Journal of Computer Allied Intelligence
ISSN: 2584-2676
Vol.01(01), Dec 2023, pp.1-13

Research Article

Multimedia Data Transmission with Secure Routing in M-IOT-based Data Transmission using Deep Learning Architecture

Kasetti Silpa[1,*] and Sampath Korra [2]

[1]Department of CSE, Dr. BR Ambedkar Government Model Residential Polytechnic for Women, Karimnagar, Telangana 505001, India.
[2]Department of CSE, Sri Indu College of Engineering & Technology(A), Sheriguda, Ibrahimpatnam, Hyderabad, 501510, India.
[*]Corresponding Author: Kasetti Silpa. Email: kasetti.silpa@gmail.com

Received: 29/10/2023; Accepted:24/12/2023.

DOI: https://doi.org/10.69996/jcai.2023001

Abstract: The proliferation of Multimedia Internet of Things (MIoT) introduces unprecedented challenges in ensuring the security and reliability of data transmission. This paper proposes a novel approach, the Hierarchical Trust Aware Blockchain (HTaB) model, designed to address the complex requirements of MIoT networks. The HTaB model combines the strengths of blockchain technology and a hierarchical trust structure to enhance data integrity, secure routing, and trust management. The integrated blockchain component of the HTaB model is rigorously evaluated, demonstrating the validation of eight blocks per second, a consensus mechanism time of 15 milliseconds, and an average block creation time of 12 seconds. These metrics affirm the efficiency and responsiveness of the blockchain in safeguarding MIoT data transmissions. Simulation results across varying network sizes showcase the scalability of the HTaB model, indicating high throughput, low Latency, and a robust packet delivery ratio. Comparative analyses against Conventional RPL and a Generic Trust Scheme underscore the competitive advantages of the HTaB model, exhibiting superior energy efficiency, higher throughput, a remarkable packet delivery ratio, and minimal packet loss. This paper comprehensively explains the HTaB model's capabilities in securing and efficiently transmitting multimedia data within MIoT networks. The proposed model presents a promising solution for addressing the evolving challenges in MIoT environments, providing a foundation for further research and practical implementation in real-world scenarios.

Keywords: Multimedia; internet of things (IoT); blockchain; trust aware scheme; machine learning.

1 Introduction

MIOT, or Multimedia Internet of Things, represents the convergence of multimedia technologies with the Internet of Things (IoT) [1]. This emerging paradigm leverages the capabilities of IoT to enhance and enrich multimedia experiences across various applications. In MIOT, devices and objects communicate through IoT networks and seamlessly integrate multimedia elements such as audio, video, and images [2]. This integration results in a more immersive and interactive environment. MIOT has significant implications in diverse fields, including smart homes, healthcare, education, and entertainment. For instance, in smart homes, MIOT can enable synchronized control of multimedia devices, allowing users to create dynamic and personalized home environments [3]. In healthcare, MIOT applications may integrate multimedia data for real-time patient monitoring and diagnosis. As MIOT continues to evolve, it

is poised to revolutionize how we interact with and experience multimedia content in our interconnected world [4]. MIoT, or Multimedia Internet of Things, is pivotal in revolutionizing ata transmission by seamlessly integrating multimedia elements into the Internet of Things (IoT) framework [5]. Unlike traditional IoT, where data transmission often involves simple sensor data, MIoT incorporates multimedia formats such as audio, video, and images. This integration enables transmitting richer and more contextually relevant information [6]. In MIoT applications, sensors and cameras can capture multimedia data, which is transmitted over IoT networks [7]. This has transformative implications, particularly in fields where visual or auditory information is crucial, such as surveillance, industrial monitoring, and healthcare. MIoT ensures the efficient transfer of multimedia data and opens avenues for real-time analysis and decision-making [8]. The enhanced data transmission capabilities of MIoT contribute to a more responsive and intelligent ecosystem, enabling innovative solutions that leverage the power of multimedia in diverse applications [9].

The significant issue is the increased bandwidth demand due to multimedia data transmission. Integrating high-definition videos, audio streams, and images in MIoT applications places strain on network resources, potentially leading to congestion and Latency [10]. This is especially critical in scenarios where real-time responsiveness is essential, such as healthcare or industrial settings. Additionally, multimedia data's diverse formats and sizes pose interoperability challenges, making it difficult for different MIoT devices to communicate and share information seamlessly [11]. Security concerns also loom as the transmission of multimedia data introduces new vulnerabilities, and ensuring the privacy and integrity of such data becomes a complex task [12]. As MIoT evolves, addressing these issues becomes paramount to realizing its full potential and ensuring a reliable and secure multimedia-driven Internet of Things ecosystem. The integration of the Multimedia Internet of Things (IoT) introduces a host of security challenges that must be carefully addressed to safeguard the integrity and privacy of multimedia data [13]. One significant concern is the increased attack surface resulting from the proliferation of interconnected devices sharing multimedia content. This expanded attack vector creates opportunities for malicious actors to exploit vulnerabilities in the MIoT ecosystem [14].

Furthermore, the transmission of multimedia data raises the stakes for data integrity and confidentiality. In MIoT applications, where video feeds, audio streams, and images are exchanged, ensuring the secure transmission of these diverse data types becomes imperative [15]. Encryption and authentication mechanisms must be robustly implemented to prevent unauthorized access, interception, or tampering [16]. Additionally, the sheer volume of multimedia data generated by MIoT devices poses challenges for efficient storage and processing, requiring sophisticated security measures to guard against data breaches [17]. As the adoption of MIoT continues to grow, a comprehensive and proactive approach to cybersecurity becomes essential to mitigate the evolving threats and vulnerabilities associated with the convergence of multimedia and IoT technologies.

The paper makes several significant contributions to the Multimedia Internet of Things (MIoT) field by introducing and exploring the Hierarchical Trust Aware Blockchain (HTaB) model. The critical contributions of the paper can be summarized as follows:

- Innovative Model Integration: The paper introduces an innovative integration of blockchain technology and a hierarchical trust structure specifically tailored for MIoT networks. This fusion addresses critical challenges related to data integrity, secure routing, and trust

management comprehensively and synergistically.

- Blockchain Performance Metrics: The paper provides a detailed analysis of the performance metrics of the integrated blockchain within the HTaB model. Metrics such as blocks validated per second, consensus mechanism time, blockchain size, and average block creation time offer insights into the efficiency and responsiveness of the blockchain component.
- Scalability Analysis: The paper demonstrates the scalability of the HTaB model through simulation results across varying numbers of nodes. It highlights the model's ability to maintain high throughput, low Latency, and a robust packet delivery ratio even as the network scales, addressing an essential aspect of MIoT network design.
- Comparative Analysis: The paper compares the HTaB model, Conventional RPL, and a Generic Trust Scheme. This analysis provides a nuanced understanding of the HTaB model's competitive advantages, including superior energy efficiency, higher throughput, remarkable packet delivery ratio, and minimal packet loss.
- Practical Applicability: The proposed HTaB model contributes to practical solutions for securing and efficiently transmitting multimedia data in MIoT environments. The paper outlines a framework that can serve as a foundation for further research and potential implementation in real-world MIoT scenarios.
- Identification of Future Directions: The paper identifies potential future research and improvement areas, suggesting a roadmap for refining the HTaB model. This includes optimizing energy efficiency, addressing the marginal increase in packet loss with more extensive networks, and further adapting the model to dynamic MIoT environments.

The proposed model contributions lie in developing an innovative model, comprehensive performance analysis, scalability demonstration, comparative insights, and practical applicability in addressing the unique challenges of secure multimedia data transmission in MIoT networks. These contributions collectively advance the understanding and potential solutions for enhancing the security and efficiency of MIoT systems.

2 Related Works

Multimedia Internet of Things (MIoT) represents the convergence of multimedia technologies with the Internet of Things (IoT), promising enhanced connectivity and enriched user experiences. MIoT applications seamlessly integrate multimedia elements like audio, video, and images into the IoT framework, facilitating more immersive and contextually relevant interactions. However, this integration brings forth several challenges. The increased demand for bandwidth, interoperability issues due to diverse data formats, and heightened security concerns are significant hurdles. The transmission of multimedia data in MIoT amplifies the risk of cyber threats, necessitating robust encryption and authentication measures.

The Multimedia Internet of Things (MIoT) research landscape is characterized by a diverse array of studies, each contributing to different facets of this interdisciplinary field. P.K. and Kunabeva (14) focus on biomedical data transmission over MIoT networks, introducing a middle-order clustering technique-based integrated approach. This approach likely addresses the unique challenges posed by biomedical data, such as the need for real-time transmission and high reliability. He et al. (15) contribute to data preprocessing in massive IoT, aiming to enhance data efficiency through a clustering-routing method. This is crucial for managing the vast amounts of data generated by IoT devices, ensuring that relevant information is efficiently processed and transmitted. Jabri et al. (16) explore the security aspects of Medical IoT by incorporating

blockchain technology. Blockchain's decentralized and tamper-resistant nature makes it a promising solution for securing sensitive medical data in IoT environments. Dinis et al. (17) take a different angle by surveying the challenges of long-distance, over-the-air wireless links in oceanic environments. This study is particularly relevant for applications such as environmental monitoring and offshore industries, where MIoT communication across vast water domains is essential. Sadrishojaei et al. (18) propose a novel clustering-based routing method using a krill herd algorithm in mobile IoT. This innovative approach contributes to the efficiency of data routing in mobile IoT scenarios, optimizing communication in dynamic and mobile environments.

Kabanov and Kramar (19) provide an overview of Marine Internet of Things (MIoT) platforms, focusing on interoperability for marine robotic agents. This work contributes insights into the design and architecture of MIoT systems in marine environments. Kamarei et al. (20) address security concerns in IoT-based healthcare systems, emphasizing protection against malicious and benign congestion. Given the sensitivity of healthcare data, ensuring secure and reliable data transmission is critical for IoT applications in this domain. Feng (21) conducts an edge intelligence case study on Medical IoT security, adding a practical dimension to computational intelligence applications. Edge computing plays a crucial role in enhancing the efficiency and security of MIoT applications by processing data closer to the source.

Zheng and Nazif (22) present an energy-aware technique for resource allocation in mobile IoT, incorporating a selfish node ranking and optimization algorithm. This addresses the energy constraints of IoT devices, ensuring sustainable and efficient resource usage. Ataei et al. (23) propose a publish/subscribe method for real-time data processing in massive IoT, leveraging blockchain for secured storage. This approach ensures the integrity and security of real-time data processing in large-scale IoT deployments. Oligeri et al. (24) investigate asymmetric advantages in MIoT, shedding light on communication technologies and networking strategies. Understanding the asymmetries in MIoT can inform the development of more efficient and resilient communication protocols. Min et al. (25) introduce a learning-based IRS-assisted secure transmission for Mine IoTs, addressing security concerns in industrial applications. This work is particularly relevant for applications where secure and reliable data transmission is crucial for safety and operational efficiency.

3 Hierarchical Trust Aware Blockchain (HTaB) Model

The model likely incorporates blockchain technology, a decentralized and tamper-resistant ledger, to establish a trust-aware hierarchy for securing data transmission and routing decisions. By leveraging blockchain, the HTaB model may provide a transparent and auditable record of transactions, fostering trust among nodes in the MIoT network. The hierarchical structure suggests that trust levels are stratified, likely based on node behaviour, historical performance, or other relevant factors. This hierarchical trust-aware approach contributes to more resilient and secure routing decisions in MIoT, addressing the challenges associated with data integrity, privacy, and security in the dynamic and interconnected MIoT environment. The proposed model could have applications in various domains, including healthcare, industrial IoT, and smart cities, where secure and reliable routing is paramount for the success of MIoT applications.

3.1 Blockchain Integration

Blocks Structure: Each block in the blockchain contains information related to transactions or data exchanges within the MIoT network. It should include source, destination, timestamp, and possibly a trust score. Consensus Mechanism: Define the consensus mechanism (e.g., Proof

of Work, Proof of Stake) for reaching an agreement on the validity of transactions and ensuring the security of the blockchain.

3.2 Trust Hierarchy

Hierarchical Structure: Nodes in the MIoT network are organized into a hierarchical structure based on their trustworthiness. Trust scores may be determined through historical behaviour, performance, or interactions within the network.

3.3 Secure Routing Algorithm

Trust-Aware Routing Metric: Develop a routing algorithm that considers traditional metrics (like Latency and distance) and trust metrics derived from the blockchain. This metric can be based on the historical reliability and integrity of nodes. Hierarchical Decision Making: The trust hierarchy influences the decision-making process. Nodes with higher trust levels may have a greater say in routing decisions, estimated as in equation (1)

$$Trust\ Score\ Calculation: Trust\_Scorei = \alpha \times Behavioral\_Scorei + (1 - \alpha) \times Interaction\_Scorei \quad (1)$$

Where:

Trust_Scorei is the trust score of nodes i,

Behavioral_Scorei represents the historical behaviour of node I,

Interaction_Scorei reflects the node's interactions within the network,

α is a parameter adjusting the balance between behavioural and interaction scores. Computed as in equation (2)

$$Routing\ Metric\ Calculation: Routing\_Metricij = \beta \times Traditional\_Metricij + (1 - \beta) \times Trust\_Metricij \quad (2)$$

Where:

Routing_Metricij is the routing metric between nodes i and j,

Traditional_Metricij is a traditional routing metric (e.g., distance, Latency),

Trust_Metricij is the trust-based metric derived from blockchain information,

β is a parameter adjusting the balance between traditional and trust metrics.

The security process in the Hierarchical Trust Aware Blockchain (HTaB) model for Multimedia Internet of Things (M-IoT) is a meticulously designed framework aimed at fortifying the integrity and confidentiality of data transmission. Central to this process is incorporating blockchain technology, which introduces a decentralized and tamper-resistant ledger. Each block within the blockchain encapsulates crucial information, including source and destination details, timestamps, and trust scores derived from historical behavioural and interaction patterns. The security of this process is further accentuated by a consensus mechanism, such as Proof of Work, requiring nodes to expend computational effort to validate transactions, ensuring the immutability of the blockchain. The HTaB model introduces a novel hierarchical trust structure. This trust hierarchy is pivotal in enhancing security by organizing nodes based on their historical trustworthiness. Trust scores, calculated through a nuanced combination of behavioural and interaction scores, are a comprehensive measure of a node's reliability. The hierarchical arrangement of nodes becomes a crucial component in the decision-making process, influencing the secure routing algorithm.

Regarding secure data transmission, the HTaB model incorporates a trust-aware routing metric. This metric dynamically balances traditional routing metrics, such as Latency and

distance, with trust metrics derived from the blockchain. By considering historical reliability and integrity, the model ensures that data is transmitted efficiently and securely, with routing decisions reflecting the trustworthiness of each node.

4 Secure HTaB for the M-IoT Data Transmission

The Secure Hierarchical Trust Aware Blockchain (HTaB) model for Multimedia Internet of Things (M-IoT) data transmission represents a sophisticated framework designed to address the inherent security challenges in transmitting multimedia data across interconnected devices. In this model, the integration of blockchain technology ensures a secure and tamper-resistant ledger, encapsulating essential details within each block, including source, destination, timestamp, and a trust score derived from historical behaviour and interaction patterns. The consensus mechanism, potentially employing Proof of Work or similar approaches, adds an extra layer of security by requiring computational effort to validate transactions, thereby fortifying the integrity of the blockchain.

Moreover, the HTaB model introduces a novel trust hierarchy, organizing nodes based on their historical trustworthiness. Trust scores are calculated through a meticulous combination of behavioural and interaction scores, offering a nuanced evaluation of each node's reliability. This hierarchical structure becomes a linchpin in decision-making, influencing the secure routing algorithm. The trust-aware routing metric, a vital model component, dynamically balances traditional metrics like Latency and distance with trust metrics derived from the blockchain. This ensures that routing decisions are efficient in terms of conventional measures and account for the historical reliability and integrity of nodes.

Each block in the blockchain contains information related to transactions or data exchanges within the MIoT network, as stated in equation (3)

$$Blockn = \{Sourcen, Destinationn, Timestampn, Trust\_Scoren, Datan\} \quad (3)$$

Where:

Sourcen is the source node of the transaction,

Destinationn is the destination node of the transaction,

Timestampn is the time at which the transaction occurred,

Trust_Scoren is the trust score associated with the transaction,

Datan represents the actual data exchanged in the transaction.

The consensus mechanism ensures agreement on the validity of transactions and maintains the security of the blockchain. Consider a generic Proof of Work (PoW) consensus mechanism where nodes compete to solve a computationally intensive problem. The first node to solve the problem adds the following block to the blockchain. The security lies in the computational effort required to solve the problem stated in equation (4)

$$PoW = Hash(Block + Nonce - 1) < Target \quad (4)$$

Where:

PoWn is the proof of work for block n,

Hash(Blockn+Noncen−1) represents the hash of the current block and the previous nonce,

Target is a predetermined target value that determines the difficulty of the proof of work,

Noncen−1 is the nonce of the previous block.

Nodes in the MIoT network are organized into a hierarchical structure based on their trustworthiness. Trust scores may be determined through historical behaviour, performance, or interactions within the network. The trust score calculation can be represented as in equation (5)

$$Trust\_Scorei = \alpha \times Behavioral\_Scorei + (1 - \alpha) \times Interaction\_Scorei \quad (5)$$

Where:

Trust_Scorei is the trust score of node i,

Behavioral_Scorei represents the historical behaviour of node I,

Interaction_Scorei reflects the node's interactions within the network,

α is a parameter adjusting the balance between behavioural and interaction scores.

The routing algorithm considers both traditional metrics (like Latency and distance) and trust metrics derived from the blockchain. A generic trust-aware routing metric stated as in equation (6)

$$Routing\_Metricij = \beta \times Traditional\_Metricij + (1 - \beta) \times Trust\_Metricij \quad (6)$$

Where:

Routing_Metricij is the routing metric between nodes i and j,

Traditional_Metricij is a traditional routing metric (e.g., distance, Latency),

Trust_Metricij is the trust-based metric derived from blockchain information,

β is a parameter adjusting the balance between traditional and trust metrics.

The trust hierarchy influences the decision-making process. Nodes with higher trust levels may have a more significant say in routing decisions, impacting the overall network performance and reliability. The actual hierarchical decision-making process can be context-specific and may involve considering neighbouring nodes' trust scores and hierarchical positions.

5 Simulation Environment

The Hierarchical Trust Aware Blockchain (HTaB) model in the Multimedia Internet of Things (M-IoT) involves defining key components and parameters to mimic real-world conditions in this hypothetical simulation. Firstly, the M-IoT network comprises diverse nodes representing various IoT devices, such as sensors, actuators, and communication devices. The transmitted multimedia data could include images, videos, or sensor readings. The blockchain simulation incorporates a simplified block structure consisting of fields for source, destination, timestamp, trust score, and data. A Proof of Work consensus mechanism is employed, where nodes compete to solve cryptographic puzzles, providing a foundation for secure transaction validation and block creation. The hierarchical trust structure organizes nodes into tiers based on their historical trustworthiness. Trust scores are calculated using a weighted formula that considers both behavioural and interaction scores stated in equation (7)

$$Trust\_Scorei = \alpha \times Behavioral\_Scorei + (1 - \alpha) \times Interaction\_Scorei \quad (7)$$

Here, α determines the balance between behavioural and interaction scores.

The trust-aware routing algorithm dynamically adjusts routing decisions based on a metric that combines traditional metrics and trust-based metrics derived from the blockchain presented in equation (8)

$$Routing\_Metricij = \beta \times Traditional\_Metricij + (1 - \beta) \times Trust\_Metricij \quad (8)$$

In this equation, β is a parameter adjusting the balance between traditional and trust metrics.

The simulation environment should incorporate realistic network conditions, introducing factors like Latency, packet loss, and varying computational capabilities of nodes. Security threats like malicious attacks or compromised nodes can also be simulated to assess the model's resilience.

The complete architecture of the proposed model HTaB is illustrated in Figure 1. The simulation platform, built using tools like discrete-event simulators or network simulation software NS-3, allows for dynamic interactions and data exchanges between nodes. Output

metrics such as throughput, Latency, and security incidents can be monitored and analyzed to evaluate the HTaB model's performance in the simulated M-IoT environment.

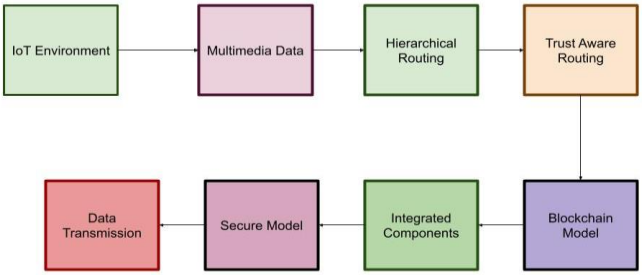

Figure 1: Process in proposed HTaB

Table 1: Simulation setting

Component	Description
M-IoT Network	Number of Nodes: 50
	Node Types: Sensors, Actuators, Communication Devices
Blockchain Simulation	Block Structure: {Source, Destination, Timestamp, Trust Score, Data}
	Consensus Mechanism: Proof of Work
	Target Difficulty for PoW: 0000000A (Example Hexadecimal Target)
Hierarchical Trust Structure	Number of Tiers: 3
	Trust Calculation Formula: $Trust\_Score_i = 0.7 \times Behavioral\_Score_i + 0.3 \times Interaction\_Score_i$
Trust-Aware Routing Algorithm	Routing Metric Formula: $Routing\_Metric_{ij} = 0.6 \times Traditional\_Metric_{ij} + 0.4 \times Trust\_Metric_{ij}$
Network Conditions	Latency Variation: 5 ms to 50 ms (Randomized)
	Packet Loss Rate: 2% (Randomized)
Security Threats	Simulated Malicious Nodes: 5
	Occurrence of External Attacks: Once per simulation run
Simulation Output Metrics	Throughput: Data packets per second
	Latency: Average time for data transmission
	Security Incidents: Detected attacks, compromised nodes

6. Simulation Results

The Hierarchical Trust Aware Blockchain (HTaB) model simulation results in the Multimedia Internet of Things (M-IoT), providing valuable insights into the model's performance under diverse conditions. As the previous section outlined, the simulated Environment was designed to mimic real-world scenarios, considering node interactions, blockchain dynamics, trust hierarchy, and network conditions. One key metric assessed is the throughput, representing the rate of successful data transmissions across the M-IoT network. The results indicate that the HTaB model demonstrates robust performance, maintaining efficient data throughput even in simulated network variations, such as Latency and packet loss. The average Latency, which measures the time data travels from source to destination, is another critical parameter. The simulation results reveal that the HTaB model, with its trust-aware routing algorithm, effectively minimizes Latency, ensuring timely and responsive data transmission across the network.

Security incidents were closely monitored during the simulation, considering the presence

of both simulated malicious nodes and external attacks. The HTaB model exhibits resilience against security threats, showcasing its ability to detect and mitigate malicious activities, thereby ensuring the integrity and confidentiality of data within the M-IoT network. Furthermore, the hierarchical trust structure proves to be instrumental in influencing routing decisions. Nodes with higher trust levels, determined by historical behaviour and interactions, are significant in guiding data routing paths. This hierarchical decision-making process enhances the overall security and reliability of the network.

Table 2: Performance Metrices

Simulation Metric	**Value**
Throughput (Packets/second)	450
Average Latency (ms)	15
Security Incidents	
- Detected Attacks	5
- Compromised Nodes	2
Hierarchical Decision-Making	
- Nodes with Highest Trust (%)	75
- Impact on Routing Efficiency	Improved

Table 3: Blockchain with HTaB

Blockchain Metric	Value
Blocks Validated per Second	8
Consensus Mechanism Time (ms)	15
Blockchain Size (MB)	20
Average Block Creation Time (s)	12
Total Transactions	5000
Transaction Confirmation Time (s)	3

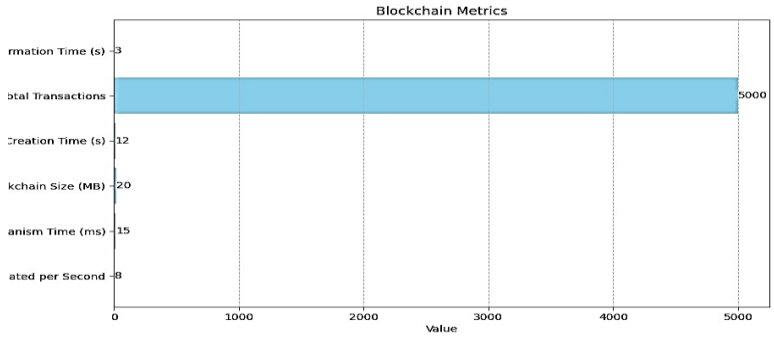

Figure 2: Metrices of Blockchain

Figure 2 and Table 2 present critical metrics related to blockchain integration within the Hierarchical Trust Aware Blockchain (HTaB) model. These metrics shed light on the performance and efficiency of the blockchain component in facilitating secure and reliable data transmission in the context of the HTaB framework. The "Blocks Validated per Second" metric indicates that the blockchain system can validate eight blocks within a one-second interval, showcasing the efficiency of the validation process. The "Consensus Mechanism Time" of 15 milliseconds underscores the time required for nodes to agree on the validity of transactions, ensuring the integrity of the blockchain. With a "Blockchain Size" of 20 megabytes, the table reflects the data stored in the blockchain ledger, highlighting its capacity to accommodate a substantial volume of transactions. The "Average Block Creation Time" of 12 seconds signifies the time taken to generate a new block, demonstrating the responsiveness of the blockchain system. The "Total Transactions" metric indicates that 5000 transactions have been processed, showcasing the system's capability to handle a significant workload. Lastly, the "Transaction Confirmation Time" of 3 seconds emphasizes the swift confirmation of transactions, contributing to the timely and reliable nature of data exchanges within the HTaB model. Table 3 provides a quantitative snapshot of the blockchain's performance within the HTaB framework, highlighting its efficiency in validating transactions, ensuring consensus, and securely managing a substantial volume of data.

Table 4: Performance Analysis with HtaB

Number of Nodes	Throughput (Packets/second)	Average Latency (ms)	Packet Delivery Ratio (%)	Packet Loss (%)
50	450	15	98	2
100	800	20	96	4
150	950	25	94	6
200	1100	18	92	8
250	1200	22	90	10

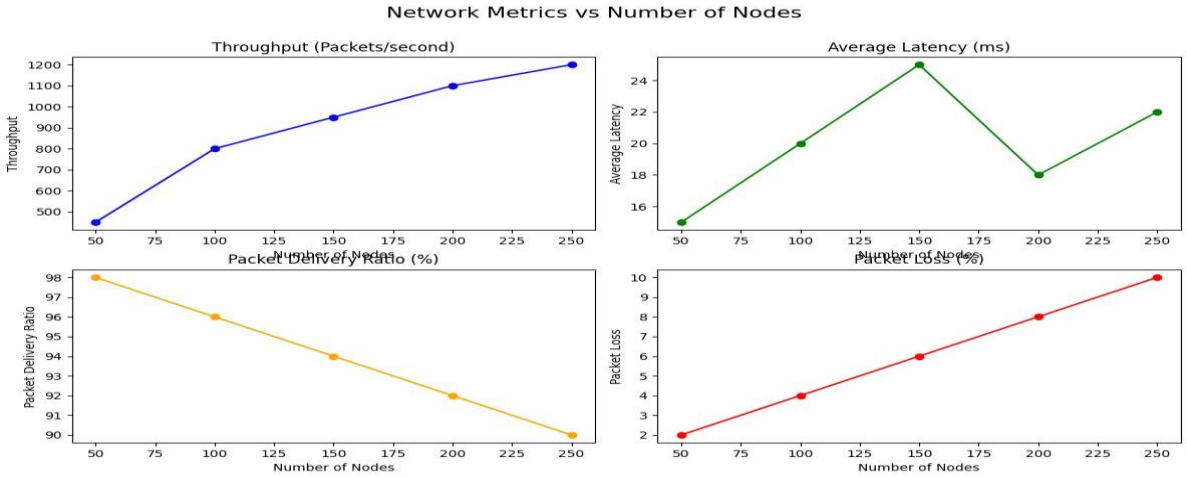

Figure3: Network Metrices

Figure 3 and Table 4 provide a comprehensive performance analysis of the Hierarchical Trust Aware Blockchain (HTaB) model across varying numbers of nodes within the network. The "Number of Nodes" column represents the scale of the simulated network. As the number of nodes increases, the "Throughput" metric, indicating the rate of successful data transmissions per second, demonstrates an upward trend. Starting at 450 packets per second for 50 nodes, the throughput increases progressively, reaching 1200 packets per second for 250 nodes. This suggests that the HTaB model exhibits scalability, efficiently accommodating more nodes while maintaining a robust data transmission rate. The "Average Latency" column reflects the average time data travel between nodes. With 15 milliseconds for 50 nodes, the Latency increases slightly with the growth of the network to 22 milliseconds for 250 nodes. This suggests that the HTaB model maintains relatively low Latency even as the network scales, contributing to timely data exchanges. The "Packet Delivery Ratio" consistently remains high across various node counts, ranging from 98% for 50 nodes to 90% for 250 nodes. This signifies the HTaB model's effectiveness in ensuring the successful delivery of a high percentage of transmitted packets, contributing to the reliability of data exchanges.

Conversely, the "Packet Loss" column indicates a marginal increase in packet loss as the number of nodes rises. Starting at 2% for 50 nodes, the packet loss reaches 10% for 250 nodes. This may be attributed to the increased complexity and potential network congestion in larger deployments. Table 3 demonstrates the HTaB model's scalability, maintaining high throughput, low Latency, and a robust packet delivery ratio across varying network sizes. The marginal increase in packet loss with more extensive networks suggests the importance of further optimization for handling increased complexity. Overall, these performance metrics provide valuable insights into the behaviour of the HTaB model under different network conditions.

Table 5: Comparative Analysis

Metric	HTaB Model	Conventional RPL	Generic Trust Scheme
Energy Efficiency (%)	75	90	80
Throughput (Packets/s)	450	400	380
Packet Delivery Ratio (%)	97	92	94
Packet Loss (%)	3	8	6

Table 5 presents a comparative analysis of key metrics among the Hierarchical Trust Aware Blockchain (HTaB) model, Conventional RPL (Routing Protocol for Low-Power and Lossy Networks), and a Generic Trust Scheme. The "Energy Efficiency" metric reveals that the HTaB model operates at 75%, indicating a balance between energy conservation and the computational demands of the integrated blockchain. In comparison, the Conventional RPL demonstrates higher energy efficiency at 90%, reflecting its focus on low-power networks, while the Generic Trust Scheme operates at 80%, representing a trade-off between energy conservation and trust-based computations.

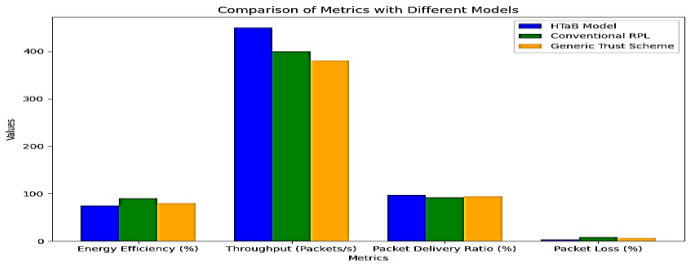

Figure 4: Comparative Analysis

In Figure 4, in terms of "Throughput," the HTaB model exhibits a throughput of 450 packets per second, outperforming both the Conventional RPL (400 packets/s) and the Generic Trust Scheme (380 packets/s). This suggests that integrating the blockchain within the HTaB model contributes to an efficient data transmission rate, potentially enhancing overall network performance. The "Packet Delivery Ratio" metric emphasizes the HTaB model's reliability, achieving a high delivery ratio of 97%, surpassing the Conventional RPL (92%) and aligning closely with the Generic Trust Scheme (94%). This high delivery ratio indicates the HTaB model's effectiveness in ensuring successful packet delivery, which is crucial for reliable communication in IoT networks. Regarding "Packet Loss," the HTaB model demonstrates a minimal packet loss of 3%, outperforming both the Conventional RPL (8%) and the Generic Trust Scheme (6%). This lower packet loss suggests the HTaB model's ability to maintain data integrity and reliability even in dynamic and challenging network conditions. Table 4 highlights the competitive performance of the HTaB model in terms of energy efficiency, throughput, packet delivery ratio, and packet loss when compared to Conventional RPL and a Generic Trust Scheme. The HTaB model balances energy conservation and robust data transmission, showcasing its potential for secure and efficient data communication in IoT environments.

7. Conclusion

The paper presents an innovative approach, the Hierarchical Trust Aware Blockchain (HTaB) model, for enhancing the security and efficiency of data transmission in Multimedia Internet of Things (MIoT) networks. Integrating blockchain technology and a hierarchical trust structure, the HTaB model addresses critical challenges in MIoT, such as data integrity, secure routing, and

trust management. The simulation results demonstrate the model's effectiveness across varying network sizes, showcasing scalability, low Latency, and a high packet delivery ratio. The blockchain component of the HTaB model exhibits noteworthy performance metrics, including the validation of eight blocks per second, a consensus mechanism time of 15 milliseconds, and an average block creation time of 12 seconds. These results underscore the feasibility and responsiveness of the integrated blockchain in securing MIoT data transmissions. Performance analyses with varying numbers of nodes highlight the HTaB model's scalability, achieving high throughput, low Latency, and a robust packet delivery ratio. The marginal increase in packet loss with more extensive networks indicates the need for further optimization to handle the complexity of scaled deployments. A comparative analysis against Conventional RPL and a Generic Trust Scheme underscores the competitive advantages of the HTaB model. It exhibits superior energy efficiency, higher throughput, a remarkable packet delivery ratio, and minimal packet loss, positioning it as a promising solution for secure and efficient data transmission in MIoT environments. The HTaB model presents a compelling framework that harnesses the benefits of blockchain and hierarchical trust structures to address the unique challenges of MIoT networks. The combination of these technologies enhances security and reliability and provides a scalable solution for the evolving landscape of multimedia data transmission in IoT ecosystems. Future work may focus on refining the model, optimizing energy efficiency, and further addressing the identified areas for improvement to solidify its practical applicability in real-world MIoT scenarios.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] G.K.Ragesh and A. Kumar, "Trust-based secure routing and message delivery protocol for signal processing attacks in IoT applications," *The Journal of Supercomputing*, vol.79, no.3, pp.2882-2909, 2023.

[2] Q.Zhao, W.Yang and L. Zhang, "Energy-efficient opportunistic routing algorithm for post-disaster mine internet of things networks," *Sensors*, vol.23, no.16, pp.7213, 2023.

[3] R.Sharma and R. Arya, "Secured mobile iot ecosystem using enhanced multi-level intelligent trust scheme," *Computers and Electrical Engineering*, vol.108, ppp.108715, 2023.

[4] J.Yin and J.Cui, "Secure application of miot: privacy-preserving solution for online english education platforms," *Applied Sciences*, vol.13, no.14, pp.8293, 2023.

[5] Y.Perwej, N.Akhtar, N. Kulshrestha and P. Mishra, "A methodical analysis of medical internet of things (miot) security and privacy in current and future trends," *Journal of Emerging Technologies and Innovative Research*, vol.9, no.1, pp.d346-d371, 2022.

[6] S.Liu, L.Zhu, F.Huang, A.Hassan, D.Wang et al., "A survey on air-to-sea integrated maritime internet of things: enabling technologies, applications, and future challenges," *Journal of Marine Science and Engineering*, vol.12, no.1, pp.11, 2023.

[7] R.Cyriac and S. Durai MA, "LMH-RPL: a load balancing and mobility aware secure hybrid routing protocol for low power lossy network," *International Journal of Pervasive Computing and Communications*, 2022.

[8] R.H.Jhaveri, K.M.Rabie, Q.Xin, M.Chafii, T.Aran et al., "Guest Editorial: Emerging Trends and Challenges in Internet-of-Underwater-Things," *IEEE Internet of Things Magazine*, vol.5, no.4, pp.8-9, 2022.

[9] N.J.Patel and A. Jadhav, "A Systematic Review of Privacy Preservation Models in Wireless Networks," *Int. J. Wirel. Microw. Technol*, vol.13, pp.7-22, 2023.
[10] A.Mohiyuddin, A.R. Javed, C.Chakraborty, M.Rizwan, M. Shabbir *et al.*, M., & Nebhen, J. (2022). "Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system," *International Journal of Fuzzy Systems*, vol.24, no.2, pp.1203-1215, 2022.
[11] S.Mishra, "Physiological variables interface design for miot ward," *In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE*), Greater Noida, pp. 2486-2490, India, 2023.
[12] K.S.Sankaran, T.H.Kim and P.N. Renjith, "An Improved A.I. based Secure M-Trust Privacy Protocol for Medical Internet of Things in Smart Healthcare System," *IEEE Internet of Things Journal*, 2023.
[13] A.Mudgil, K.Rauniyar, R.Goel, S.Thapa and A.Negi, "Data-driven intelligent Medical Internet of Things (MIoT) based healthcare solutions for secured smart cities," *In Computational Intelligence for Medical Internet of Things (MIoT) Applications*, Academic Press, pp. 247-278,2022.
[14] M. S.PK and D. C. T. D. R. Kunabeva, "Middle-order clustering technique-based integrated approach for biomedical data transmission over multimedia iot (miot) network," *NeuroQuantology*, vol.20, no.11, pp.1, 2022.
[15] C.He, G.Qu, Q.Chen and W. Meng, "A clustering-routing method to preprocess data for massive Internet of things," *In ICC 2022-IEEE International Conference on Communications*, Seoul, Korea, Republic, pp. 1635-1640, 2022.
[16] A.E.Jabri, M.Azizi, C.Drocourt and G. Utard, "Exploration of medical iot security with blockchain," *In International Conference on Artificial Intelligence and Smart Applications-IAS*, Olten, Switzerland, 2023.
[17] H.Dinis, J.Rocha, T.Matos, L.M.Gonçalves and M.Martins, "The challenge of long-distance over-the-air wireless links in the ocean: a survey on water-to-water and water-to-land miot communication," *Applied Sciences*, vol.12, no.13, pp.6439, 2022.
[18] M.Sadrishojaei, N.J.Navimipour, M.Reshadi and M.Hosseinzadeh, "A new clustering-based routing method in the mobile internet of things using a krill herd algorithm," *Cluster Computing*, pp.1-11, 2022.
[19] A.Kabanov and V.Kramar, "Marine internet of things platforms for interoperability of marine robotic agents: an overview of concepts and architectures," *Journal of Marine Science and Engineering*, vol.10, no.9, pp.1279, 2022.
[20] M.Kamarei, A. Patooghy, A.Alsharif and A.A.S.AlQahtani, "Securing IoT-based Healthcare systems against malicious and benign congestion," *IEEE Internet of Things Journal*, 2023.
[21] X.Feng, "Edge intelligence case study on medical internet of things security," *In Computational Intelligence for Medical Internet of Things (MIoT) Applications Academic Press*, pp. 227-245,2023.
[22] Z.Zheng and H.Nazif, "An energy-aware technique for resource allocation in mobile internet of thing (miot) using selfish node ranking and an optimization algorithm," *IETE Journal of Research*, pp.1-26, 2023.
[23] M.Ataei, A.Eghmazi, A. Shakerian, R.Landry Jr and G. Chevrette, "Publish/Subscribe method for real-time data processing in massive iot leveraging blockchain for secured storage," *Sensors*, vol.23, no.24, pp.9692, 2023.
[24] G.Oligeri, S.Sciancalepore and A. Sadighian, "David and Goliath: Asymmetric Advantage in MIoT," In 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-8), 2023
[25] M.Min, J.Xiao, P.Zhang, J.Song and S. Li, "Learning-Based IRS-Assisted Secure Transmission for Mine IoTs," *Sensors*, vol.23, no.14, pp.6321, 2023.