Journal of Intelligent Systems and Internet of Things
Vol. 12, No. 01, PP. 110-128, 2024
DOI: https://doi.org/10.54216/JISIoT.120109

Zero Trust-Based Blockchain Based IoT Security with Consensus and Access Control Framework

Ahmad Raza Khan*

Information Technology Department, College of Computer and Information Sciences, Majmaah University, AlMajmaah, 11952, Saudi Arabia

Emails: ar.khan@mu.edu.sa

Abstract

As the Internet and computer technology develop, more gadgets are linked wirelessly, expanding the Internet of Things (IoT). IoT is a huge network of sensors and gateways that links them. IoT devices generate images, music, video, digital signals, and more by interacting with their surroundings. To exchange resources and information, all IoT equipment and apps may connect to the Internet. Everything is connected in our world. Due to the broad deployment and massive size of IoT devices, access control of device resources is problematic. Obtaining IoT device resources unlawfully will have major implications since they include personal and sensitive information. Many systems and situations employ access control technologies to secure resources. Discriminatory, identity-based, and MAC access control schemes are traditional (mandatory access control). However, these centralized methods have single-point failure, scalability issues, poor dependability, and low throughput. IoT devices may belong to several organizations or people, be mobile, and function badly, making centralized access management problematic. Another innovative data management solution is blockchain, which uses distributed storage to stabilize data. A transaction writes the data reading or modification record into a block, and the blocks are connected as a chain using a hash to maintain data integrity. It synchronizes data between nodes via a peer-to-peer network and consensus process, assuring data consistency for blockchain network participants. Zero Trust-Based Blockchain, an open source blockchain development platform, offers more efficient consensus methods, larger throughputs, smart contracts, and support for different organizations and ledgers. Proposed work build the fabric-IoT access control system using Zero Trust-Based Blockchain to apply blockchain technology to IoT access control in this study. Distributed processing and storage for IoT data may solve these critical issues with blockchain. Thus, developing distributed IoT-based e-healthcare services using blockchain technology may have been feasible. FabricIoT can keep records, handle dynamic access control, and solve the IoT access control problem using distributed architecture.

Received: August 19, 2023 Revised: November 19, 2023 Accepted: February 26, 2024

Keywords: Blockchain; Zero Trust Architecture; Control Framework; Security; Internet of Things.

1. Introduction

Computing advances have made the Internet of Things (IoT) important to most people's everyday life. Based on the Internet of Computers, the Internet of Things connects anything that can be linked to the Internet using defined protocols employing GPS, RFID, and infrared sensors. We study intelligent identification, monitoring, management, localization, tracking, and constructing an innovative Internet that spans the globe and provides all types of information services [1] for joining the supply chain. The Internet of Things allows data collection and transmission from various sources. IoT applications include smart grids and healthcare networks. The numerous portions of the system are out of sync in time, making information flow and system performance difficult. It's important to upload a patient's real-sequential cords system to a server in sequence. If the medical personnel obtained the incorrect information, it may be costly and troublesome. What has been mentioned shows that Io T [2] requires a universal system time to collaborate. Time synchronisation methods vary, but most concentrate on accuracy and speed [3].

However, few consider security during time synchronisation. These issues are genuine and difficult to answer in the open IoT ecosystem since so many nodes and devices might be targeted. Because they can't verify messages, certain regular nodes may synchronise time [4] incorrectly. We can't determine whether the communications are legitimate. The network would get the erroneous time from these usual nodes, making matters worse. This means that even a few of malicious nodes may disrupt the network's ability to maintain precise time. As a result, there must be a reliable method for the timekeeping of IoT systems [5]. A few different approaches have been considered for this topic, and the present best practises are based on all of them. We investigate and evaluate a method that, like the flooding time.

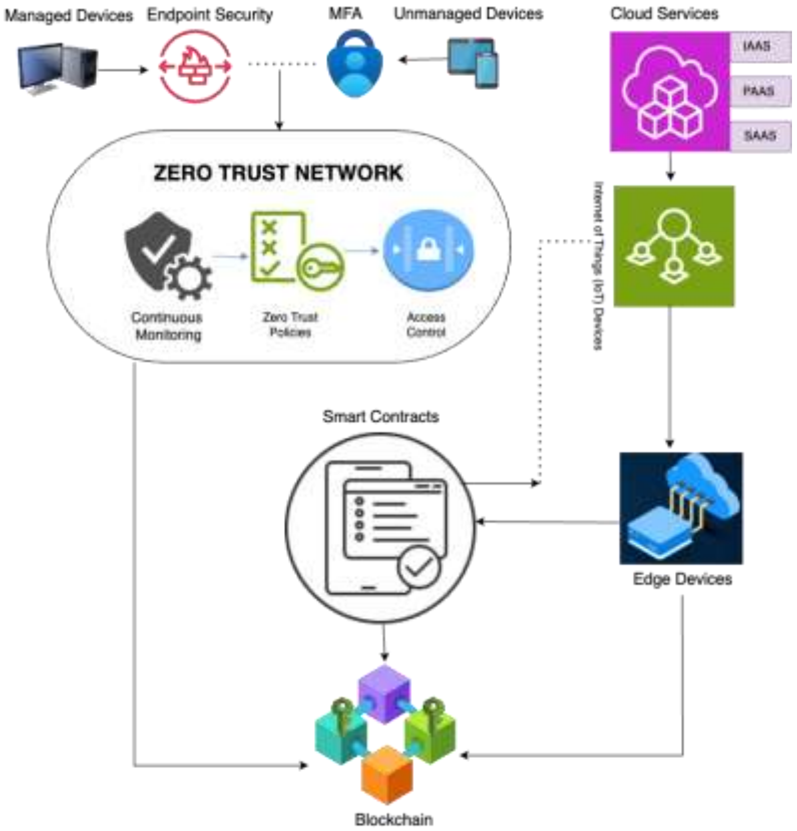

Figure 1: Basic Structure of IoT Security with Zero Trust Access Control Framework

In Figure 1 we can see the Zero Trust Access Control Framework, which is the foundation of Internet of Things security. All the centralised protocols [6] in this system use the same set of reference nodes. To be more precise, the time source is at the absolute bottom of the hierarchy. Data packets in a tree structure are sent by the time source to the nodes that are its offspring. On the other hand, assaults on nodes, particularly reference nodes, might render such designs useless. The subsequent nodes may have the inappropriate characteristics if the time synchronisation fails. Another option for achieving global time synchronisation in a distributed system is to employ several protocols.

Network nodes may keep the whole system in sync by sharing information when they are near to one another. Conversely, in distributed networks, it is guaranteed that any node may communicate with its neighbour. In contrast to tree networks, which are limited to bidirectional communication, this is a definite advantage. Because changing the number of nodes in the graph does not alter the system's behaviour or need additional effort, such as re-building the tree, this technique is robust and scalable. Decentralized networks, on the other hand, conceal the timetable [7]. As a result, we lack certainty about it. As soon as one node modifies the system time, every other node will experience a discordant state.

Research investigating the potential use of blockchain technology as a foundational layer to guarantee correct time synchronisation on the Internet of Things is underway (IoT). Malicious nodes cannot alter the error time to coincide with the rest of the network since the technology behind the blockchain cannot be altered or disrupted. Thanks to the distributed ledger, each node in the network may begin syncing its own time, and each node can independently ensure that the time it uses is accurate. There's no other method to ensure accurate time synchronisation than this. Verification is required of all nodes [8] seeking to join a consortium blockchain. The intricate machinery of time travel functions without a hitch. Utilizing a blockchain ensures security regardless of the nature of the device requiring time synchronisation. This holds true because malicious actors are unable to alter the block chain. Identifying the specific nodes responsible for the error time is an important part of our study. Finding a solution to this issue is comparable to finding a way to prevent rogue nodes from propagating error time [9]. A request to log all blockchain-based user device interactions and reach consensus among all nodes was implemented on top of the framework. All these links are recorded in transactions.

Why? Because the sensor device's RAM and storage capacity are somewhat limited. It's simple to replicate. Due to this, the sensor device struggles to consistently carry out security activities that need a high level of expertise. You may sort authorised loT nodes and prohibit access to dangerous or malicious node-active devices using the blockchain verification [9] and compromise methods. Data gathered and stored centrally via the Internet of Things (IoT) poses privacy and security risks due to the centralization of information about people's lives and jobs. If there is a data breach involving the central database or if the government or manufacturers get access to specific backdoors, these organisations may unlawfully gather information about users without their consent [10]. examine users' devices and maybe gain control of them.

Customers' rights and interests are jeopardised when a firm prioritises profit before consumer consent. When a manufacturer sells user data to other parties without their consent, it is engaging in this practise. Because all nodes are online at the same time and data is encrypted throughout, the distributed ledger known as the blockchain does not need a governing body. In addition to being prohibitively costly, centralised databases can squander precious processing and storage resources. It could take a long time to discover the erroneous node among hundreds of millions of them when an estimate fails. Centralized networking is already used by the majority of existing Internet of Things systems. The cost and storage capacity of a single massive server or centralised cloud reach their limitations when hundreds of millions of nodes are linked to it.

The principles of confidentiality and security should underpin every data system. We state that in order for a system to be considered secure, it must adhere to the three IAC requirements: availability, privacy, and integrity.

Having secure, fast access to a wealth of comprehensive, current patient records. Improvements in patient care and better collaboration across disciplines are both brought about by the standardisation of medical records and the introduction of innovative medical technology [11]. Expert medical advice, quicker diagnosis, and easier access to visiting doctors are a few advantages. Thanks to improvements in patient information management, documentation, and duplication, less hours are lost trying to find standardised notes, x-rays, information on admission or release, and other kinds of paperwork.

Management of assets: When doing business on a global scale, the risks and costs of quality management in conventional operations become much more apparent. Since the blockchain's ledger is composed of encrypted data, errors are less likely to occur, which is particularly important when these stages require dealing with foreign money. Making international payments is notoriously complicated, costly, and cash-friendly when it comes to transactions. International money transactions could take a few days, or more, to complete. Many businesses are now developing blockchain-based solutions; examples are bits Park and abra. There are a lot of new services and apps coming out of the Internet of Things (IoT), but all of them rely on a core set of standards, protocols, architecture, and security measures.

The structure of paper is as follows; section 2 includes literature survey; section 3 includes methodology of proposed work; section 4 includes experimental results and analysis; section 5 includes conclusion and Future work.

2. Literature Survey

Wireless multi-hop networks are vulnerable to a variety of security threats, including wormhole attacks, black hole attacks, grey hole attacks, among others [12], since an attacker may theoretically gain control of some of the devices that make up the network. Every node in an IoT network affects the wireless multi-hop network's security in its own unique way, which is an often-overlooked aspect [4]. Aggressive nodes in a wireless multi-hop network may launch a Gray Hole Assault (GHA) or Selective Forwarding Attack when they act together. Finding and countering this assault is also not easy. In a grey hole attack, an infected or malicious upstream node selectively discards incoming packets instead of sending them on to the next hop. As an alternative to transmitting the packets to the node further downstream, this is carried out. Even in the absence of an attack, wireless channels could suffer unexpected packet loss because of medium and MAC collisions [13]. Whether the channel is utilized alone or not, this is still the case. Consequently, differentiating GHA from regular packet loss is not a simple task. Since we are supposing that the buffer is big enough to accommodate all of the nodes, it cannot overflow.

When just one node's packets are deliberately destroyed, a variant of the Gray Hole Attack known as the Selective Gray Hole Attack becomes more challenging (SGHA). A Byzantine assault follows [14]. An insider may take complete control of a legitimate node or nodes in a network using a Byzantine attack. The perpetrator may cause the system to eventually crash by reprogramming these nodes to do harmful actions that disrupt the network's initial purpose. The foundation of any multi-hop network is the security and privacy of the data sent between devices. First proposed in the Byzantine general’s problem [15] was the notion of a Byzantine war. In this issue, a gang of betraying generals plot to prevent the loyal generals from reaching a consensus to forward their own agenda. When even a small number of valid nodes start acting contrary to the intended function of the network, this is known as a Byzantine assault.

There is some effort on GHA, but much of it goes toward finding malicious rogue nodes that act the same way for all data flows, regardless of where they come from or go to. Some studies have looked at the idea that GHA could be reliant on the contents of packets, for instance [17]. Degradation of network performance by systematic packet rejection is widely believed to be the principal goal of a GHA attacker in the extant research.

In this case, we will use a classic Byzantine tactic to defeat GHA. Our enemy A is going to be rational and organized, with a goal in mind and a strategy to achieve it. If A has proprietary information about the victim, they will choose them in a way that allows them to reap the most benefit with the least amount of effort. This proves that the attacker isn't aiming to hamper the network's performance per se, and that not every node in A might be a victim. As a result, we go over one-use case of the GHA in which the infected node is only harmful for specified data flows (s). So far, GHA detection systems have either missed the attack entirely or missed it when the packet loss rate was far lower than typical (when packet drop rate is higher than normal packet drop rate). Since the usual reaction to a classic GHA attack is to remove the offending node, distinguishing between the two types of GHA is essential. Without node-side malicious behaviour in each data flow, this would be pointless and lead to underutilization of resources. Therefore, it is guaranteed that nodes that were not hit by the attack will keep their QoS properties, including latency, throughput, and others. The GHA takes use of the fact that all nodes near a malicious node are victims [18], but this kind of attack is simple to notice as it targets only one data flow or a small subset of data flows. In addition to the fact that deleting a packet is simpler than forwarding it, this might be the trigger for an attack to be conducted from a compromised node. For a hacked node, using its resources to conduct a GHA would be pointless. Instead, the node may save some resources by rejecting the packet.

When a node only utilizes packets from a certain source node to execute GHA, we provide a possible method in this work that might identify and stop an attack [19]. Instances where criterion-based GHA might be used include attacks on packets end route to certain nodes (such the gateway) or on packets in transit between specific pairs of nodes. It is possible to make the approach more general such that it can detect any GHA given certain conditions. The nodes may be able to mix the attack into the backdrop by performing GHA at random intervals, making it difficult to observe. This form of attack has the potential to interrupt a target node’s connection discreetly and rapidly.

The home network may link to several appliances and fixtures. Doorways, windows, fans, table lamps, and ceiling lights are all part of this category. Two separate pathways, A and B, are shown in the data flow diagram. A path begins at the entrance, while B begins at a ceiling light. Presumably, the hacked red-colored network node would selectively remove A-related traffic. When trying to identify attacks, all the previously revealed GHA detection methods have taken the data forwarding rate per node into consideration. In this case, the compromised node's data forwarding rate shouldn't be impacted by losing a small percentage of packets in any particular flow. Since the damaged corridor links the main entrance to the front door, the property is at risk if no one reports the incident.

When the military employs a reconnaissance programme, such an occurrence is not out of the question. By limiting the assault to nodes inside a certain zone, an attacker might more easily approach the zone from the direction of the victim. An entire nation's security might be jeopardized by this. An analogous approach would be to selectively disable alert signals from certain zones in smart inventory tracking or disaster warning systems, or to disable just the trigger signal required to activate a mission-critical application, in the event that a situation requiring immediate attention has a catastrophic effect. A few examples of wireless multi-hop networks that could be vulnerable to these kinds of assaults include those used for home automation, defence, electronic health records, smart warehouses, autonomous vehicle networks, and any other system that keeps information unique to individual nodes. Consequently, we must act quickly to identify these assaults and secure the system.

An ally commits a promotion attack when they persistently devalue a node's reputation score, irrespective of the node's actions [20]. A downgrade attack occurs, on the other hand, when an ally gives a node a high reputation score despite the node's negative behaviour. Hackers may use the collusion strategy of demoting or elevating another node to conceal the harmful behaviour of a compromised node. It is possible that certain algorithms can keep running properly even when there is widespread collusion. To see how well the algorithm works in a wireless multi-hop network, we put it through its paces on the OMNeT++ platform. This research expands upon previous work by providing an optimised and enhanced detection system that can swiftly identify GHA regardless of whether the attacker is rational or employs a criterion-based assault [21]. This is one of the outcomes of the study.

If the software detects even a partial penetration of the system, it will be able to accurately identify the attack and the attacker. The reason for this is because the detection mechanism is distinct in that it assigns a reputation score to each data flow. Because this approach is novel, the converse is also true. The suggested method may notify the system of an impending attack and help with the implementation of a mitigation plan that considers QoS. To prevent disastrous data loss, nodes that are geographically near to the gateway are subject to a more rigorous detection method. This is the reason for our focus on these instances inside a GHA that are happening on a network with one hop:

An adequate degree of trust between all IoT components is essential for the network's successful operation. Most of the time, people don't care about how each device affects the security of the multi-hop network. Due to the presence of insecure devices linked to these networks, they are susceptible to many types of assaults. Among all those susceptible devices, SGHA is the one that this study is primarily concentrating on. To avoid detection, most of the early GHA investigations employed a fragmented multi-path approach and concentrated only on the attack detection mechanism [22]. Despite how easily the strategy could be put into action, the amount of communication required increased by a large magnitude. If there is only a single attacker on each route, it will fail. A critical step in these kinds of inside attacks—detection of the compromised node—was also missed. An example of a solution proposed by the authors is the watchdog strategy, which entails designating a subset of nodes to keep an eye out for suspicious behaviour in the network to detect hacked nodes. It is possible to observe a forwarding node's actions in two ways: first, by listening in on the data transmissions of nearby nodes; and second, by making use of acknowledgments at the link or network levels.

Table 1 : Comparison of Existing works

Method	**Key Features**	**Limitations**
Traditional Byzantine Strategy	- Adversary (A) is logical and works toward a goal with a plan	- Assumes GHA attacker's primary objective is to degrade network performance
	- A chooses victims based on unique knowledge to maximize benefit or minimize expenditure	- Fails to detect GHA when the packet loss rate is much lower than usual
	- Focuses on specific GHA where the compromised node is malicious only for certain data flows	- Eradicating the offending node is the standard response, leading to resource underutilization
Criterion-Based GHA Detection	- Detects and counters an attack when a node uses packets from a certain source node	- Difficulty in differentiating between conventional GHA and SGHA
	- Can be applied to various situations, such as attacks on specific nodes or between nodes	- Attacks conducted at random intervals might blend into the background, making detection challenging

Watchdog Technique	- Assigns a small group of nodes to monitor the network for signs of abnormal activity	- Increased communication overhead due to the need for multiple nodes to monitor the network
Channel Aware Detection (CAD)	- Considers channel losses in wireless medium during detection and counteraction	- Does not explicitly consider collaboration between nodes
Reputation-Based Algorithms	- Addresses promotion and downgrade assaults, where allies assign reputation scores	- Collusion tactics may be used by attackers to manipulate reputation scores
Smart Contracts in loT Security	- Uses Smart Contracts for access control and mitigation strategies	- Requires a robust blockchain infrastructure; may have scalability challenges with a large number of loT devices
Zero Trust Architecture	- Implements continuous monitoring and entity verification for enhanced	- Implementation complexity; may require significant changes to existing network architectures

The authors introduced a technique called Channel Aware Detection (CAD) in their publication [23]. While detecting and countering the assault, it considered the channel losses which are inherent to a wireless medium, but it did not consider collaboration [24]. They verified receipt of link layer acknowledgments by listening in on downstream nodes' data transfers; this allowed them to draw their conclusion about the upstream nodes.

To prove our system can detect source-centric SGHAs, we construct one that can recognize any kind of criterion-based SGHA. Data flows that originate from a certain source node are the only ones targeted in the source-centric variant of source-centric SGHA. We improved the scheme's detection accuracy by reducing the chance of false alarms and missed detection.

3. Proposed System Model

The suggested project aims to create a new and strong security framework for the Internet of Things (IoT) by combining Zero Trust architecture, Blockchain consensus mechanisms, and smart contract-based access controls. At its core, the system aims to change the way IoT devices are secured by following the ideas of Zero Trust. This means that devices are not automatically trusted and must constantly prove who they are. Adding Blockchain technology creates a decentralised ledger that can't be changed. This solves problems with data integrity and openness in IoT transactions.

When put on the Blockchain, smart contracts are a key part of automating and decentralising access control policies. This makes sure that security rules are followed consistently and openly across the entire IoT ecosystem, reducing the need for centralised systems that can fail in one place. Continuous authentication mechanisms improve overall security by checking the identities of devices on the fly and in real time. This lowers the risk of unauthorised access and possible security breaches.

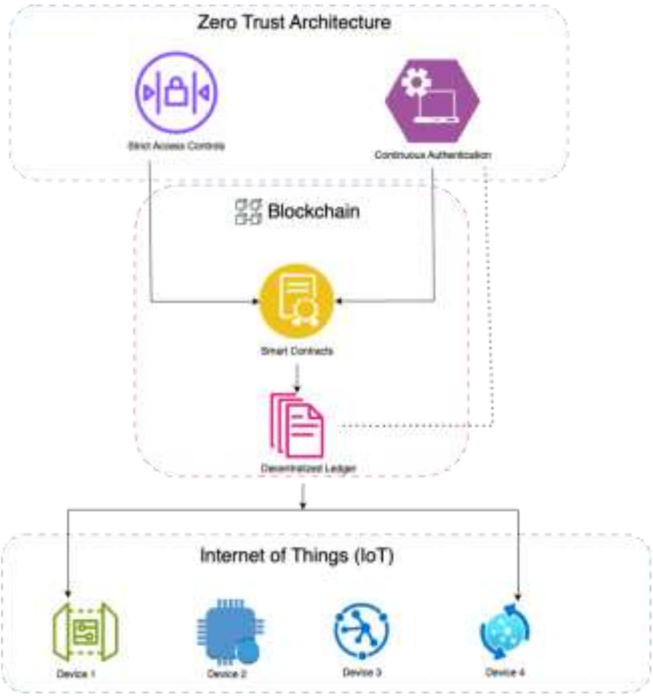

Figure 2: Proposed IoT Security Model

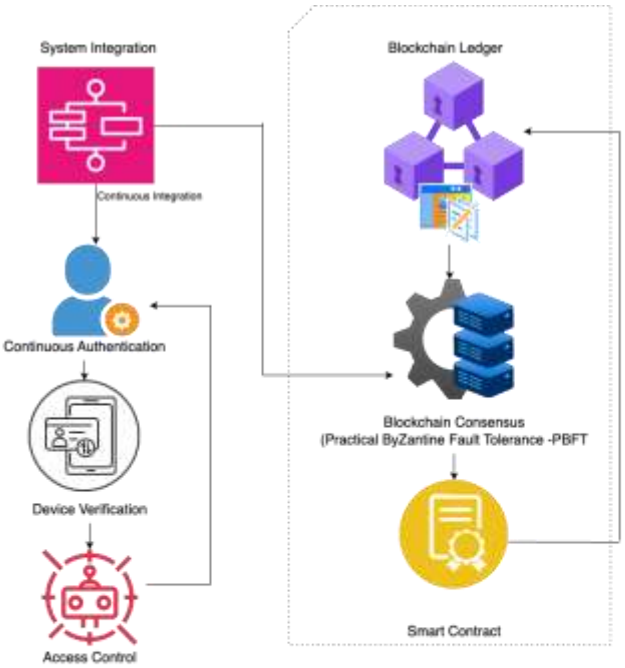

Figure 3: IoT Security with Zero Trust-Based Blockchain Consensus and Access Control

If this proposed system model is used, the IoT landscape will have a better security framework that not only fixes problems but also sets the stage for a security infrastructure that can grow and work with other systems. The spreading of security rules and the addition of ledgers that can't be changed make the IoT ecosystem stronger and better able to handle cyber threats that are always changing.

A. Zero Trust Architecture Integration:

There is no implicit trust in any user, device, or system component in Zero Trust Architecture (ZTA), even if they are inside the network perimeter. For this method to work, there must be constant authentication, strict access controls, and real-time confirmation of device identities. Continuous authentication makes sure that devices' identities are checked all the time as they interact with the loT ecosystem. This uses cryptographic methods and protocols to make sure that devices are real and that they can be trusted.

$$\text{Device-Signature}_{\ t} = \text{Sign (PrivateKey, DeviceData}_{\ t}) \qquad (1)$$

Here, Device-Signature $_{t}$ represents the cryptographic signature generated by the device's private key (PrivateKey) for the current device data (DeviceData $_{t}$) at time$t$. This signature is continually verified to ensure the ongoing authenticity of the device.

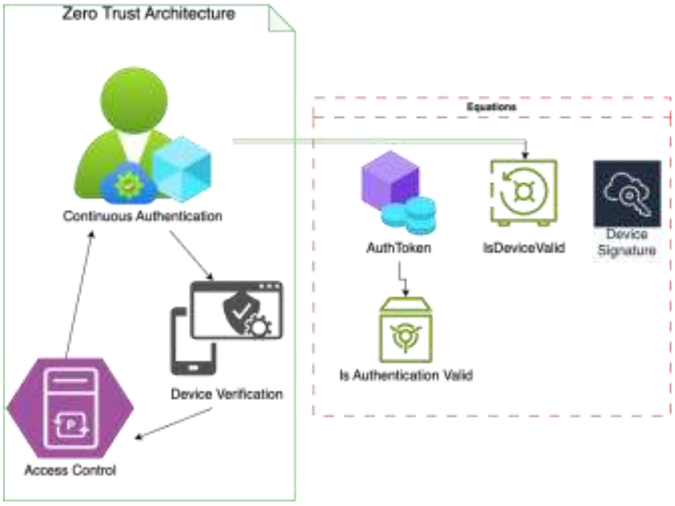

Figure 4: Zero Trust Architecture Model

Zero Trust says that you shouldn't trust any device or user by default, and you should only give access to people who need it. Policy enforcement points evaluate and enforce security policies based on a variety of contextual factors. These points are used to control access.

Device identity verification is the process of constantly checking that a device is who it says it is by looking at its unique features. This process makes sure that a device is who it says it is while it's connected to the loT network.

$$\text{IsDeviceValid}_{\ t} = \text{Verify (PublicKey}_{\text{ Device}}\text{, DeviceSignature}_{\ t}\text{, DeviceData}_{\ t}) \qquad (2)$$

Checking the cryptographic signature of a device using its public key (PublicKe) and the current device data (DeviceData) at time t tells us if the device is valid (IsDeviceValid-t.). When Zero Trust Architecture is used, device identities are constantly checked, decisions about dynamic access control are made, and cryptographic methods are used to make sure that IoT devices are always safe. These equations are basic parts of the Zero Trust principles that are built into the proposed security framework for loT.

$$\text{AuthToken}_{\ t} = \text{HMAC (PrivateKey, DeviceData}_{\ t} || \text{ Timestamp}_{\ t}) \qquad (3)$$

AuthToken, -t, is a time-stamped authentication token that is made by using the device's private key to generate a Hash-based Message Authentication Code (HMAC).

$$\text{(IsAuthenticationValid}_{\ t} = \text{Verify(PublicKey Device}_{\text{ , AuthToken}}\text{ , DeviceData}_{\ t} || \text{ Timestamp}_{\ t}\text{)} \qquad (4)$$

As part of continuous device authentication, the authentication token (AuthToken, -$_{\mathrm{e}}$.) is compared to the device's public key (PublicKe, -Device.), the current device data (DeviceData, -$_{\mathrm{e}}$.), and the timestamp (Timestamp, -$_{\mathrm{e}}$.)..

B. Blockchain Consensus Mechanism

A strong Blockchain consensus mechanism is built into the proposed system to make IoT transactions safer and more open. In a decentralised network, consensus mechanisms are very important for making sure that all nodes agree on what to do. A useful Byzantine Fault Tolerant (PBFT) consensus mechanism, which is often found in permissioned Blockchains, will be built into the proposed system mode.

$$\text{Prepare}_{\text{ Block}} = \text{Sign}\left(\text{ PrivateKey}_{\text{ Node}}\text{ , Hash (PrePrepare Block)}\right) \qquad (5)$$

The nodes in a PBFT consensus mechanism talk to each other to agree on what the state of the Blockchain is. So, even if some nodes are bad or malicious, the majority of them will still reach a consensus..

$$\text{PrePrepare}_{\text{Block}} = \text{Sign}\left(\text{PrivateKey}_{\text{Node}}, \text{Block}_{\text{Data}}\right) \quad (6)$$

During the pre-prepare phase, a node uses its private key to sign the proposed block (Block-Data).

Nodes also sign the hash of the pre-prepared block (PrePrepare Block) during the prepare phase, which shows that they are even more committed to the proposed block.

$$\text{Commit}_{\text{Block}} = \text{Sign}\left(\text{PrivateKe}_{\text{Node}}, \text{Hash}\left(\text{Prepare}_{\text{Block}}\right)\right) \quad (7)$$

$$\text{IsTransactionValid} = \left(\text{Count}\left(\text{Commits}\right) \geq \text{Threshold}_{\text{Consensus}}\right) \quad (8)$$

The transaction's validity (IsTransactionValid) is checked by counting the number of committed signatures (Commits) and comparing it to a consensus threshold that has already been set (Threshold Consensus).

$$\text{CreateBlock} = \text{Concatenate}(\text{Transactions}, \text{Commits}) \quad (9)$$

To make a new Blockchain block (CreateBlock), you need to join together valid transactions and the commit signatures that go with them. To sum up, adding a PBFT consensus mechanism makes sure that transactions are safely checked and added to the Blockchain only when a large enough number of nodes agree. In addition, this makes the proposed system more secure and clear, making it a solid base for safe low-level transactions.

C. Smart Contract-Based Access Control

In the suggested system, smart contract-based access control becomes a key part of making the huge world of the Internet of Things safer (IoT). These smart, self-executing contracts, which live on a decentralised Blockchain, act as digital guardians, following set rules and conditions to control who can use IoT resources. These contracts include equations that describe complex access control policies and decide which devices can access and which ones can't. Event triggers make Blockchain transparent by carefully recording every access granted or denied. This creates a record of decisions that can't be changed and can be checked. The system is based on decentralisation, and decisions about who can access what are made on the Blockchain. Equations make sure that only devices that meet certain requirements can access resources. This makes the whole IoT ecosystem safer. Equations that control time-based or event-triggered revocation make automated access revocation possible. This adds a dynamic layer to the access control framework. Access control can be easily added to the overall IoT security architecture because smart contracts can work with other Blockchain transactions. Once smart contracts are in place, they can't be changed without permission. This makes sure that access control policies stay consistent and reliable over time.

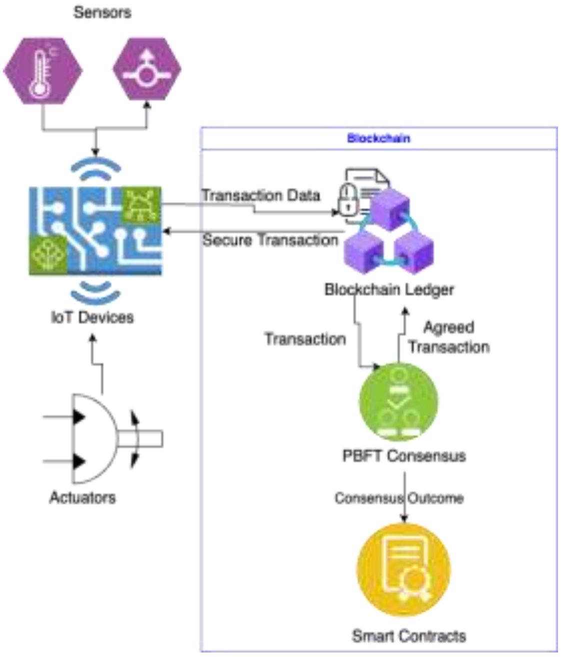

Figure 5: IoT Security with Blockchain Mechanism

When smart contracts are used for access control, they change the way things are thought about by adding programmability, decentralisation, and transparency to IoT security. Equations in these contracts not only write down rules and choices, but they also show how strong and reliable the system is, making it a good way to control who can access the complicated and linked world of the Internet of Things.

AuthorizedDevices [Device] = true (10)

When a smart contract gives access to a device, it sets the corresponding entry in the mapping.

AuthorizedDevices to true..

AuthorizedDevices [Device] = false (11)

require(AuthorizedDevices[msg.sender],"Accessdenied") (12)

emit AccessGranted(Device) (13)

This equation sets off an event that records that access has been granted to a certain device on the Blockchain.

D. Access Control Framework

The Access Control Framework suggested in this system is meant to make controlling access in the Internet of Things (IoT) ecosystem strong and safe. The Zero Trust model used in this framework goes against the usual idea of trust and stresses constant checking and approval for every access attempt. Equations store the basic ideas of Zero Trust and make sure that decisions about access depend on the current verification status of the entity asking for access.

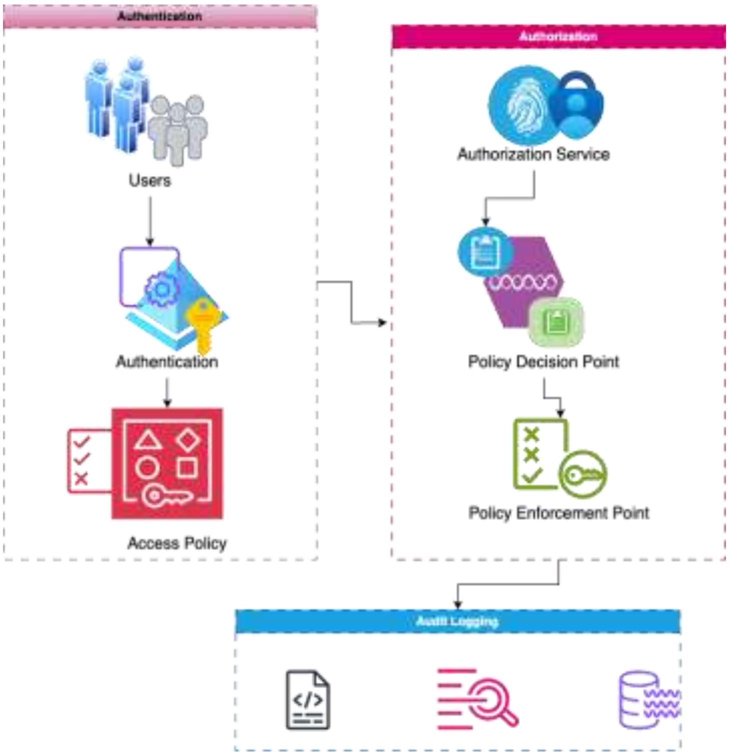

Figure 6: Access Control Framework

Adding Blockchain consensus mechanisms to the framework makes it more stable. Using mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) in consensus equations makes it easier for people across the network to agree on decisions about who can access what. This decentralised consensus makes sure that access decisions can't be changed and are clear because they are recorded safely on the Blockchain.

Smart contracts are a key part of the framework because they put Blockchain access control policies into action. Smart contracts use equations to set rules for giving, taking away, or granting access. This makes access control hard to change and easy to check. Smart contracts use conditional logic to make sure that decisions about access are in line with policies that have already been set.

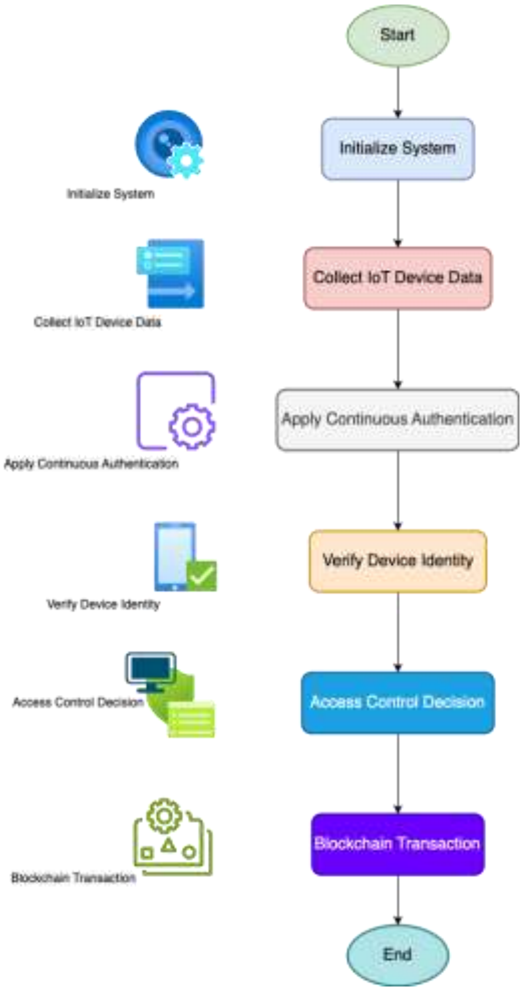

Figure 7: Flowchart of Proposed Work

Once set up on the Blockchain, access policies can't be changed. This gives the Zero Trust model a stable and unchangeable base.

The Access Control Framework is a big change in IoT security because it combines the ideas of Zero Trust with Blockchain's decentralised and impossible to change features. This framework makes sure that access is controlled in a way that is continuous, clear, and reliable in the connected and changing world of the Internet of Things. The study introduces a novel dynamic load-balancing approach integrating deep learning, reinforcement learning, and hybrid optimization techniques to enhance cloud performance. Implemented in Python and CloudSim, the model effectively allocates work between VMs and PMs, resulting in improved resource utilization and shortened makespan. Rigorous assessments affirm its efficacy in optimizing cloud performance under varying workloads and resource conditions.

4.Experimental Results And Analysis

To create a simulation environment remarkably close to actuality we assumed a cooperative CR network with the following parameters nearly following IEEE802.22 standards. The sensing sampling frequency (f_s) is 6Mhz

$$\text{Noise Power } (N_0) = -95.2\text{dBm} \approx 3.01 \times 10^{-13} \text{ watt}$$

$$\text{Signal power } (P) = -116\text{dBm} \approx 2.5 \times 10^{-15} \text{ watt}$$

The number of mobile CRs (N) is a variable considered in different conditions.

The number of sensing events (M) measured before deciding is also considered as a variable in different network conditions.

Frame duration is assumed to be 20 ms

The sensing interval Δt is the same as frame duration assuming one sensing event in

each frame. The velocity of each CR is also considered as a variable to see the impact of it on

sensing. It is also assumed that CRs are not changing their velocity in between two successive.

sensing and they are moving straight. Decorrelation distance (d_{corr}) is 150 m considering.

sub-urban areas. Both homogeneous and heterogeneous CRs are considered for simulation.

A. Simulation Parameters

The Proposed methodologies are used to assess the simulations. Uncoded Bit Error Rate and Normalized Mean Squared Error (NMSE) are used to evaluate the performance. Table 1 displays the parameters used for the simulation. The article discusses the utilization of virtualized multimedia tools for integrating video conferencing solutions into teaching and learning environments. It explores the implementation of these tools to enhance educational experiences, likely focusing on the benefits, challenges, and applications of such technology in educational settings [26]. The experimental results of the proposed method were evaluated using the following metrics: signal-to-noise ratio (SNR) relative to detection probability, throughput, settling time, energy efficiency, detection threshold, number of bands each base station occupied, and bands occupied by each base station individually.

Table 2: Simulation parameters

Parameter	**Measures**
The maximum content time I	2
Total decision round R	100
Maximum Occupancy time k	50,000
Maximum number of the subgroup	4
No of spectrum bands M	100
No of base station N	10
Size of Group	50
LL Limit	1500
GL Limit	50
Perturbation Rate	0.4

B. Throughput Performance

The suggested technique of throughput for different load factors is shown in Figure 8. At a load value of 100%, the x-axis indicates k(hat), while the y-axis indicates 96.0 percent throughput. At a load value of 150 percent, the x-axis indicates k(hat), while the y-axis indicates 96.55 percent throughput. The x-axis shows the dynamic load in kilowatts (hat) and the y-axis shows the throughput percent. Based on these findings, we concluded that the suggested RR algorithm achieves throughput and good trade-off at k=40,000, and it also performs better with load factor.

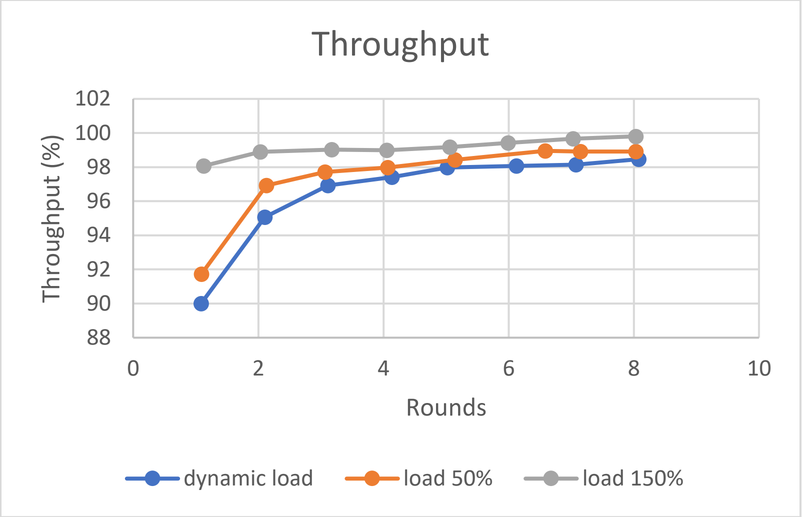

Figure 8: Throughput

C. Settling Time

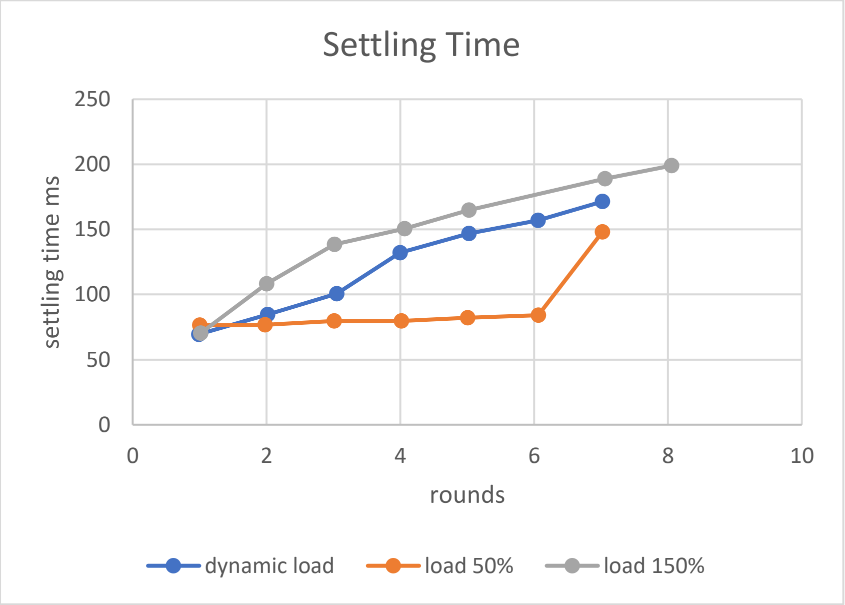

Figure 9: Settling Time

For different load factors, the suggested technique of establishing time performance is shown in Figure 9. The x-axis shows 1 k(hat) and the y-axis shows 70 settling time percent at 100 percent load, 150 percent load shows the same relationship, and dynamic load shows the same relationship with x-axis representing 1 k(hat) and y-axis representing 80 settling time percent. Based on these findings, the suggested RR-based scheduling technique drastically cuts down on settling time by making use of open space bandwidth to lessen interference. The suggested approach was used to attain a settling time of k = 30,000. The settling time performed well under the dynamic load.

D. Energy efficiency

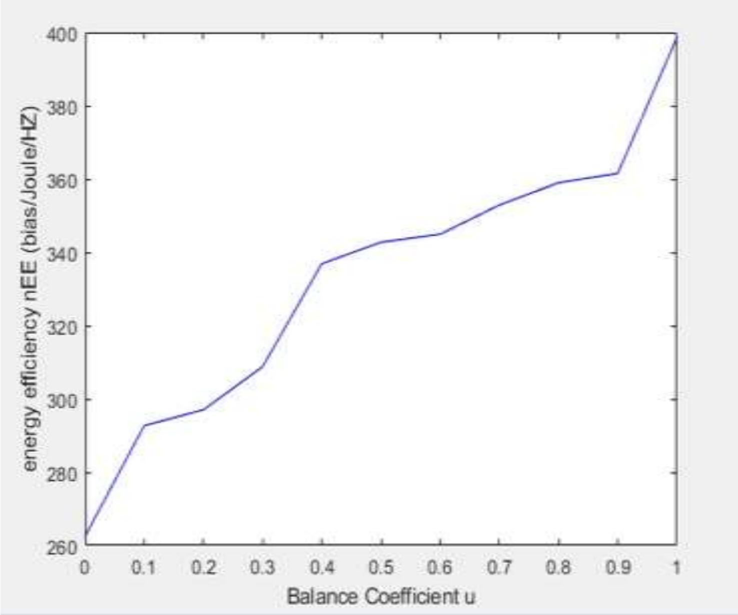

Figure 10: Energy efficiency

Figure 10 shows the energy efficiency performance approach that has been presented. A system's energy efficiency was changed along the X-axis of this image, which is defined by the balancing coefficient u. With no balanced coefficient, the energy-efficient nEE (blasé/Joule/HZ) gives 265 kilowatt-hours, but with one balanced coefficient, it reaches 400 kilowatt-hours.

E. Detection threshold

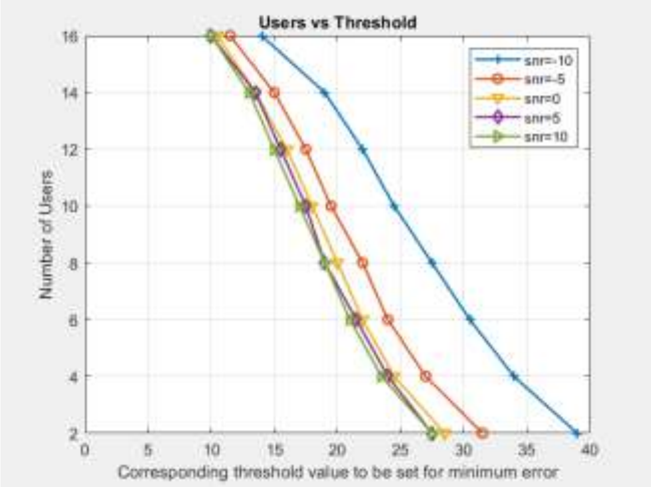

Figure 11: Detection threshold

The energy efficiency of the proposed system is described at the observed threshold value illustrated in Figure 11. The x-axis value represents a full load detection threshold of 129.3, while the y-axis value represents an energy efficiency of 8.7 nEE(bias/Joule/HZ). The detection threshold at full load is shown on the x-axis at 129.3, while the energy efficiency at full load is shown on the y-axis at 8.3. Based on the data, the energy efficiency nEE(bias/Joule/HZ) is 7.6 and the detection threshold is 129.3 at full load (x-axis). The cutoff level for decreased detection at 6 Hz reaches 130.3 dB while operating at full load. Under a 150 percent load, the proposed method reaches 130 dB at 5.8 Hz, and under a dynamic load, it achieves 130 dB at 5.4 Hz, demonstrating its great efficiency.

E.A. Number of bands occupied by BS.

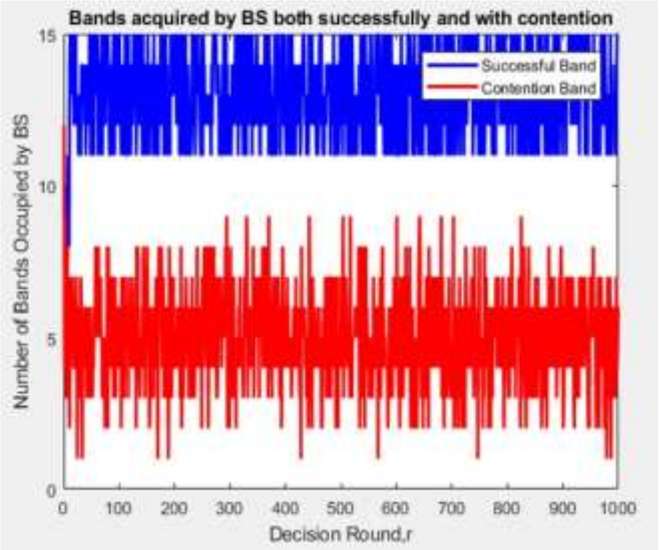

Figure 12: No of successful and contention bands occupied by BS.

As the decision-making round advances, Figure 12 shows the nodes of the successful and contentious bands that NS occupies. Since BS are constantly adding new bands and removing old ones, our investigation confirmed that the number of successfully acquired band BS fluctuated with time. A successful band will use 8–15 bands of BS. As the band in dispute filled out bands 2–7. The BSs prioritizes bands who have achieved success.

E.B. Bands occupied by each BS.

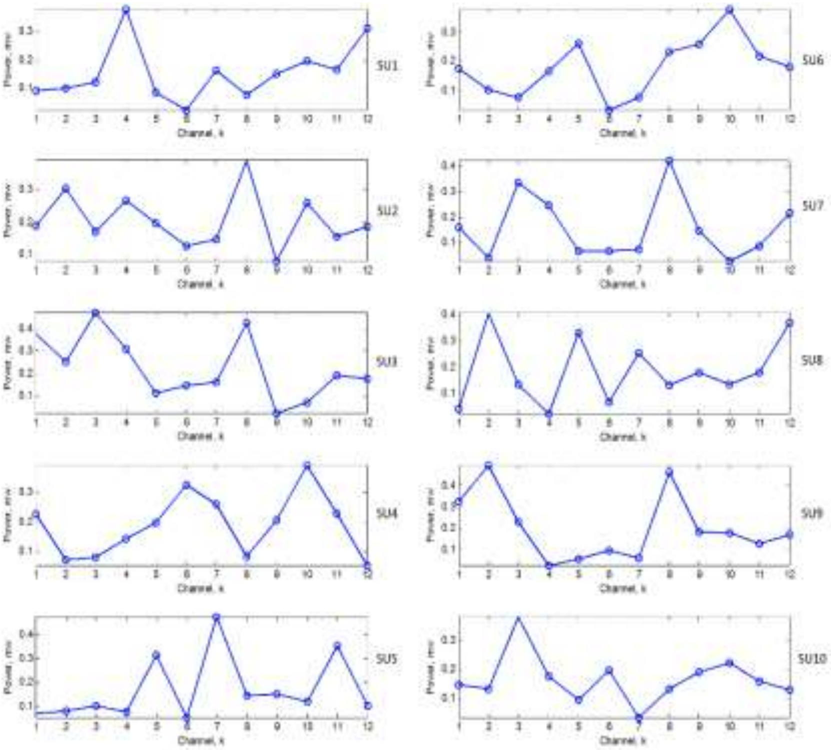

Figure 13 : Analysis of bands occupied by each base station.

Figure 13 shows the total number of bands obtained for each BS. The BS is used to identify the bands that were successfully acquired. The successful band and contention band are determined by evaluating the bands used by each BS. For the perfect centralized system, we calculate Sn, the probability system, and GA learning. For every base station (BS), the central control system distributes the available spectrum bands (M-1) evenly among the N competing BS, yielding 9.9 bands (Sn - (M-1)/N). The BS evaluates spectral bands with a probability of 88 (Sn = 88). The number of spectrum accesses per BS in the GA learning example is S= 5.85. The suggested opportunistic method distributes M = 100 existing bands evenly across BS, bringing it extremely close to the central system's value. Because the method is dispersed, the Sn difference is algorithm dependent. Both opportunistic and centralized methods have about the same Sn value. While GA learning gets a minimum of 5.85 by bands among all BS, probabilistic learning gets a minimum of 88. The impact of a severe collision cannot be mitigated by either approach. Activated PUs with a spectrum license are evaluated for the proposed system's resilience and flexibility based on predicted testing findings.

Therefore, CRN makes use of the reduced spectrum bands. The article presents a study on establishing a secure Platform as a Service (PAAS) environment over a hybrid cloud infrastructure by employing load-balanced Docker containers. It likely discusses the implementation of Docker containers to enhance security and scalability in a PAAS environment deployed over a hybrid cloud setup. The study may cover topics such as container orchestration, load balancing techniques, and security measures aimed at ensuring robust and efficient operations within the hybrid cloud environment [27].

5. Conclusion

In conclusion, the proposed work introduces a comprehensive security framework for the Internet of Things (IoT) by leveraging the principles of Zero Trust architecture, Blockchain consensus mechanisms, and a sophisticated access control framework. Sharing hazard intelligence figure amongst systems enables collective security approach to improve a much more comprehensive understanding of existing and prospective threats. Traditional authentication principles are extended to include data access control. The existing confidentiality provided by existing web pages are insufficient to ensure safety. This was primarily because many users were merely unaware of the problems that were resting to be utilized by an intruder. As a result, our blueprint was to create a security tool to create a guide system that was accessible to all users. The application validated whether the user implemented properly, the numerous types of methods using various lists such as the app two - step checking system. The proposed RTASS system was utilized to develop security models at network layer and application layer. The RTASS network model could be developed using machine learning techniques to identify securing attacks and RTASS application layer model was developed using secure authentication and data transmission of lo T device data. Following conclusions were observed in this work: Attack detection in IoT is a critical task for maintaining the safety of Internet of Things traffics. Several researchers had been using machine ML techniques to follow and stop suspicious IoT traffic in recent years. However, in the existence of inadequate characteristics, these Machine Learning frame works cause misclassification as well as time difficulty during the educational experience. This significant issue had to be addressed by creating a framework for ideal and exact characteristics segment from malignant IoT traffics. For this purpose, a new framework, model has been proposed. To begin, the RTASS network security framework proposed a feature selection approach that combined ranking based chi-square, Correlation analysis by Pearson, and co-relation in score to retrieve relevant attributes from across all set of data. These would be clustering methods that purify out descriptors extra smoothly and quickly. Traditional authentication ideas would be extended in the future to monitor and identify information as it is handled by distributed platforms. They'll be creating quite well usage restrictions to ensure privacy characteristic features across large amounts of data while enabling classifier techniques to function then assessments on the way to run on the upper. Internet of thing (IoTs) As extra information is together transported and evaluated over unified platform; Application contextual factors will progress appropriate practical capabilities to try to enforce adequate safety restrictions. As the IoT continues to grow and diversify, future work could explore quantum resistant.

Acknowledgement: The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2024-996).

References

[1] Renuka, N., and Satya Sairam, M. (2019). ‘‘Peak-to-average power ratio performance of transform precoding-based orthogonal frequency division multiplexing offset quadrature amplitude modulation.’’ In Smart Intelligent Computing and Applications, pp. 241–248. Springer, Singapore.

[2] Raghunatharao, D., Prasad, T. J., & Prasad, M. G. (2020). Optimal pilot-based channel estimation in cognitive radio. Wireless Personal Communications, 114(4), 2801–2819. https://doi.org/ 10.1007/s11277-020-07504-x

[3] Salih, B. M., Badr, B., Baghdadi, A., & Francine, K. (2022, May). Quality of service optimization in OFDM-based cognitive radio network. In 2022 19th International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 1731-1736). IEEE.

[4] Sedighi, S, Taherpour, A, Gazor, S & Khattab, T 2017, 'Eigen value- based multiple antenna spectrum sensing: higher order moments',IEEE Transactions on Wireless Communications, vol.16, pp.1168-1184.

[5] Shaat, M., & Bader, F. (2010). Computationally efficient power allocation algorithm in multicarrier-based cognitive radio networks: OFDM and FBMC systems. EURASIP Journal on Advances in Signal Processing, 2010, 1-13.

[6] Shuangfei Z Y Cheng, W Lu & Z Zhang 2016, 'Deep Structured Energy Based εodels for Anomaly Detection', Proceedings of the 33rd International Conference on Machine Learning, New York, NY, USA.

[7] Siddiqi, M. Z., Wuttisittikulkij, L., Mirza, I. S., Chaudhary, S., & Paranianifard, A. (2022, May). Adaptive Modulation and Power Allocation in Green Cognitive Radio Networks. In 2022 19th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 1-4). IEEE.

[8] Sidhu, G. A. S., Gao, F., Wang, W., & Chen, W. (2013). Resource allocation in relay-aided OFDM cognitive radio networks. IEEE Transactions on Vehicular Technology, 62(8), 3700-3710.
Signal processing, vol. 120, pp. 385-408.

[9] Simsir S & Taspinar 2020, 'A novel discrete cuckoo search algorithm- based selective mapping technique to minimize the PAPR universal filtered multicarrier signal', International Journal of Communication Systems, vol.33,no.18,p.e4640

[10] Singh, S & Patra, SK 2014, 'Partial transmit sequence based PAPR reduction for OFDM using Best harmony search evolutionary algorithm', Proceedings of the 8th International Conference on Bio inspired Information and Communications Technologies, pp. 75-80

[11] Sofotasios, PC, Mohjazi, L, Muhaidat, S, Al-Qutayri, M & Karagiannidis, GK 2016, 'Energy detection of unknown signals over cascaded fading channels', IEEE Antennas and Wireless Propagation Letters, vol. 15, pp. 135-138.

[12] Spooner, Cε & Nicholls, RB 2009, 'Spectrum sensing based on spectral correlation', Cognitive Radio Technology, vol. 2, pp. 593-634.

[13] Sultana, A., Zhao, L., & Fernando, X. (2016, September). Power allocation using geometric water filling for OFDM-based cognitive radio networks. In 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall) (pp. 1-5). IEEE.

[14] Sun, C, Zhang, W & δetaief, KB 2007, 'Cluster-based cooperative spectrum sensing in cognitive radio systems', In 2007 IEEE international conference on communications, pp. 2511-2515.

[15] Suresh Dannana, Babji Prasad Chapa & Gottapu Sasibhushana Rao 2019, 'Spectrum Sensing for OFDε Cognitive Radio using εatched Filter Detection', International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, vol. 8, no. 2, pp. 1-6.

[16] Sutton, PD, Nolan, KE & Doyle, δE 2008, 'Cyclostationary signatures in practical cognitive radio applications', IEEE Journal on selected areas in Communications, vol. 26, no. 1, pp. 13-24.

[17] Tamilselvi, T., Rajendran, V., & Bharathy, G. T. (2022, January). Comparative analysis of CP-OFDM and F-OFDM schemes for cognitive networks. In AIP Conference Proceedings (Vol. 2385, No. 1, p. 060002). AIP Publishing LLC

[18] Tan, CE & Wassell, IJ 2003 'Data bearing peak reduction carriers for OFDε systems', the Fourth Pacific Rim Conference on Multimedia, Proceedings of the 2003 Joint, vol. 2, pp. 854-858.

[19] Taspinar, N & simsir, 2019, 'Dual symbol optimization-based partial transmit sequence technique for PAPR reduction in WOLA-OFDM waveform', International Journal of Communication Systems, vol. 32, no. 14, p. e4081.

[20] Teo, Zhong, & Ng, BCh 2010, 'An Iterative Threshold Selection Algorithm for Cooperative Sensing in a Cognitive Radio Network', IEEE Symposium on New Frontiers in Dynamic Spectrum, pp. 1-8.

[21] Tosato, F, Sandell, M & Tanahashi, ε 2016, 'Tone reservation for PAPR reduction: An optimal approach through sphere encoding', 2016 IEEE International Conference on Communications (ICC), pp. 1-6.

[22] Vadivelu, R, Sankaranarayanan, K & Vijayakumari, V 2014, 'εatched filter based spectrum sensing for cognitive radio at low signal to noise ratio', Journal of Theoretical and Applied Information Technology, vol. 62, no. 1, pp. 107-113.

[23] Van der Neut, N, Maharaj, BT, De Lange, F, González, GJ, Gregorio, F & Cousseau, J 2014, 'PAPR reduction in FBεC using an ACE- based linear programming optimization', EURASIP Journal on Advances in Signal Processing, vol. 1, pp. 1-21.

[24] Vangala, S & Sundru, A 2016, ‘Adaptive Clipping Active Constellation Extension for PAPR Reduction of OFDM/OQAM System’, Procedia Computer Science, vol. 93, pp. 617-623.

[25] Ahmad. R. khan, (2024). “Dynamic Load Balancing in Cloud Computing: An Optimized RL-Based Clustering with Multi-Objective Optimized Task Scheduling”, International journal Processes.

[26] Ahmad. R. Khan (2022). “Using virtualized multimedia tools for video conferencing solution integrated in teaching and learning environment”, Journal of Discrete Mathematical Sciences and Cryptography, 25:3, 801-815, DOI: 10.1080/09720529.2021.2014137.

[27] Khan AR (2022). Secure PAAS environment over hybrid cloud using load-balanced Docker containers. International Journal of Advanced and Applied Sciences, 9(3): 133-141.

Appendix:

```
    \documentclass{article}

    \usepackage{algorithm}

    \usepackage{algpseudocode}

    \usepackage{amsmath}

    \begin{document}

     % Algorithm 1: Continuous Authentication

    \begin{algorithm}

    \caption{Continuous Authentication}

    \begin{algorithmic}[1]

        \State \textbf{Input:} Device private key (\textit{PrivateKey}), Device data at time $t$
      (\textit{DeviceData$_t$})

    \State \textbf{Output:} Device signature (\textit{Device-Signature$_t$})

    \State Compute \textit{Device-Signature$_t$} $\gets$ Sign(\textit{PrivateKey}, \textit{DeviceData$_t$})

    \end{algorithmic}

    \end{algorithm}


    % Algorithm 2: Device Identity Verification

    \begin{algorithm}

  \caption{Device Identity Verification}

  \begin{algorithmic}[1]

     \State \textbf{Input:} Device public key (\textit{PublicKey$_{Device}$}), Device signature
    (\textit{DeviceSignature$_t$}), Device data at time $t$ (\textit{DeviceData$_t$})

  \State \textbf{Output:} IsDeviceValid$_t$

     \State Compute \textit{IsDeviceValid$_t$} $\gets$ Verify(\textit{PublicKey$_{Device}$},
    \textit{DeviceSignature$_t$}, \textit{DeviceData$_t$})

  \end{algorithmic}

  \end{algorithm}


  % Algorithm 3: Authentication Token Generation
```

```
 \begin{algorithm}
 \caption{Authentication Token Generation}
 \begin{algorithmic}[1]
   \State \textbf{Input:} Device private key (\textit{PrivateKey}), Device data at time $t$ (\textit{DeviceData$_t$}), Timestamp at time $t$ (\textit{Timestamp$_t$})
 \State \textbf{Output:} Authentication token (\textit{AuthToken$_t$})
 \State Compute \textit{AuthToken$_t$} $\gets$ HMAC(\textit{PrivateKey}, \textit{DeviceData$_t$} $||$ \textit{Timestamp$_t$})
\end{algorithmic}
\end{algorithm}
```

% Algorithm 4: Authentication Verification

```
\begin{algorithm}
\caption{Authentication Verification}
\begin{algorithmic}[1]
 \State \textbf{Input:} Device public key (\textit{PublicKey$_{Device}$}), Authentication token (\textit{AuthToken$_t$}), Device data at time $t$ (\textit{DeviceData$_t$}), Timestamp at time $t$ (\textit{Timestamp$_t$})
\State \textbf{Output:} IsAuthenticationValid$_t$
 \State Compute \textit{IsAuthenticationValid$_t$} $\gets$ Verify(\textit{PublicKey$_{Device}$}, \textit{AuthToken$_t$}, \textit{DeviceData$_t$} $||$ \textit{Timestamp$_t$})
 \end{algorithmic}
 \end{algorithm}
 \end{document}
```