol. 11, pp. 150–160, 2024.

[5] M. U. Nasir, O. K. Khalil, K. Ateeq, B. S. A. Almogadwy, M. A. Khan, M. H. Azam, and K. M. Adnan, "Federated machine learning based fetal health prediction empowered with bio-signal cardiotocography." *Computers, Materials & Continua*, vol. 78, no. 3, 2024.

[6] S. Otoum, I. Al Ridhawi, and H. Mouftah, "Securing critical iot infras- tructures with blockchain-supported federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2592–2601, 2021.

[7] R. N. Asif, A. Ditta, H. Alquhayz, S. Abbas, M. A. Khan, T. M. Ghazal, and S.-W. Lee, "Detecting electrocardiogram arrhythmia empowered with weighted federated learning," *IEEE Access*, 2023.

[8] S. Abbas, G. F. Issa, A. Fatima, T. Abbas, T. M. Ghazal, M. Ahmad, C. Y. Yeun, and M. A. Khan, "Fused weighted federated deep extreme machine learning based on intelligent lung cancer disease prediction model for healthcare 5.0," *International Journal of Intelligent Systems*, vol. 2023, no. 1, p. 2599161, 2023.

[9] A. Ali, M. A. Khan, and H. Choi, "Hydrogen storage prediction in dibenzyltoluene as liquid organic hydrogen carrier empowered with weighted federated machine learning," *Mathematics*, vol. 10, no. 20, p. 3846, 2022.

[10] J. Pang, Y. Huang, Z. Xie, Q. Han, and Z. Cai, "Realizing the heterogeneity: A self-organized federated learning framework for iot," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3088–3098, 2020.

[11] M. U. Nasir, M. Zubair, T. M. Ghazal, M. F. Khan, M. Ahmad, A.-u. Rahman, H. A. Hamadi, M. A. Khan, and W. Mansoor, "Kidney cancer prediction empowered with blockchain security using transfer learning," *Sensors*, vol. 22, no. 19, p. 7483, 2022.

[12] M. U. Nasir, S. Khan, S. Mehmood, M. A. Khan, M. Zubair, and S. O. Hwang, "Network meddling detection using machine learning empowered with blockchain technology," *Sensors*, vol. 22, no. 18, p. 6755, 2022.

[13] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049–4058, 2021.

[14] M. U. Nasir, S. Khan, S. Mehmood, M. A. Khan, A.-u. Rahman, and S. O. Hwang, "Iomt-based osteosarcoma cancer detection in histopathol- ogy images using transfer learning empowered with blockchain, fog computing, and edge computing," *Sensors*, vol. 22, no. 14, p. 5444, 2022.

[15] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach," *Ieee Access*, vol. 8, pp. 205 071–205 087, 2020.

[16] 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.

[17] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020.

[18] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser, and A. Ali, "A machine learning approach for blockchain-based smart home networks security," *IEEE Network*, vol. 35, no. 3, pp. 223–229, 2020.

[19] H. Tian, X. Ge, J. Wang, C. Li, and H. Pan, "Research on distributed blockchain-based privacy-preserving and data security framework in iot," *IET Communications*, vol. 14, no. 13, pp. 2038–2047, 2020.

[20] J. Lin, W. Long, A. Zhang, and Y. Chai, "Blockchain and IoT-based architecture design for intellectual property protection," *International Journal of Crowd Science*, vol. 4, no. 3, pp. 283–293, 2020.

[21] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.

[22] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, and F. Wortmann, "Blockchain for the iot: privacy-preserving protection of sensor data," *Journal of the Association for Information Systems*, vol. 20, no. 9, pp. 1274–1309, 2019.

[23] W.-J. Tsaur, J.-C. Chang, and C.-L. Chen, "A highly secure iot firmware update mechanism using blockchain," *Sensors*, vol. 22, no. 2, p. 530, 2022.

[24] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial iot," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5926–5937, 2020.

[25] K. Yu, L. Tan, C. Yang, K.-K. R. Choo, A. K. Bashir, J. J. Rodrigues, and T. Sato, "A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings," *IEEE Internet of*

Things Journal, vol. 9, no. 11, pp. 8154–8167, 2021.

[26] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, "Blockchain-based secure time protection scheme in iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671–4679, 2018.

[27] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of things intrusion detection: Centralized, on-device, or federated learning?" *IEEE Network*, vol. 34, no. 6, pp. 310–317, 2020.

[28] Z. Wei, Q. Pei, N. Zhang, X. Liu, C. Wu, and A. Taherkordi, "Lightweight federated learning for large-scale iot devices with privacy guarantee," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3179– 3191, 2023.

[29] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, and S. Yu, "Security and privacy-enhanced federated learning for anomaly detection in iot infrastructures," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3492–3500, 2022.

[30] X. Ma, Q. Jiang, M. Shojafar, M. Alazab, S. Kumar, and S. Kumari, "Disbezant: secure and robust federated learning against byzantine attack in iot enabled mts," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2492–2502, 2022.

[31] Y. Xu, Z. Lu, K. Gai, Q. Duan, J. Lin, J. Wu, and K.-K. R. Choo, "Besifl: Blockchain-empowered secure and incentive federated learning paradigm in iot," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6561–6573, 2021.

[32] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," *IEEE Access*, vol. 8, pp. 114 066– 114 077, 2020.

[33] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent iot applications: A cloud-edge based framework," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 35–44, 2020.

[34] S. Chesney, K. Roy, and S. Khorsandroo, "Machine learning algorithms for preventing iot cybersecurity attacks," in *Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 3*. Springer, 2021, pp. 679–686.

[35] 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.

[36] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero, and L. A. Trejo, "Toward the protection of iot networks: Intro- ducing the latam-ddos-iot dataset," *IEEE Access*, vol. 10, pp. 106 909– 106 920, 2022.

[37] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in iot using machine learning and blockchain: Threats and countermeasures," *ACM computing surveys (csur)*, vol. 53, no. 6, pp. 1–37, 2020.

[38] S. Atbib, C. Saadi, and H. Chaoui, "Design of a distributed intrusion detection system for streaming data in iot environments," in *2023 9th International Conference on Optimization and Applications (ICOA)*. IEEE, 2023, pp. 1–6.

[39] N. Adhikari and M. Ramkumar, "Iot and blockchain integration: applications, opportunities, and challenges," *Network*, vol. 3, no. 1, pp. 115–141, 2023.

[40] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecurity: A review," *IEEE Access*, vol. 10, pp. 19 572–19 585, 2022.

[41] N. Wang, J. Fu, S. Zhang, Z. Zhang, J. Qiao, J. Liu, and B. K. Bhargava, "Secure and distributed iot data storage in clouds based on secret sharing and collaborative blockchain," *IEEE/ACM Transactions on Networking*, 2022.

XI- SYSTEMATIC TABLE REVIEW

ID	Article Citation	Date	Contributions	Limitations	Article type	Author(s)	Topic Type	Topic Area
1	Nasir et al. Cervical Cancer Prediction with Federated ML	2024	Privacy-preserving cancer prediction. Evaluation	Limited to cervical cancer. evaluation methods	Research Paper	Nasir, Khalil, Ateeq, et al	Federated Learning	Healthcare
2	Naz et al. Semantic Error Detection with Federated ML	2024	Improved semantic error detection.	Non-IID data challenges.	Research Paper	Naz, Abbas, Khan, et al.	Federated Learning	Semantic Detection
3	Nasir et al. Fetal Health Prediction with Federated ML	2024	Enhanced privacy in fetal health prediction.	in real-time.	Research Paper	Nasir, Khalil, Ateeq, et al.	Federated Learning	Semantic Detection
4	Asif et al. ECG Arrhythmia Detection with Federated ML	2023	Research trends	Communication overhead	Research Paper	Asif, Ditta, Alquhayz, et al.	Federated Learning	Healthcare
5	Abbas et al. Lung Cancer Detection with Federated Deep Learning	2023	Hybrid federated learning model for lung cancer.	Limited scability	Research Paper	Abbas, Issa, Fatima, et al.	Federated Learning	Healthcare
6	Ali et al. Hydrogen Storage with Federated ML	2022	Federated ML for energy systems.	Limited scalability.	Research Paper	Ali, Khan, Choi	Federated Learning	Healthcare
7	Nasir et al. Kidney Cancer Prediction with Blockchain	2022	Blockchain-enhanced privacy for kidney cancer.	Latency and infrastructure needs.	Research Paper	Nasir, Zubair, Ghazal, et al.	Federated Learning	Healthcare
8	Nasir et al. Network Meddling Detection with Blockchain	2022	Blockchain-secured ML for network security.	Blockchain scalability	Research Paper	Nasir, Khan, Mehmood, et al.	Blockchain, ML	Healthcare
9	Nasir et al. Osteosarcoma Detection with Blockchain and IoMT	2022	IoMT-powered cancer detection with blockchain.	High power and latency	Research Paper	Nasir, Khan, Mehmood, et al.	Blockchain, ML	Healthcare
10	Farooq et al. Smart Home Security with Blockchain	2022	Improved security for smart homes with ML and blockchain.	Privacy and data integrity concerns.	Research Paper	Farooq, Khan, Rehman, et al.	Blockchain, ML	Smart Home
11	Khan et al. Smart Home Networks with Blockchain	2020	Enhanced security using blockchain for smart homes.	Energy and resource constraints.	Research Paper	Khan, Abbas, s Rehman, et al.	Blockchain, ML	Smart Home