Volume 9, Issue 3, March – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

Machine Learning-based Intrusion Detection System Through WPA3 Protocol in Smart Contract System

Mohammad Sayduzzaman[1]; Jarin Tasnim Tamanna[1]; Sadia Sazzad[1]
[1]Department of CSE, National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka-1350

Muaz Rahman[2]
[2]Department of EEE, National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka-1350

Tawhidur Rahman[3]
[3]Digital Security & Digital Diplomacy, ICT Division, Agargaon, Dhaka-1207

Abstract:- Nowadays, the Internet has become one of the basic human needs of professionals. With the massive number of devices, reliability, and security will be crucial in the coming ages. Routers are common to provide us with the internet. These routers can be operated in different modes. Some routers use the Wifi Security Protocol (WPA) or WPA2, and the Wifi Alliance introduced WPA3 on 25 June 2018. There are a lot of papers regarding Smart Contract (SC)–based IDS as well as Machine Learning-based IDS. Very few discuss combining SC and ML-based IDS for different authentication processes. In this paper, we will discuss how combining SC and ML plays a vital role in authentication. Also, we play the role of embedded IDS system so that existing vulnerabilities of the WPA2 and WPA3 can be reduced to 99.62%.

Keywords:- *Machine Learning, Smart Contract, WPA3 Protocol, Router, Cybersecurity, Data Analysis.*

I. INTRODUCTION

With the rapid development of technology, security is one of the biggest threats now. This security threat is to the information we have, process, and transmit [1], [2]. While transmitting any critical information we should think of its security and also the existing vulnerability of the medium we use. As we are highly dependent on Wifi for using the www for any data transmission, we should know its vulnerability and be aware of it. Wifi maintains the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. In case of using public wifi, we should avoid any type of financial transmission as well as we should refrain from transmitting any confidential or private information. In Fig.1. the general concept of SCandML based IDS is given. Wifi alliances have introduced 8 different models of existing wifi [3], [4]. Wifi 8 will be adopted within 2028. Fig. 2. [5] describes different generations of wifi. Where * marked wifi 0, 1, 2, 3 are from retroactive inference. This is why they do not exist in official nomenclature, and Wifi 8 will be adopted by 2028. Generations of wifi and their adapter driver must be installed in the operating system to access www properly. One potential rule is that if the adapter has a WPA2-PSK (AES) method, a separate driver must be installed for proper connectivity. Otherwise, that will not work [3], [6]. Network security is crucial in any system run by smart contracts [7]. Traditional security measures, however, might not be enough to recognize and stop advanced cyber threats. The goal of this project is to create a strong Intrusion Detection System (IDS) that operates within the WPA3 protocol by utilizing machine learning techniques. To find any security flaws, the IDS will examine user behavior, network traffic patterns, and anomaly detection. The system's integration with smart contracts will enable it to react to threats on its own and improve the overall security posture of decentralized networks using the WPA3 protocol [8].

Growing Complexity and Sophistication of Cyberthreats: Conventional intrusion detection systems may find it more difficult to identify and stop new security flaws and attacks as a result of the growing sophistication and complexity of cyber threats [9]. Through the analysis of massive amounts of data and the identification of patterns suggestive of harmful behavior, machine learning presents the possibility of improving detection capabilities. The necessity of robust security method: Robust security methods are necessary for decentralized systems that run on blockchain networks and are managed by smart contracts to guard against cyberattacks, illegal access, and data breaches. It is imperative to guarantee the integrity and security of these systems in order to preserve trust and dependability in decentralized platforms and apps. Enhanced security for WPA3: Wi-Fi security has advanced significantly with the release of the Wi-Fi Protected Access 3 (WPA3) protocol, which offers more robust encryption techniques and defense against a wider range of threats than its predecessors. Wi-Fi networks' security posture can be further improved by integrating machine learning-based intrusion detection with WPA3, adding more lines of protection against possible at-tackers [10], [11].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

Scalable and adaptive security solutions: Machine learning algorithms have the ability to adapt and evolve over time, continuously learning from new data and improving their detection capabilities. By leveraging machine learning within the context of smart contract systems, organizations can deploy scalable and adaptive security solutions capable of addressing evolving cyber threats in decentralized environments [12]. Security automation based on smart contracts: Operating on blockchain networks, smart contracts allow predefined rules and policies to be executed autonomously. Security measures can be automated and enforced in real time by integrating machine learning-based intrusion detection with smart con-tracts. This enables proactive threat identification and response without the need for human interaction. The main contribution of the paper is–

- To improve IDS's overall performance, we have combined machine learning with smart contract implementation and put out a novel methodology.
- Our methods will be put into practice, making WPA3 more dependable and secure.
- We assess various models and combine the findings for additional study.

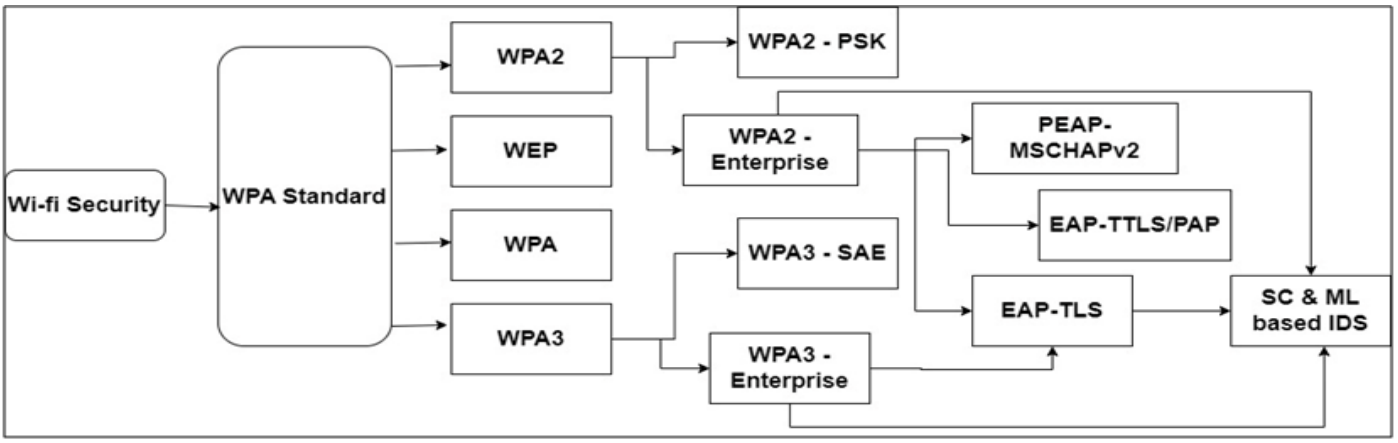

Fig 1 Concept of SCandML based IDS

➢ *Organization:*

This article is organized as follows: The author discusses the previous works and basic idea of IDS in section II, along with attack vector detection and their solution. Then, proposed SC & ML-based IDS for WPA3 and Algorithm in section III. The evaluation of the results and an adequate discussion are presented in section IV. Finally, the conclusion, along with a few considerations, limitations, and future discussions, is in section V.

II. BACKGROUND AND LITERATURE REVIEW

From the very beginning of wifi technology, Intrusion Detection Systems played a vital role in detecting any inhuman as well as unwanted activities that may breach the overall security and open the ground for critical cyber-attacks [13]. IDS can be an anomaly or signature-based [14]. Researchers are researching smart contract-based IDS as well as ML-based IDS. Recently, they have been combining different technologies like SC & ML for better performance. Below, we will discuss the adoption process of SC & ML, followed by a section with previous work. Required abbreviations are listed in Table 1.

Table 1 List of Common Abbreviations with Description

Keys	Description
AI	Artificial Intelligence
AFD	Armed Forces Division
AP	Access Point
Wifi	Wireless Fidelity
www	World Wide Web
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access Version 2
WPA3	Wi-Fi Protected Access® 3
WEP	Wired Equivalent Privacy
IEEE	Institute of Electrical and Electronics Engineers
PSK	Pre-Shared Key
AES	Advanced Encryption Standard
SAE	Simultaneous Authentication of Equals
SAE-PK	Simultaneous Authentication of Equals Public Key
Sec	Hash Extension Security Parameter

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

SSID	Service Set Identifier
AES-GCM	AES With Galois/Counter Mode
EAP	Extensible Authentication Protocol
RC4	Rivest Cipher 4
SSID	Service Set Identifier
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
MS-CHAPv3	Microsoft Challenge Handshake Authentication Protocol Version 3
TTLS	Tunneled Transport Layer Security
ECDSA	Elliptic Curve Digital Signature Algorithm
IDS	Intrusion Detection System
SC	Smart Contract
ML	Machine Learning
MFP	Management Frame Protection
EAP	Extensible Authentication Protocol
KCM	Key Confirmation Messages
DApp	Decentralized Application or System
SSI	Self-Sovereign Identity
ISI	Information Sciences Institute
USC	University of Southern California

While researching from the very beginning, we found huge papers full of hesitation about whether WPA3 is the miracle of technology that can never be backdated. [15] or it is just a simple improvement over WPA3, which is still vulnerable to all those attacks that are very common in WPA2, while WPA3 is configured to serve both WPA2 & WPA3 supported devices [16]. We approach further to find something exclusive, and then we find several ML approaches for securing WPA3, but few of them are standard as we have to maintain an easy-to-implement approach for WLAN or Wifi [17]. Next, we go for technology like blockchain; we found and interesting part of Blockchain is Ethereum-based smart contracts. Both the server and the client will communicate, and no third party will be involved; the transaction will be recorded on a universal ledger. Then, for authentication and intrusion detection, we take ML [18]. We have tried different ML algorithms so that different vendors can choose suitable options for them. In our system, we have found that Random Forest detects 99.62% of unwanted authorization approaches that fail to connect via WPA3.

Normally, wi-fi technology exchanges information via hand-shake. In the handshaking device the router shares a hashed version of the Wi -Fi password. One major flaw is that an attacker within range can simply listen in and capture the hash password when you connect. Once the handshake is captured, they can just leave and use a program like Hashcat to try to crack the network password. Now, if the attacker isn't in range when a device is connecting, they don't really need to wait. They can just force a handshake by sending management frames called de-auth packets. This will disconnect the actual device from the Wi-Fi network, forcing it to exchange a new handshake anyway while the attacker just listens in. This is the second major flaw. Table II shows the difference between WEP and different WPA versions [19], [20].

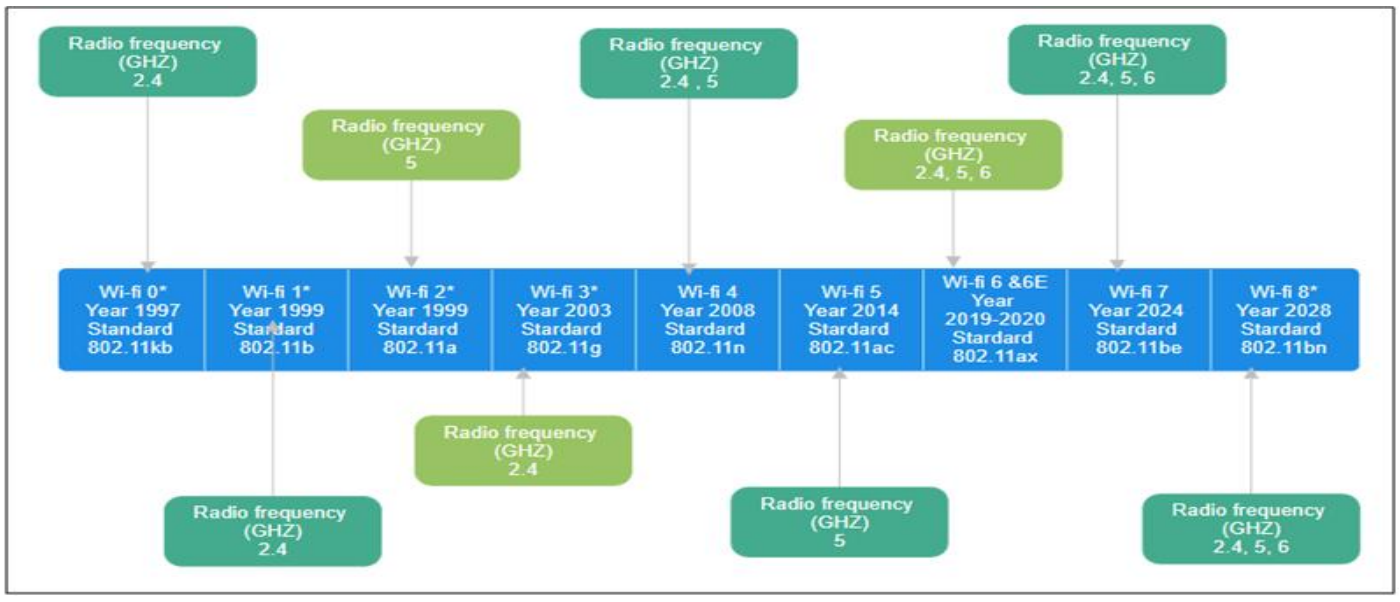

Fig 2 Overviews of Timeline for Wi-fi Network

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

Table 2 Difference between Different WPA Versions

Type	WEP	WPA	WPA2	WPA3
Encryption Method	RC4	RC4/TKIP	AES	AES-256 in GCM mode with SHA-384
Encryption key size	40 bits	128 bits	128 bits	128 bits, 192 bits, and 256 bits
IV size	24 bits	48 bits	128 bits	256 bits
Authentication process	Weak	802.1x -EAP	PEAP-MSCHAPv3, EAP-TTLS/PAP, and EAP-TLS	SAE, EAP
Data Integrity	CRC 32 - ICV	MIC	CCMP	AES-GCM

From Table 2, we can see that WEP uses RC4 as an encryption method, where each encryption key size is about 40 bits, and the initialization vector is 24 bits, where data integrity is CRC 32- TCV, but its authentication process proved weak. WPA3 comes with huge coverage. It has the following key features:

- WPA3-Personal Only Mode.
- WPA3-Personal Transition Mode.
- WPA3-Personal SAE-PK only Mode.
- WPA3-Enterprise only Mode.
- WPA3-Enterprise Transition Mode.
- WPA3-Enterprise 192-bit Mode.

WPA3 adopted the Management Frame Protection (MFP) and now WPA3 is harder to brute-force or dictionary attack. In WPA3, credentials comprise of [21].

➢ *Here is the Fingerprint Equation for WPA3:*

- Fingerprint =L(Hash(SSID||M||K_ AP), 0, 8 ∗ Sec + 19∗λ/4−5)

➢ *And the Password shall then be Determined as Follows:*

- Password Base=Base32(P (0)||P (1)||. . . ||P (λ/4− 1))
- Password=Add Separators (P asswordBase||ChkSum)

More details of this equation is available for further research at https://www.wi-fi.org/system/files/WPA3 Specification v3.3.pdf. In WPA3, a Dragonfly handshake is designed to frustrate attackers. While a nearby attacker could capture a handshake, it takes too long to brute force, and they have to stay in range of the router to try every single password guess. De-Auth packets and other management frames are also now encrypted in WPA3, which prevents attackers from jamming a WPA3 network by forging De-Auth packets between a router and any connected devices.

WPA3 also includes a feature called forward secrecy, and what this means is that if someone was able to capture some of your Wi-Fi traffic and later on learned your password, they wouldn't be able to go back and decrypt everything that they gathered. Now for this and all the other security updates, you should definitely update to WPA3. could leak data, the creators of WPA3 were forced to react with a hasty fix to address the timing attack, but in doing so, they also made it possible to jam WPA3. So, to break down the original issue, when a device joins a WPA3 network, the router converts, while, unfortunately, a nearby attacker can measure this by the time it takes for the router to reply, and this information lets the attacker more easily brute force the WiFi password. Then, based on the unique amount of time it takes for WPA3 routers to process different passwords, hackers can rule out large groups of password guesses to try brute-forcing attacks. This breaks WPA3's promise of immunity from brute-forcing attacks less than a year after its release. They decide to solve this by always making the access points perform a lot of computations and always reply a bit slower. The way that we made it reply slower is by making this algorithm that is used internally perform a few iterations of a certain function. Now, this prevents the timing leak if done properly. However, doing these iterations adds a lot of overhead. So if you then, for example, implement WK3 on a very lightweight device or an IoT device, this countermeasure means they possibly are vulnerable to denial-of-service attacks, or they don't or implement just a weak version and then they might be vulnerable to the side channels. As mentioned, their fix paved the way for a fairly simple denial-of-service attack. Hackers can send many handshakes at the same time, causing the router to crash and taking the network completely offline [22], [23].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

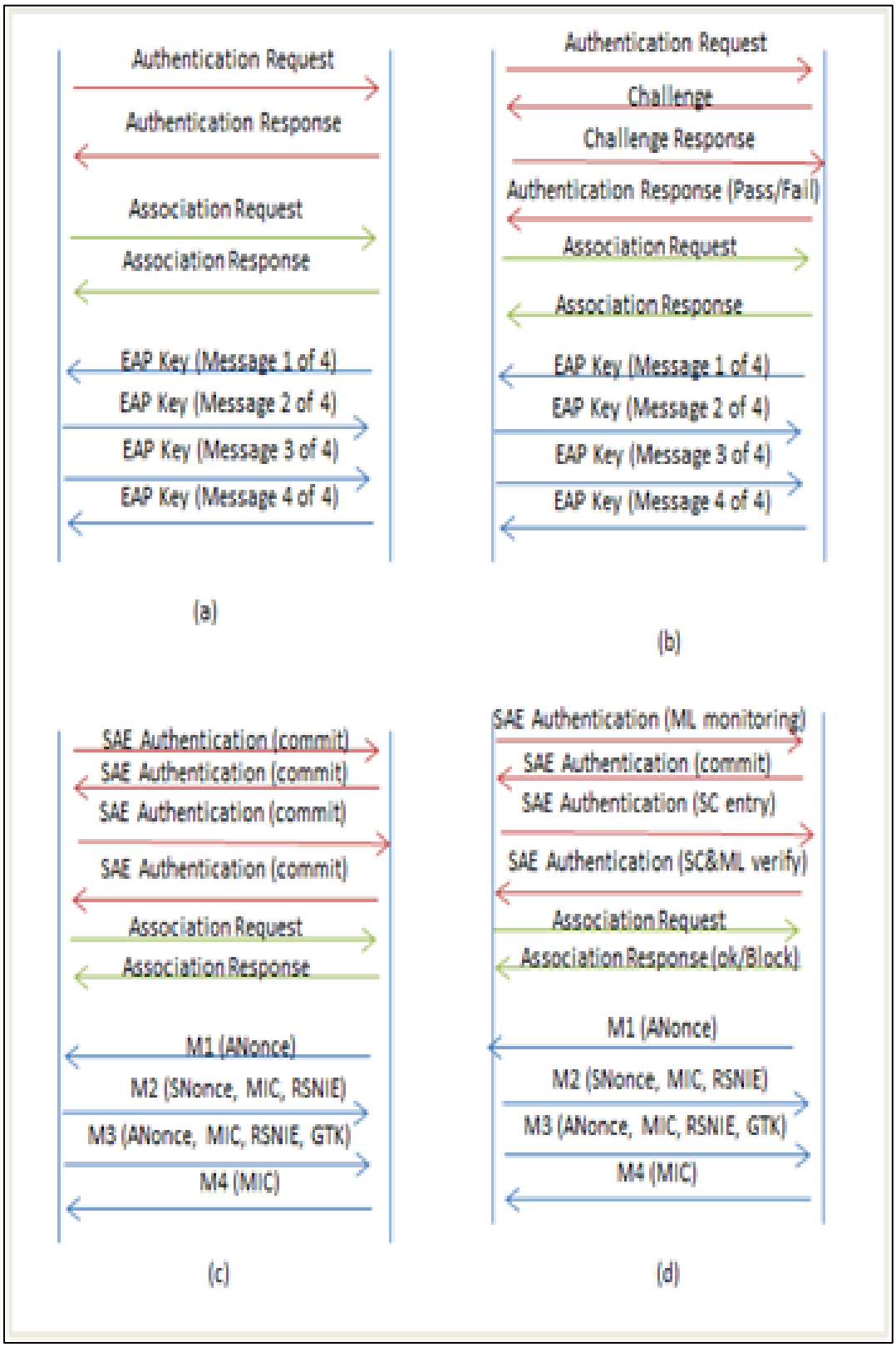

Fig 3 (a) 4-Way Handshake (b) Shared Key Authentication Process. (c) Existing WPA3 Model and (d) A Proposed Model for WPA3.

In Fig. 3. among these four scenarios in case (a) after authentication and association, a 4-way handshake takes place using Extensible Authentication Protocol. This represents an open system authentication. Case (b) represents a shared key authentication process. Case (c) is the existing WPA3 model, and case (d) is the proposed model. ML will monitor, and SC will make an entry. After a successful verification process, it will improve further. Table III shows a list of existing works that were analyzed on WPA3 IDS.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

Table 3 List of Attacks and Necessary Tools Along with their Solutions

Attacks	Attack method	Impact	Mitigation Process
Downgrade to serve WPA2 devices	Client connects to WPA2 rather WPA3	AP becomes vulnerable	Device firmware to be updated
Authentication Flood attack	Denial of service	AP goes offline	SC & ML based IDS
SAE out of range attack	Denial of service	AP goes offline	SC based real time token
SAE unsupported group attack	Denial of service	AP goes offline	SC based group token
Downgrade group attack	AP flooding	AP becomes vulnerable	ML based authentication
Timing side channel attack	Brute-force	System leaks information about the password	SC & ML based IDS
Deauthentication Attack	Brute-force / dictionary	AP goes offline	SC & ML based IDS
Beacon/Probe flood attack	Response flooding	Confuse clients find the legitimate AP	SC & ML based IDS

Table 3 shows a list of attacks and necessary tools along with their solutions [16], [24]. Previously, some commercial signature-based IDS was developed after the failure of anomaly-based IDS [25] likely Snort-Wireless [26], AirMagnet [27] and AirDefence [27] were successful for WPA2. However, they are not updated enough to work successfully for WPA3. Here comes the concept of SC & ML-based IDS systems. In Table IV a list of previous work is given in a brief.

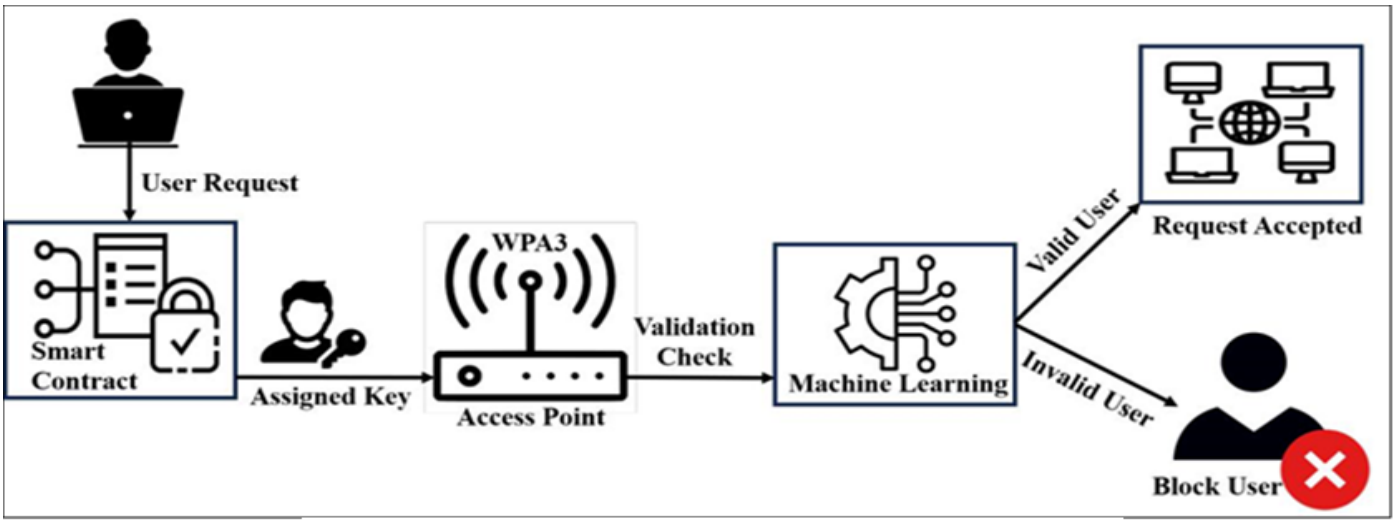

Fig 4 Proposed Architecture for SCML-based IDS for WPA3 Network

Table 4 List of Existing Works Analysis on WPA3 IDS:

Work	Platform	Contribution	Architecture	Method
Christopher P. Kohlios et.al [26]	Four-way handshake attack flow.	Attack vector analysis	WPA2, WPA3	Attack flow analysis
Dalal, Neil, et al. [27]	Attack vector	Signature based IDS	WPA2, WPA3	Signature based IDS
Saini, Rahul et al. [18]	WPA3 enterprise network Protected	IDS and Attack flow	WPA3	Signature based IDS
Alsharbaty, Firas S an Ali et al. [28]	Protected wifi	Electronic substation	WPA3	Hybrid IDS
Bhutta, A.A et al. [29]	LightGBM	Realtime	WPA3	Lightweight wifi IDS
Koutras, Dimitris et al. [30]	Automatated IDS	Automation	WPA3	ID based method
Thankappan, M., Rifa Pous et al. [31]	Protected wifi	Signature based IDS	WPA3	Signature based IDS
Saifan, Ramzi and Radi et al. [32]	Log Monitoring	Mitigationtool	WPA2	Log Monitoring
Kishiyama , Brian and Guerrero et al. [33]	Security Policies Automation	Security Policies Automation	WPA2	Security Policies Automation
Qaddoori, Sahar L and Ali et al. [34]	Industrial IOT	IDS	WPA2	ML
Uszko,Krzysztof and Kasprzyk et al. [35]	5G WAN	Rule based IDS	WPA2	ML
Narayana, Datta Sai et al. [36]	Protected Network	Prevent Hijaking	WEP	Adaptive threat defebding
Stella,Kand Menaka et al. [37]	Wifi Hotspot	Traffic monitoring	Detecting spoofing	Threat defebdibg
Mansour, Salah Eddine et al. [38]	IoT-Fog Networks	Improving security	IOT	AI Image processing

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

III. PROPOSED SCML-BASED IDS FOR WPA3

Fig. 4. is the Proposed Architecture for SCML-based IDS for WPA3. Fig. 5. Describes the step-by-step method for our proposed SCandML-based IDS system in (Fig. 4.):

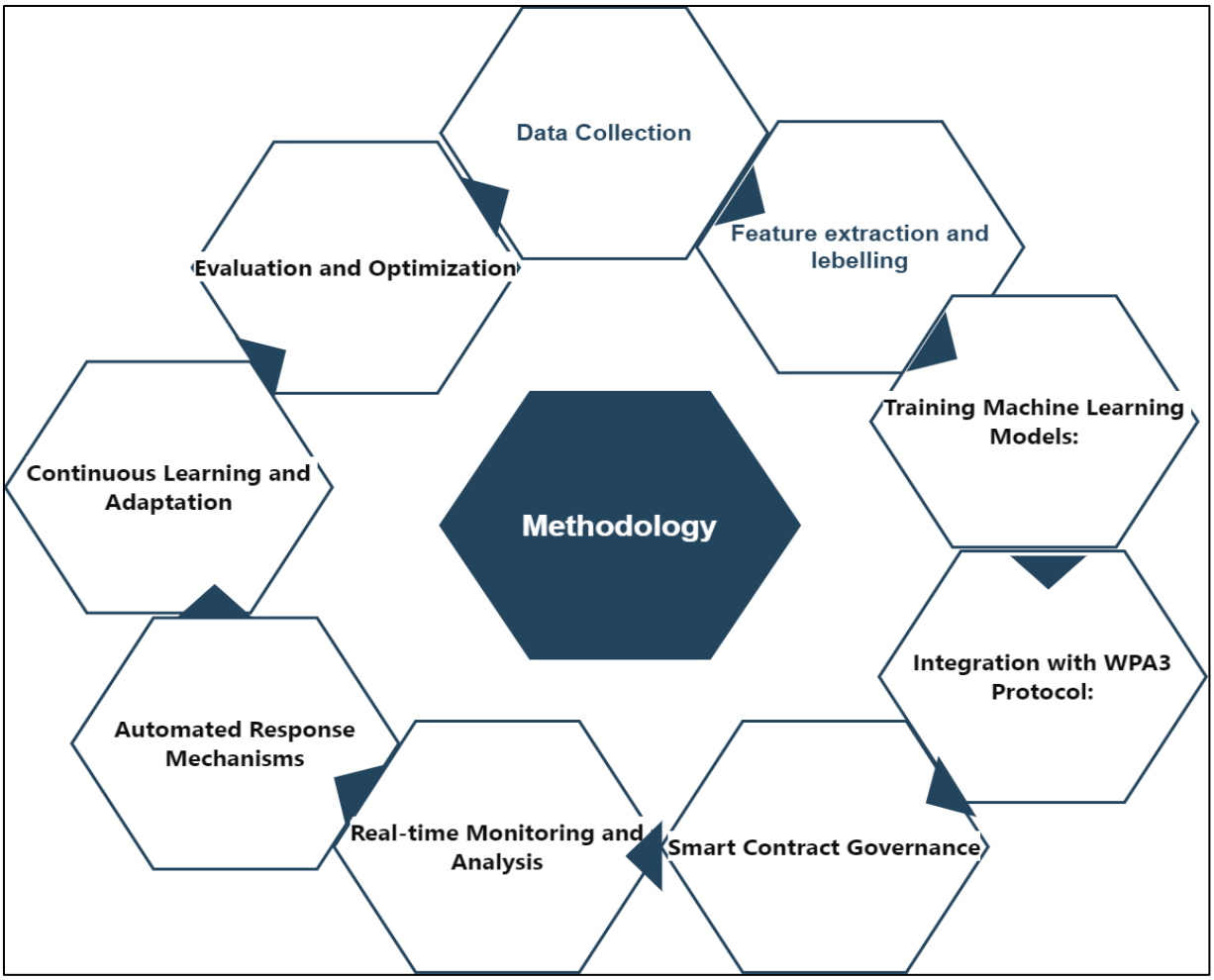

Fig 5 Proposed Methodology of SCandML based IDS

➢ *Data Collection:*

Obtain network traffic data from Wi-Fi access points that are using the WPA3 protocol, such as packet headers, payload details, and metadata. Gather extra contextual data on user activity, device information, and network topology [39], [40].

➢ *Feature Extraction and Labeling:*

To depict network traffic patterns and behavior, extract pertinent elements from the data that has been gathered. Packet size, connection frequency, protocol utilization, source and destination IP addresses, and timestamps are a few examples of features. Moreover, the gathered data will be classified according to predetermined criteria as either normal or abnormal [41], [42].

➢ *Smart Contract Governance:*

Create smart contracts to control how the decentralized network's intrusion detection system operates. Establish guidelines and procedures, such as thresholds for anomaly detection and the steps to be taken after discovery to identify and address security threats [45].

➢ *Real-Time Monitoring and Analysis:*

Use the integrated solution to deploy real-time network traffic monitoring. Use the machine learning models that have been trained to analyze incoming data streams and find any irregularities or potential security issues [46].

➢ *Automated Response Mechanisms:*

Incorporate automated reaction systems inside the smart contracts to address identified security risks. Removing access privileges, upgrading encryption keys, barring questionable people, and setting off alarms for additional research are a few examples of possible actions.

➢ *Continuous Learning and Adaptation:*

Retrain and up-date the machine learning models frequently in response to input from ongoing network research and monitoring. Include systems that allow response plans and detection levels to be dynamically adjusted in order to respond to changing security threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

➢ *Evaluation and Optimization:*
Assess the intrusion detection system's performance on a regular basis with regard to response efficacy, false positive/negative rates, and detection accuracy. To increase the system's effectiveness over time, optimize it based on performance indicators and input from security incidents.

By using this approach, businesses can leverage the powers of machine learning, the WPA3 protocol, and smart contract governance to create a strong Machine Learning-based Intrusion Detection System through WPA3 Protocol in Smart Contract System that improves security within decentralized networks. We have demonstrated how our suggested method-ology can be employed with the current WPA3 design in Fig. 3.

➢ *ML-based Intrusion Detection Process*
Within the field of artificial intelligence (AI), machine learning is a subset that allows systems to learn from data and make judgments or predictions without requiring explicit programming. To find patterns and anomalies suggestive of security dangers, machine learning algorithms are trained on massive databases of historical security-related data in the field of cybersecurity. Among the crucial facets of machine learning are:

- Training Data
- Feature Extraction
- Model Training
- Model Evaluation and Validation, and
- Deployment and Monitoring

A number of parameters are crucial to the design, implementation, and assessment of an intrusion detection process based on machine learning and smart contracts. Fig. 6 represents some crucial factors:

- *Data Sources:*
Parameters pertaining to the data sources—such as system logs, network traffic logs, sensor data, or external threat intelligence feeds—that are utilized to detect intrusions.

- *Feature Selection:*
Factors, such as feature types, feature extraction strategies, and feature engineering techniques, that are involved in choosing pertinent features from the data to train machine learning models.

- *Machine Learning Algorithms:*
Parameters pertaining to the selection of machine learning algorithms for intrusion detection, including unsupervised anomaly detection techniques, decision trees, random forests, support vector machines, and neural networks.

- *Model Training:*
Hyperparameters, optimization methods, cross-validation techniques, and training/validation/testing data splits are some of the parameters that are involved in the training of machine learning models.

- *Smart Contract Design:*
Parameters for creating smart con-tracts that regulate the intrusion detection process, including as access control methods, situations that set off alerts or responses, and contract logic.

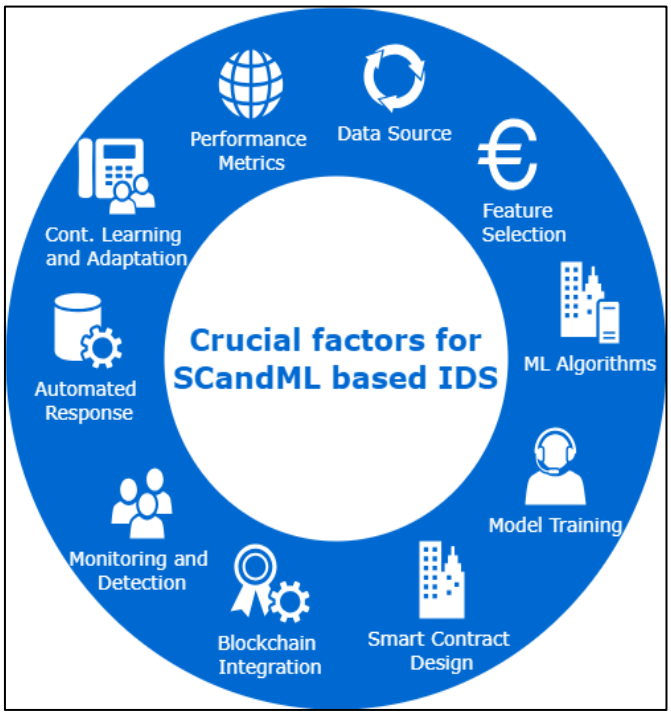

Fig 6 Key Parameters of SCandML based IDS

- *Blockchain Integration:*
Issues including data storage, off-chain data access, transaction fees, and blockchain scalability considerations that are involved in combining machine learning models with smart contracts on a blockchain network [47].

- *Real-Time Monitoring and Detection:*
Specifications such as sample rates, data streaming protocols, processing delay, and resource requirements for continuous monitoring that are connected to real-time network activity monitoring.

- *Automated Response Mechanisms:*
In smart contracts, automated reaction mechanisms can be specified. These include response actions, thresholds for starting reactions, and escalation processes for handling security incidents.

- *Continuous Learning and Adaptation:*
Details include update frequency, retraining methods, feedback systems, concepts, and data drift management procedures that are related to the intrusion detection system's continuous learning and adaptability.

- *Performance Metrics:*
For evaluating the recall, accuracy, precision, F1-score, false positive and false negative rates, detection latency, and scalability of the intrusion detection system can be considered.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

- *Community Consensus and Governance:*

Characteristics of the decentralized network's governance and community involvement, including voting procedures, stakeholders' involvement, consensus algorithms, and transparency standards, are part of Community Consensus and Governance. Behavioral analysis and machine learning approaches are frequently used in cybersecurity to improve threat detection capabilities, which helps to identify and address security issues more successfully [48]. Through the early detection of suspicious activity and possible security breaches, these strategies assist to stay ahead of cyber threats. In some situations, such as decentralized applications or systems where access control is controlled via a blockchain network, smart contracts can make barring a user easier.

➢ *To Block a user, a Smart Contract can be Created as Follows:*

User Identification The smart contract needs a way to identify the user or account that should be blocked. This could involve the user providing some form of unique identifier, such as an Ethereum address or a digital identity stored on the blockchain.

Blocking Mechanism, the blocking mechanism's implementation is handled by logic in the smart contract. This rationale outlines the circumstances in which a user should be blocked as well as the steps to be performed when blocking has been decided.

Authorization and Access Control The smart contract checks users' credentials and permissions before enabling them to engage with the system or application. A user is blocked by the smart contract if their access requests are rejected in the future, depending on pre-established rules or criteria.

Event Logging and Notification The smart contract may log the action on the blockchain or emit an event when a user is blocked. In addition to promoting openness, this makes the blocking event visible to other network users.

Revocation of Privileges The smart contract may remove some of the prohibited user's rights or privileges, depending on the application or system requirements. In a decentralized social media site, for instance, a blocked user might no longer be able to communicate with other users or upload material.

Appeal or Dispute Resolution In certain situations, the smart contract might have procedures that allow users to con-test actions taken against them or appeal-blocking decisions. This can entail giving people a way to submit proof or contest the legitimacy of the blocking event.

➢ *Approaches of Smart Contracts*

Fig. 7. illustrated the flow diagram for controlling user access via smart contract:

User Interface The user interface is where users initiate the authentication process. This could be a web interface, mobile app, or desktop application.

Authentication Service This component verifies the user's identity and credentials. It may involve traditional methods like username/password, bio metric authentication, or decentralized identity solutions such as Self-Sovereign Identity (SSI).

Smart contracts contain the authentication logic for the DApp. They define the rules and criteria for authenticating users and granting access to the application's features and functionalities.

Blockchain Network The smart contract(s) run on a blockchain network, which serves as the underlying infrastructure for the DApp. The blockchain ensures the integrity and security of user authentication processes.

Consensus Protocol The consensus protocol governs how transactions and smart contract state changes are validated and agreed upon by network participants. It ensures the immutability and trustworthiness of the blockchain network.

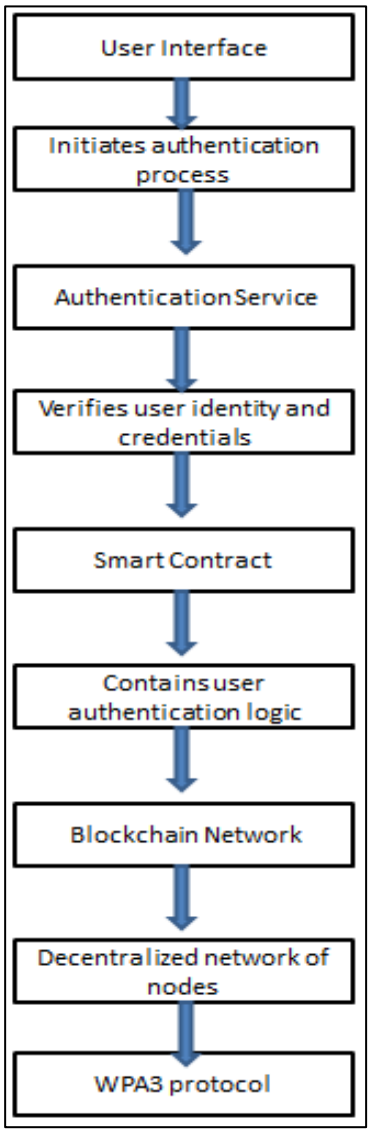

Fig 7 Flow Diagram for Controlling user Access via Smart Contract

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

WPA3 Handshaking Process Fig. 3(c). explained an overview of existing WPA3 handshaking process, which is discussed below [16]:

SAE Handshake Initialization: The SAE handshake begins with the client sending a ”commit” message containing some unique IDs like MAC address. The access point (AP) responds with its own commitment value and generates a random nonce. Both parties use their commitment values and the nonces to calculate the shared secret.

- Step 1: The client and AP deal with the Pairwise Master Key (PMK). The PMK is then used to generate other keys such as the Pairwise Transient Key (PTK) and Group Transient Key (GTK) which are prepossessing tasks to establish a connection.
- Step 2: Exchanging messages is important to confirm the position of the secret key. This includes the exchange of Key Confirmation Messages (KCMs) to verify the integrity of the key exchange process.
- Step 3: Once verification and key exchange process is completed then the secure connection is established. In this process negotiated encryption algorithm (e.g., GCMP-256) can be used.
- Step 4: By changing the encryption keys on a regular basis, WPA3 maintains forward secrecy, making it more difficult for an attacker to decrypt previous conversations—even if they are able to access the keys. This is a considerable improvement in WPA3 over WPA2.

➢ *The Integration of Smart Contracts*

The integration of Smart contracts with Wi-Fi Protected Access 3 (WPA3) would include blockchain technology with WPA3’s permission and authentication protocols. Here is a theoretical explanation of how this integration might function:

Decentralization of Identity Management: Manage user IDs for Wi-Fi access by utilizing blockchain-based decentralized identity systems like Self-Sovereign Identity (SSI). Every user might have a distinct digital identity that is kept on the blockchain and contains authorization codes and login credentials for using Wi-Fi networks.

➢ *Using Smart Contracts for Access Control*

On a blockchain network (like Ethereum), smart contracts can be used to control access to WiFi networks. The access point can communicate with the blockchain network through smart contracts when a user tries to connect to a WPA3-secured Wi-Fi network in order to confirm the user’s identity and authorization [49].

- *Authentication and Authorization:*

The user’s device can start a transaction with the access control smart contract once it is connected to the Wi-Fi network. Based on specified rules stored on the blockchain, the smart contract can confirm the user’s digital identity and determine whether they have the required permissions to access the network. The smart contract may authorize access if the user satisfies the authentication and authorization requirements by supplying the session key or other credentials needed for WPA3 authentication.

- *Secure Communication:*

After authorization, the user’s device can use the standard WPA3 protocols to create a secure connection with the access point. According to WPA3 standards, all communication between the user’s device and the access point is encrypted and safe [50].

- *Transparency:*

All-access control transactions and inter-actions with smart contracts are recorded in an immutable ledger that blockchain technology offers. Network administrators are able to detect and monitor user access to Wi-Fi networks in real-time, which also provides transparency.

- *Decentralized Network Governance:*

Decentralized management of Wi-Fi network configurations and policies is another application for smart contracts. Smart contracts might regulate network factors like key management, access controls, and encryption techniques, offering a visible and im-penetrable governance structure [51]. However, when putting such solutions into practice in real-world circumstances, it’s crucial to take into account practical issues like scalability, interoperability, and regulatory compliance. Integrating smart contracts with Wi-Fi Protected Access 3 (WPA3) in the event of a hacking attack involves leveraging blockchain technology’s inherent security features to mitigate and respond to such attacks [52].

➢ *Here’s how this Integration could Enhance Security and Resilience:*

- *Real-Time Threat Detection:*

Smart contracts have the ability to continuously scan the blockchain network for any questionable WiFi-related activities. The smart contract has the ability to send out alerts in response to anomalies like repeated unsuccessful authentication attempts or unwanted access attempts.

- *Automated Response Mechanisms:*

It is possible to program smart contracts to launch automated reactions in response to attempted hacking. For instance, the smart contract might dynamically modify access control settings to improve security or momentarily stop additional access attempts from the shady source in the event that it detects a brute-force attack.

- *Secure Recovery Processes:*

After a hacker assault, smart contracts can enforce safe recovery procedures like reissuing login credentials or resetting access rights. With the use of smart contracts, these recovery procedures may be regulated and automated, lowering the possibility of additional security breaches or human error [53].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

- *Community Consensus Mechanisms:*

When it comes to Wi-Fi security, smart contracts have the potential to im-prove network resilience by utilizing community consensus to evaluate and address new threats jointly. Organizations can adopt a more proactive and resilient approach to cybersecurity by combining smart contracts with WPA3 and blockchain technology. By utilizing automated threat detection, response mechanisms, and immutable audit trails, these strategies can significantly lessen the impact of hacking attacks.

➢ *Integration with Machine Learning IDS*

Smart contract data can be analyzed by machine learning algorithms, which can then be trained to spot trends that point to possible security risks or questionable activity. Anomalies such as strange connection attempts, strange traffic patterns, or recognized attack signatures can be identified by the machine learning model [54].

- *Smart Contract-Based Decision Making:*

The machine learning model has the ability to use the smart contract to send out alerts or notifications when it notices questionable activities. Based on predetermined rules or regulations, smart contracts are able to assess the context and degree of detected anomalies and decide on the best course of action.

- *Automated Response and Mitigation:*

To reduce any security risks, smart contracts can start automated reaction systems. This could entail limiting access, barring questionable people for a short while, or changing security settings like encryption keys.

- *Continuous Learning and Adaptation:*

The machine learning model is able to adjust its detection capabilities to threats that change over time by continuously learning from new data. Over time, smart contracts can help to increase the efficacy of the IDS by facilitating the integration of updated security policies and machine learning models. Here are some techniques that can be implemented within smart contracts to block suspicious users in the context of Wi-Fi Protected Access 3 (WPA3):

- *Threshold-based Anomaly Detection:*

Set thresholds in the smart contract to track different data, such as the quantity of unsuccessful authentication attempts, odd traffic patterns, or abrupt activity spikes. Consider the user to be suspect and start blocking mechanisms if the detected metrics are higher than predetermined levels.

- *Whitelist and Blacklist Management:*

Keep lists of recognized, trustworthy, and questionable users on both the whitelist and the blacklist within the smart contract. Put the user on the blacklist when suspicious activity is discovered to stop them from accessing the network again.

- *Dynamic Access Control Policies:*

Within the smart contract, define dynamic access control restrictions depending on contextual data such device kind, location, time of day, and user behavior. Real-time access privilege adjustments can be made for suspicious users, either by temporarily removing their access or reducing it.

- *Rate Limiting and Throttling:*

Use rate-limiting and throttling techniques in the smart contract to restrict the quantity of connections or requests that a single user may make in a certain amount of time. If a user exceeds the permitted criteria, they may be automatically blocked.

- *Behavioral Analysis and Machine Learning:*

Make ad-vantage of machine learning techniques to examine trends in user behavior and spot deviations that point to questionable activities.

To increase the machine learning model's accuracy in identifying malicious activity, train it with historical data. In this paper, we will focus on Machine Learning and Behavioral Analysis [55].

➢ *Behavioral Analysis*

In behavioral analysis, entities like individuals, devices, apps, or networks are observed, and their behaviors, interactions, and patterns of behavior are analyzed. The aim is to find abnormalities in behavior that might point to malevolent or illegal activities. Among the crucial facets of behavioral analysis are:

- Baseline Establishment
- Anomaly Detection
- Contextual Establishment, and
- Continuous monitoring

➢ *Description of Proposed Algorithm*

In a nutshell, the process can be represented in an algorithm. The proposed architecture firstly collects a flag value which is uniquely assigned from the system to the user who wants to access the system to use the data. Then, the value, along with the information, was passed through the smart contact. In the smart contract system, the value is updated from the flag value to another unique value where a private key is added. Then, the smart contract checks whether there is any anomaly directed or not, comparing the value with the system. If the anomaly is detected, the value is then returned to the smart contract, but if there is no anomaly, then the value is passed to the machine learning model. Again, the value is updated, and the value is with the system and authenticates the user as a valid user if the value is matched. As a result, the invalid user can be directed, and the data sharing security is ensured.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

Algorithm 1: Proposed security system to check the validity of the user with the help of Smart Contract

```
Output: Authenticate the user and provide the
        permission to the user to access data
while (function accessSystem(user)==True) do
  Step 1: Collect flag value from the system flag
    value = system.assignFlagValue(user);
  Step 2: Pass value through smart contract
    updated value =
        smart contract.updateValue(flag value, user);
  Step 3: Anomaly Detection
   if smart contract.detectAnomaly(updated value)
    then
      return smart contract.handleAnomaly()
   else
      Step 4: Pass value to machine learning model
          authenticated value =
           machine learning.authenticate(updated value)
   end
   Step 5: Value Update and Authentication
   if authenticated value == system.checkValue():
    then
      Valid user, grant access
      return "Access granted"
   else
      Invalid user, direct accordingly
      return "Access denied"
   end
end
```

In summary, the DApp authentication process involves the user interface initiating authentication, an authentication service verifying user identity, smart contracts containing authentication logic, and a blockchain network ensuring the security and integrity of the authentication process.

IV. RESULT ANALYSIS

A machine learning and smart contract-based intrusion detection process's performance, efficacy, and efficiency in identifying and averting security risks within a decentralized network are assessed as part of its result analysis. Key components of result analysis include the following:

A. Performance Metrics

- *Accuracy:*

The percentage of security threats that are accurately identified out of all instances. Precision: The percentage of security threats successfully recognized out of all instances that are categorized as threats. Recall: The percentage of security risks that were accurately recognized out of all real threats. F1-score: A fair performance indicator derived from the harmonic mean of recall and precision. False Positive Rate: The percentage of cases mislabeled as threats out of all cases that are not threats. False Negative Rate: The percentage of cases that, out of all actual threats, are mistakenly categorized as non-threats.

- *Detection Capabilities:*

Examine the system's capacity to identify various security risks, such as known assaults, zero-day exploits, and unusual activity. Evaluate how sensitive the system is to variations in the threat landscape, attack patterns, and network circumstances.

- *Response Effectiveness:*

Analyze how well smart contract-triggered automated reaction mechanisms mitigate identified security threats. Evaluate how quickly and suitably response actions—like stopping malicious activity, removing access, or initiating incident response workflows—are carried out.

- *False Positive Analysis:*

Examine cases of false positives to find the root reasons, which may include noisy data, incorrectly constructed models or inadequate feature selection. To reduce false positives without sacrificing detection accuracy, change the response thresholds, feature selection criteria, or model parameters.

- *False Negative Analysis:*

Analyze false negative cases to comprehend security dangers that were overlooked and possible intrusion detection system blind spots. Improve feature engineering and model training to increase sensitivity to new or subtle security threats.

- *Feedback and Iterative Improvement:*

Collect feedback regarding system performance, response actions, and secu-rity incidents in order to continuously enhance the intrusion detection process. Apply the knowledge gained to feature selection, smart contract governance, model retraining, and system architecture as a whole.

- *Scalability and Resource Efficiency:*

Examine the intrusion detection system's scalability to manage rising network traffic volumes and evolving security threat complexity. Optimize the use of resources, including memory, bandwidth, and compute power, to guarantee the system operates effectively in decentralized contexts.

- *Overall System Reliability and Trustworthiness:*

Assess the intrusion detection system's dependability and credibility in preserving the security and integrity of the network. To determine the overall effectiveness of a system, measure user satisfaction, system uptime, and adherence to security standards. Organizations can improve the security posture of decentralized networks by doing thorough result analysis to pinpoint areas for improvement and strengths and weaknesses in their Machine Learning and Smart Contract-based Intrusion Detection Process.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

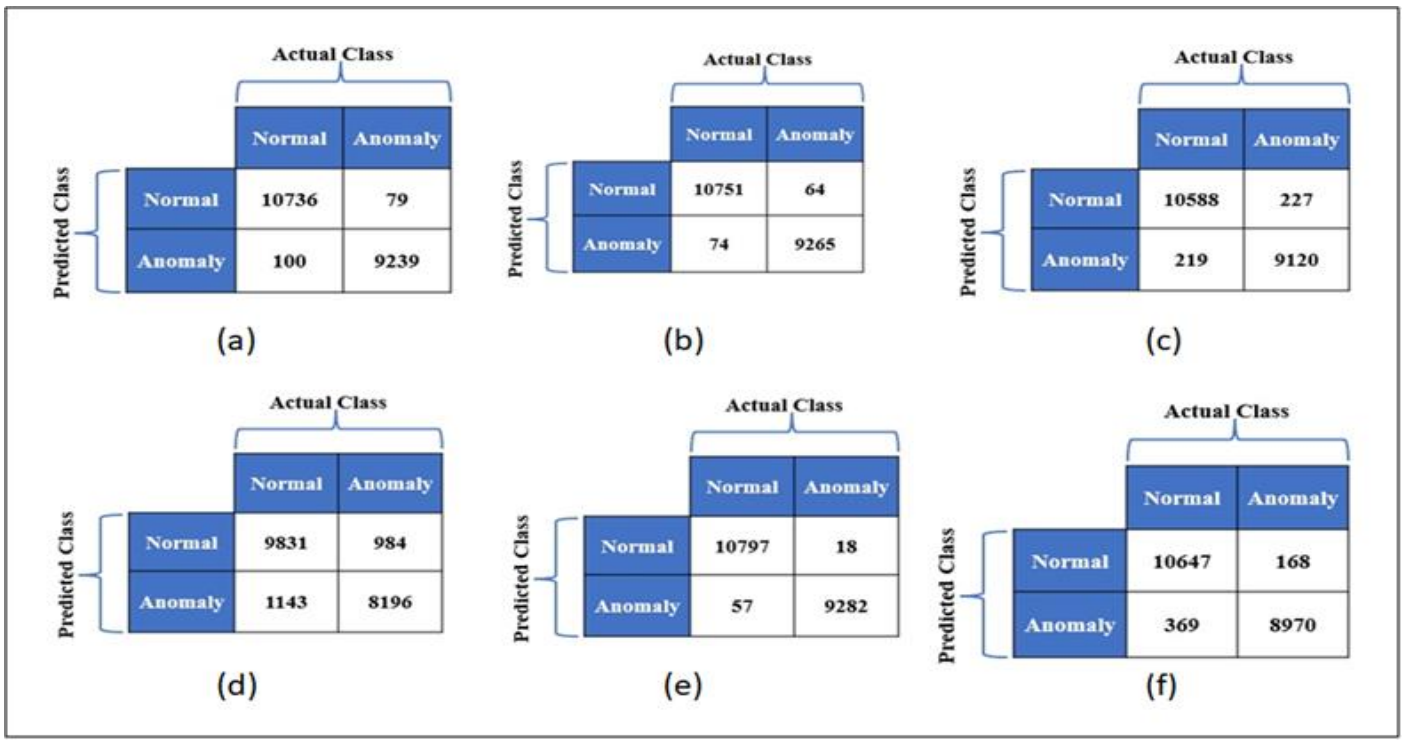

Fig 8 Confusion Matrix of Different Methods

B. Dataset

A popular benchmark dataset in the fields of network security and intrusion detection is KDD Cup'99 [56]. It was made in 1999 specifically for the Third International Knowledge Discovery and Data Mining Tools Competition. The dataset was developed by researchers from the Information Security Institute (ISI) at the University of Southern California (USC) and the Information Sciences Institute (ISI), along with other contributors. We also use this dataset for our system. Some key features of the KDD Cup'99 dataset:

➢ *Purpose:*

The purpose of the dataset creation was to support research in the areas of network security and intrusion detection. It is made up of numerous examples of network traffic data, including both benign and malevolent activity.

➢ *Data Characteristics:*

A variety of network traffic statis-tics, including both common and malicious activity, are included in the dataset. Numerous network protocols are covered, including TCP, UDP, ICMP, and others. Because the data instances are labeled with distinct attack kinds, supervised learning tasks can benefit from using them.

➢ *Data Format:*

The dataset is presented in tabular style, where a network connection or session is represented by each row. Numerous attributes or features, such as the protocol type, service type, source and destination IP addresses, etc., describe the properties of the network connection in each row.

➢ *Class Imbalance:*

A problem with the KDD Cup'99 dataset is its class imbalance, with most cases being associated with legitimate activity and only a tiny proportion being malicious attacks. This imbalance needs to be handled carefully during model training and evaluation since it can impact how well machine learning models function.

➢ *Preprocessing Requirements:*

Preprocessing the dataset is frequently necessary before using it for machine learning studies because of its size and complexity. This could involve fixing class imbalance, encoding category data, handling missing values, and normalizing numerical features [57].

➢ *Use in Research and Benchmarking:*

Researchers and practitioners have utilized the KDD Cup'99 dataset ex-tensively to evaluate intrusion detection systems, assess machine learning algorithm performance, and compare various methods for identifying and thwarting network attacks.

All things considered, the KDD Cup'99 dataset continues to be an important tool for furthering research in intrusion detection and network security, offering a consistent bench-mark for assessing the efficacy of different detection methods and algorithms. Fig. 8. Describes the Confusion Matrix for different ML models were,

- Confusion Matrix for KNN
- Confusion Matrix for KStar
- Confusion Matrix for Logistic Regression
- Confusion Matrix for Na¨ıve Bayes
- Confusion Matrix for Random Forest
- Confusion Matrix for SGD

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

We have used total 25193 data and among them performance testing was done on 80percent data and Training data was 20 percent. Our outcomes are as follows:

Fig. 9. Is the comparison chart of the output of different methods we have used. Where (a) Calculates the accuracy of different ML models. and (b) Calculates the accuracy against Time. By observing Fig. 9. and Fig. 10. whether or not time is taken into account, Random Forest stands out among the rest.

C. Accuracy Analysis with respect to Time

Model Name	Accuracy (%)	Time (Sec)
Naïve Bayes	89.44	0.72
SGD	97.33	0.32
KNN	99.11	9.65
Random Forest	99.62	0.49
Logistic Regression	97.79	0.09
KStar	99.31	333.11

Fig 9 Comparison Chart of Different Method we have used

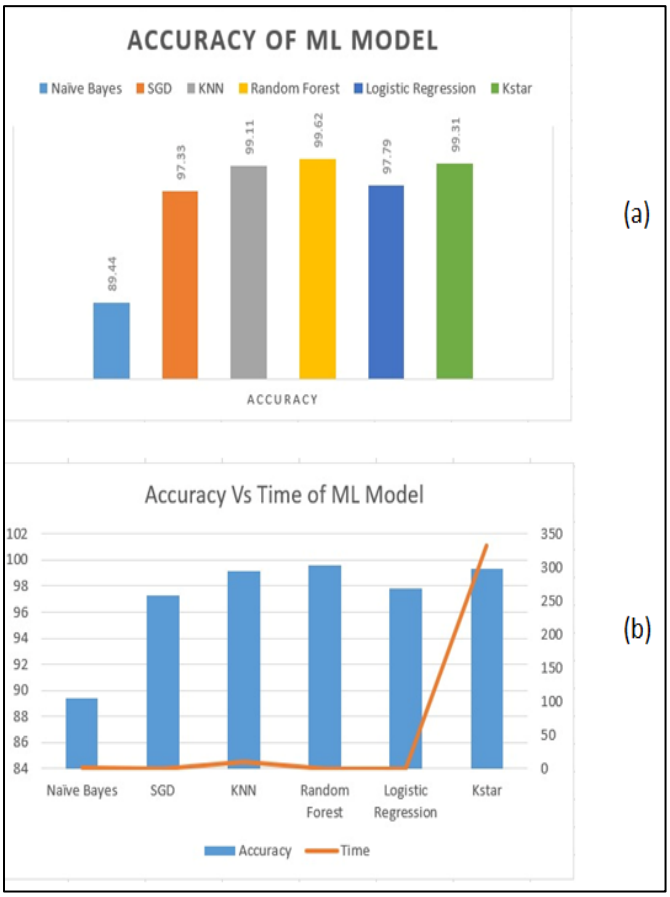

Fig 10 Accuracy of ML Models

V. CONCLUSION

Organizations can effectively and accurately identify a variety of security concerns, such as well-known assaults and unusual patterns, by utilizing a combination of machine learning algorithms. A decentralized governance framework for automating threat detection, initiating actions to identified threats, and guaranteeing accountability and transparency in security operations is offered via smart contracts. The amalgamation of machine learning with smart contracts provides decentralized networks with enhanced security posture through automatic reaction capabilities, adaptive learning, and real-time monitoring. In the future, Advanced Machine Learning Techniques: Subsequent investigations may examine the application of sophisticated machine learning methodologies, such deep learning and reinforcement learning, to enhance the precision and efficiency of intrusion detection systems. Overall, the field of machine learning and intrusion detection based on smart contracts has enormous potential to transform cybersecurity in decentralized systems in the future. Through the consideration of the previously described factors and the adoption of continuous technological progress and cooperation, institutions can construct robust and flexible security systems that are able to repel dynamic cyberattacks in the decentralized environment.

REFERENCES

[1]. A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. P. Mahmud, M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," IEEE Access, vol. 8, pp. 209 594–209 609, 2020.

[2]. A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescape, M. Hasan, M. Sookhak, and A. Mosavi, "Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot," IEEE Access, vol. 9, pp. 28 361–28 376, 2021.

[3]. E. Oughton, G. Geraci, M. Polese, and V. Shah, "Prospective evaluation of next generation wireless broadband technologies: 6g versus wi-fi 7/8," Available at SSRN 4528119, 2023.

[4]. A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, and B. Minaei-Bidgoli, "Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management," IEEE Access, vol. 8, pp. 140 008–140 018, 2020.

[5]. L. G. Giordano, G. Geraci, M. Carrascosa, and B. Bellalta, "What will wi-fi 8 be? a primer on ieee 802.11 bn ultra high reliability," arXiv preprint arXiv:2303.10442, 2023.

[6]. M. T. Ahmed, R. Islam, M. A. Rahman, M. J. Islam, A. Rahman, and Kabir, "An image-based digital forensic investigation framework for crime analysis," in 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM). IEEE, 2023, pp. 1–6.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

[7]. M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, "Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3850–3864, 2022.

[8]. A. Rahman, C. Chakraborty, A. Anwar, M. Karim, M. Islam, D. Kundu, Rahman, S. S. Band et al., "Sdn–iot empowered intelligent frame-work for industry 4.0 applications during covid-19 pandemic," Cluster Computing, vol. 25, no. 4, pp. 2351–2368, 2022.

[9]. A. Rahman, U. Sara, D. Kundu, S. Islam, M. J. Islam, M. Hasan, Rahman, and M. K. Nasir, "Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture," International Journal of Advanced Computer Science and Applications, vol. 11, no. 9, 2020.

[10]. M. J. Islam, A. Rahman, S. Kabir, A. Khatun, A. Pritom, and Chowdhury, "Sdot-nfv: A distributed sdn based security system with iot for smart city environments," GUB Journal of Science and Engineering, vol. 7, pp. 27–35, Jul. 2021.

[11]. A. Rahman, K. Hasan, D. Kundu, M. J. Islam, T. Debnath, S. S. Band, and N. Kumar, "On the icn-iot with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," Future Generation Computer Systems, vol. 138, pp.61–88, 2023.

[12]. A. Rahman, M. Rahman, D. Kundu, M. R. Karim, S. S. Band, and M. Sookhak, "Study on iot for sars-cov-2 with healthcare:present and future perspective," Mathematical Biosciences and Engineering, vol. 18, no. 6, pp. 9697–9726, 2021.

[13]. H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, 2013.

[14]. S. Axelsson, "Research in intrusion-detection systems: A survey," Tech-nical report 98–17. Department of Computer Engineering, Chalmers . . . , Tech. Rep., 1998.

[15]. M. Appel and I. S. Guenther, "Wpa 3-improvements over wpa 2 or broken again?" Network, vol. 7, pp. 1–4, 2020.

[16]. M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd," in IEEE Symposium on Security & Privacy (SP). IEEE, 2020.

[17]. K. I. Qureshi, L. Wang, L. Sun, C. Zhu, and L. Shu, "A review on design and implementation of software-defined wlans," IEEE Systems Journal, vol. 14, no. 2, pp. 2601–2614, 2020.

[18]. R. Saini, D. Halder, and A. M. Baswade, "Rids: Real-time intrusion detection system for wpa3 enabled enterprise networks," in GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, 2022, pp. 43–48.

[19]. K. A. Adbeib, "Comprehensive study on wi-fi security protocols by analyzing wep, wpa, and wpa2," African Journal of Advanced Pure and Applied Sciences (AJAPAS), pp. 385–402, 2023.

[20]. H. I. Bulbul, I. Batmaz, and M. Ozel, "Wireless network security: comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security proto-cols," in Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, 2008, pp. 1–6.

[21]. A. Halbouni, L.-Y. Ong, and M.-C. Leow, "Wireless security proto-cols wpa3: A systematic literature review," IEEE Access, vol. 11, pp. 112 438–112 450, 2023.

[22]. D. Kundu, M. M. Rahman, A. Rahman, D. Das, U. R. Siddiqi, M. G. R. Alam, S. K. Dey, G. Muhammad, and Z. Ali, "Federated deep learning for monkeypox disease detection on gan-augmented dataset," IEEE Access, 2024.

[23]. A. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, "Distblocksdn: A distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities," in 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019, pp. 1–6.

[24]. N. Dalal, N. Akhtar, A. Gupta, N. Karamchandani, G. S. Kasbekar, and J. Parekh, "A wireless intrusion detection system for 802.11 wpa3 networks," in 2022 14th International Conference on COMmunication Systems NETworkS (COMSNETS), 2022, pp. 384–392.

[25]. H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer networks, vol. 31, no. 8, pp. 805–822, 1999.

[26]. C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for wi-fi and wpa3," Electronics, vol. 7, no. 11, p. 284, 2018.

[27]. N. Dalal, N. Akhtar, A. Gupta, N. Karamchandani, G. S. Kasbekar, and J. Parekh, "A wireless intrusion detection system for 802.11 wpa3 networks," in 2022 14th international conference on COMmunication systems & NETworkS (COMSNETS). IEEE, 2022, pp. 384–392.

[28]. F. S. Alsharbaty and Q. I. Ali, "Smart electrical substation cybersecurity model based on wpa3 and cooperative hybrid intrusion detection system (chids)," Smart Grids and Sustainable Energy, vol. 9, no. 1, p. 11, 2024.

[29]. A. A. Bhutta, M. u. Nisa, and A. N. Mian, "Lightweight real-time wifi-based intrusion detection system using lightgbm," Wireless Networks, vol. 30, no. 2, pp. 749–761, 2024.

[30]. D. Koutras, P. Dimitrellos, P. Kotzanikolaou, and C. Douligeris, "Auto-mated wifi incident detection attack tool on 802.11 networks," in 2023 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2023, pp. 464–469.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

[31]. M. Thankappan, H. Rifa`-Pous, and C. Garrigues, "A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected wi-fi networks," IEEE Access, 2024.

[32]. R. Saifan, M. Radi, H. Al-Dabbagh, and B. Mansour, "A lightweight log-monitoring-based mitigation tool against wlan attacks," 2023.

[33]. B. Kishiyama, J. Guerrero, and I. Alsmadi, "Security policies automation in software defined networking," Available at SSRN 4384690, 2023.

[34]. S. L. Qaddoori and Q. I. Ali, "An efficient security model for industrial internet of things (iiot) system based on machine learning principles," Al-Rafidain Engineering Journal (AREJ), vol. 28, no. 1, pp. 329–340, 2023.

[35]. K. Uszko, M. Kasprzyk, M. Natkaniec, and P. Chołda, "Rule-based system with machine learning support for detecting anomalies in 5g wlans," Electronics, vol. 12, no. 11, p. 2355, 2023.

[36]. D. S. M. Narayana, S. B. Nookala, S. Chopra, and U. Shanmugam, "An adaptive threat defence mechanism through self defending network to prevent hijacking in wifi network," in 2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS). IEEE, 2023, pp. 133–138.

[37]. K. Stella, M. Menaka, C. S. Kumar, A. P. Xavier, and H. Sarvesh, "Detection of hotspot spoofing by monitoring network traffic," in 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). IEEE, 2023, pp. 794–800.

[38]. S.-E. Mansour, A. Sakhi, L. Kzaz, and A. Sekkaki, "Enhancing security mechanisms for iot-fog networks," Journal of Robotics and Control (JRC), vol. 5, no. 1, pp. 152–159, 2024.

[39]. S. Islam, U. Sara, A. Kawsar, A. Rahman, D. Kundu, D. D. Dipta, A. R. Karim, and M. Hasan, "Sgbba: An efficient method for prediction system in machine learning using imbalance dataset," International Journal of Advanced Computer Science and Applications, vol. 12, no. 3, 2021.

[40]. A. Rahman, M. S. Hossain, G. Muhammad, D. Kundu, T. Debnath, Rahman, M. S. I. Khan, P. Tiwari, and S. S. Band, "Federated learning-based ai approaches in smart healthcare: concepts, taxonomies, challenges and open issues," Cluster computing, vol. 26, no. 4, pp. 2271– 2311, 2023.

[41]. S. I. Khan, A. Shahrior, R. Karim, M. Hasan, and A. Rahman, "Multinet: A deep neural network approach for detecting breast cancer through multi-scale feature fusion," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 8, pp. 6217–6228, 2022.

[42]. T. Debnath, M. M. Reza, A. Rahman, A. Beheshti, S. S. Band, and Alinejad-Rokny, "Four-layer ConvNet to facial emotion recognition with minimal epochs and the significance of data diversity," Scientific Reports, vol. 12, no. 1, p. 6991, dec 2022. [Online]. Available: https://www.nature.com/articles/s41598-022-11173-0

[43]. M. S. I. Khan, A. Rahman, T. Debnath, M. R. Karim, M. K. Nasir,S. Band, A. Mosavi, and I. Dehzangi, "Accurate brain tumor detection using deep convolutional neural network," Computational and Structural Biotechnology Journal, vol. 20, pp. 4733–4745, 2022.

[44]. A. Rahman, A. Montieri, D. Kundu, M. Karim, M. Islam, S. Umme, Nascita, A. Pescape´ et al., "On the integration of blockchain and sdn: Overview, applications, and future perspectives," Journal of Network and Systems Management, vol. 30, no. 4, pp. 1–44,

[45]. A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and Tiwari, "Towards a blockchain-sdn-based secure architecture for cloud computing in smart industrial iot," Digital Communications and Networks, vol. 9, no. 2, pp. 411–421, 2023.

[46]. A. I. Udoy, M. A. Rahaman, M. J. Islam, A. Rahman, Z. Ali, and Muhammad, "4sqr-code: A 4-state qr code generation model for increasing data storing capacity in the digital twin framework," Journal of Advanced Research, 2023.

[47]. A. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom, and M. Razaul Karim, "Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network," in 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1–6.

[48]. A. Rahman, M. J. Islam, M. R. Karim, D. Kundu, and S. Kabir, "An intelligent vaccine distribution process in covid-19 pandemic through blockchain-sdn framework from bangladesh perspective," in 2021 Inter-national Conference on Electronics, Communications and Information Technology (ICECIT), 2021, pp. 1–4.

[49]. A. Rahman, M. A. H. Wadud, M. J. Islam, D. Kundu, T. A.-U.-H. Bhuiyan, G. Muhammad, and Z. Ali, "Internet of medical things and blockchain-enabled patient-centric agent through sdn for remote patient monitoring in 5g network," Scientific Reports, vol. 14, no. 1, p. 5297, 2024.

[50]. A. Rahman, J. Islam, D. Kundu, R. Karim, Z. Rahman, S. S. Band, Sookhak, P. Tiwari, and N. Kumar, "Impacts of blockchain in software-defined internet of things ecosystem with network function virtualization for smart applications: Present perspectives and future directions," International Journal of Communication Systems, p. e5429, 2023.

[51]. M. Hasan, A. Rahman, M. R. Karim, M. S. I. Khan, and M. J. Islam, "Normalized approach to find optimal number of topics in latent dirichlet allocation (lda)," in Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Springer, 2021, pp. 341– 354.

[52]. K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabir, "Preventive determination and avoidance of ddos attack with sdn over the iot networks," in 2021 International Conference on Au-tomation, Control and Mechatronics for Industry 4.0 (ACMI), 2021, pp. 1–6.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2149

[53]. A. Rahman, K. Hasan, and S. Jeong, “An enhanced security architecture for industry 4.0 applications based on software-defined networking,” in 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), 2022, pp. 2127–2130.

[54]. A. Rahman, T. Debnath, D. Kundu, M. S. I. Khan, A. A. Aishi, Sazzad, M. Sayduzzaman, and S. S. Band, “Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities,” AIMS Public Health, vol. 11, no. 1, pp. 58–109, 2024.

[55]. M. A. Rahaman, K. U. Oyshe, P. K. Chowdhury, T. Debnath, A. Rahman, and M. S. I. Khan, “Computer vision-based six layered convneural network to recognize sign language for both numeral and alphabet signs,” Biomimetic Intelligence and Robotics, vol. 4, no. 1, p. 100141, 2024.

[56]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the kdd cup 99 data set,” in 2009 IEEE symposium on computational intelligence for security and defense applications. Ieee, 2009, pp. 1–6.

[57]. S. N. Nobel, M. A. H. Wadud, A. Rahman, D. Kundu, A. A. Aishi, Sazzad, M. Rahman, M. A. Imran, O. F. Sifat, M. Sayduzzaman et al., “Categorization of dehydrated food through hybrid deep transfer learning techniques,” Statistics, Optimization & Information Computing, 2024.