Hybrid Internet Architecture and Protocol (HIAP): A Self-Evolving and Transformative Framework for Enabling Seamless Real-Time Applications and Secure Peer-to-Peer File Sharing in the Internet of Everything (IoE)

Walter Antonio Campos Ugaz[1*], Maria del Rocío Hende Santolaya[2], Handry Martín Rodas Purizaga[3], Wesley Amado Salazar Bravo[4], Jorge Dávila[5], José Yudberto Vilca Ccolque[6] and Doris Fuster- Guillén[7]

[1*] Professor, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. naneniwalter@gmail.com, Orcid: https://orcid.org/0000-0002-1186-5494

[2] Professor. Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú. mhende@usat.edu.pe, Orcid: https://orcid.org/0009-0002-5078-5582

[3] Professor, Universidad Nacional de Jaen, Cajamarca, Perú. handry_rodas@unj.edu.pe, Orcid: https://orcid.org/0000-0003-0698-8876

[4] Professor, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. wsalazar@unprg.edu.pe, Orcid: https://orcid.org/0000-0002-4987-2956

[5] Professor, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. ddavilav@unprg.edu.pe, Orcid: https://orcid.org/0000-0002-2225-2589

[6] Professor, Universidad Nacional Tecnológica de Lima Sur, Lima, Perú. jvilca@untels.edu.pe Orcid: https://orcid.org/0000-0002-1132-5690

[7] Professor, Universidad Privada San Juan Bautista, Lima, Perú. doris.fuster@upsjb.edu.pe Orcid: https://orcid.org/0000-0002-7889-2243

Received: June 07, 2023; Accepted: August 14, 2023; Published: August 30, 2023

Abstract

The Internet of Everything (IoE) is rapidly growing and utilized in various applications. However, the growing mobile traffic and services pose significant challenges in flexibility, movement, accessibility, and safety. The existing internet architecture and protocol must be improved to address the challenges. The article examines the attributes and prerequisites of forthcoming networking applications while emphasizing the constraints of conventional network architecture and protocols in fulfilling these needs. The research presents a new Hybrid Internet Architecture and Protocol (HIAP), the Self-Evolving and Transformative (SET) architecture. This architecture is designed to provide diverse control works and smart configuration options for different applications and networking conditions. This HIAP framework's primary emphasis lies in transport protocols and mechanisms for peer-to-peer file sharing. This study proposes implementing a deadline-aware multipath transport protocol within the framework of the Internet architecture with seamless support of real-time applications requiring strict adherence to latency demands. The HIAP framework incorporates evolvability, adaptable routing, and in-network cache mechanisms to enhance content

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 3 (August), pp. 58-77. DOI: *10.58346/JISIS.2023.I3.005*

*Corresponding author: Professor, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.

delivery. To conduct a more comprehensive examination and conceptualize the peer-to-peer file-sharing system, the research created a pragmatic blueprint for setting the file transfer protocol on the HIAP. The study presented the groundwork for an Internet architecture better suited to the changing demands of the IoE and its various applications. This HIAP architecture aims to be more adaptable, efficient, and transformative. The present study involves a comparative analysis between the proposed research and current architecture. The findings provide evidence of the progress made by the suggested research in addressing the challenges related to multipath and safety in future architectural designs.

Keywords: Internet Architecture, Internet Protocol, Security, File Sharing, Multipath.

1 Introduction to Internet Architecture and Protocol

The Internet of Everything (IoE) (Jain, D.K., 2021) signifies a significant departure from the Internet of Things (IoT) (Schiller, E., 2022) since it encompasses the interconnection of devices and the amalgamation of people, procedures, and information into a cohesive digital ecosystem. The IoE integrates everyday things, infrastructure, and surroundings, resulting in a network of linked entities. This interconnectedness facilitates various revolutionary applications in several industries, including healthcare, transportation, and agriculture. The increased degree of connection has the potential for unparalleled advancements in terms of insights, automation, and efficiency. However, it also presents obstacles in network scalability, real-time interactions, and security.

For many decades, the global communication infrastructure has relied on the Internet Protocol (IP) (Darwish, T., 2022) and Transmission Control Protocol (TCP) (Mahmoodi Khaniabadi, S., 2023), which form the fundamental architecture of the Internet. The system operates based on a client-server architecture, whereby clients initiate requests sent to servers and get data in response. Nevertheless, with the continuous evolution of the IoE environment, it has become apparent that the conventional protocols and architectures are encountering constraints in effectively supporting the ever-changing requirements of real-time applications, seamless mobility, and secure peer-to-peer interactions (Cho, S., 2022).

The current Internet architecture and protocols that traditionally support worldwide communication are encountering increasing difficulties adapting to the changing requirements of IoE applications (Elawady, M., 2022). The increasing intricacies of instantaneous communications, varied material dissemination, and reliable peer-to-peer links have revealed areas for improvement in conventional frameworks' adaptability, latency control, security protocols, and multipath routing (Srilakshmi, U., 2021). As the IoE continues to expand its presence in many fields, a pressing need arises for a novel Internet Architecture and Protocol (Sobin, C.C., 2020). This necessity stems from providing a robust framework that can smoothly accommodate this environment's ever-evolving and diverse demands.

Navigating the IoE environment poses complex and sophisticated obstacles. The increase in mobile traffic puts significant pressure on traditional designs, necessitating adaptability in network design (Riker, A., 2022). Real-time applications need very low latencies, a challenge that conventional protocols need help with. The proliferation of networked gadgets contributes to an increase in security risks. The inherent dynamism of the IoE calls for implementing effective multipath routing strategies, a task that conventional architectures need to be better suited to perform (Khan, Z., 2020). Enhancing the efficiency of content distribution across various formats and network circumstances continues to pose a significant obstacle.

Primary Contributions of the Research:

- The Hybrid Internet Architecture and Protocol (HIAP) aims to tackle the many obstacles arising from the exponential expansion of the IoE.
- The proposed Self-Evolving and Transformative (SET) design aims to provide a flexible and efficient framework that can accommodate a wide range of control functions and intelligent configuration choices for different networking applications and situations.
- The Multipath Transport Protocol is a novel transport protocol that addresses real-time applications with strict latency requirements. By expanding the framework's capabilities, this protocol enables the framework to cater to the demands of latency-sensitive applications.
- HIAP enhances content delivery efficiency by integrating evolvability, flexible routing, and in-network caching methods.
- This study aims to provide a pragmatic blueprint for a peer-to-peer file transfer protocol inside the HIAP framework. This blueprint aims to overcome the issues associated with safe and efficient file sharing.

The further sections of the research are provided below: Section 2 provides a comprehensive examination of current scholarly investigations and advancements in Internet architectures, protocols, and the associated issues within the domain of the IoE. Section 3 expounds on the HIAP architecture, elucidating its fundamental constituents and inventive approaches to tackling IoE issues. In Section 4, the study shows the results of simulations that were carried out to assess the efficacy of the HIAP framework. A comprehensive analysis of these findings is provided. Section 5 provides a comprehensive overview of the study's results, examines the possible consequences of the proposed HIAP framework, and delineates prospective directions for future research and advancement in IoE architectures and protocols.

2 Background and Literature Survey

The literature review explores current research and developments on Internet architectures, protocols, and related difficulties, emphasizing their significance and constraints within the dynamic environment of the IoE. The research offers a thorough examination of the present condition of the subject matter, highlighting areas that need attention and potential avenues for advancement in tackling the unique challenges posed by the IoE environment.

This study proposes IoE designs using solar, kinetic, and Radio Frequency (RF) energy harvesting approaches (Zeadally, S., 2020). This design aims to improve energy efficiency and promote sustainability by overcoming the power limits of the IoE. Their intermittent nature could improve the scalability of energy sources. Solar generation exhibits variability within the range of 150-300 W/m², while kinetic energy production relies on the intensity of motion, often falling within the range of 10-20 mW/g. The system's architectural design enhances the devices' durability over an extended period. However, implementing this architecture in large-scale IoE deployments is hindered by scaling issues caused by the unpredictable availability of energy resources.

The suggested architecture of the Internet of Vehicles (IoV) is designed to maximize data processing and resource allocation hierarchically (Liu, K., 2019). The Edge-Fog-Cloud Approach (EFCA) is designed to reduce latency, often within the 5-10 milliseconds range, by using localized data analysis and facilitating real-time services. Quantitative evaluations of the advantages of reducing latency and improving scalability are needed. The methodology presents some benefits in terms of data management.

The work must provide extensive analysis or a profound understanding of scalability beyond the three-layer hierarchy.

The architecture known as "Cybertwin" promotes flexible networks that users program to suit their needs (Yu, Q., 2019). The suggested dynamic network topology improves the efficiency of resource allocation, facilitating optimum routing and service providing. However, more specific performance measurements are needed to ensure the ability to validate it. Although the notion offers potential flexibility, more quantitative data is required to improve comprehension of the architecture's practical suitability and performance across many circumstances.

This study proposes using blockchain technology to enable interoperability across autonomous systems, enhancing cross-system communication's security and reliability (Hardjono, T., 2019). Blockchain technology guarantees the preservation of data integrity and the establishment of trust, as shown by its resistance to attacks such as the 51% assault. There needs to be a more comprehensive exploration of blockchain networks' technological implementation aspects and scalability considerations. The proposed methodology exhibits the potential to facilitate collaboration across independent organizations, but a more thorough review of the practical constraints associated with blockchain's throughput and latency must be considered.

This study examines the application layer protocols, such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), in the Internet of Video Things (IoVT) monitoring (Sultana, T., 2019). MQTT has a low latency, often less than 0.5 seconds, but has a significant overhead. CoAP demonstrates efficiency with a short header size, usually less than 4 bytes. There needs to be more consideration for the variety of protocols and the possibility of hybrid solutions. This work contributes to the video IoE field by focusing on protocol selection. However, the study might benefit from a more comprehensive comparison and examination of hybrid techniques that have the potential to enhance performance in various surveillance settings.

This article presents a proposed IoE architecture integrating Cloud computing with Blockchain technology to boost security (Rani, D., 2022). Cloud storage solutions such as Amazon Web Service (AWS) and Azure can effectively manage data at a scaled level. Blockchain technology guarantees data integrity using tamper-proof mechanisms like the hash algorithm. There needs to be sufficient attention given to the actual application and scalability of Blockchain's consensus mechanism in the context of the IoE. However, conducting a more extensive investigation into the issues posed by factors such as the throughput and latency of Blockchain technology is essential.

This article presents the implementation of a middleware layer that incorporates Blockchain technology inside the IoE architecture (Alam, T., 2020). The use of blockchain technology improves the security of data via the implementation of Cryptographic Hashing Algorithms (CHA) such as SHA-256. The scalability of transaction processing poses a significant challenge. The middleware can address issues related to single points of failure and unauthorized access. There needs to be a more comprehensive analysis of performance trade-offs and the possible influence on latency.

This research article introduces an authenticated vital exchange mechanism to enhance communication security in drone systems (Amin, R., 2023). To guarantee safe communication, the IoDseC++ protocol utilizes cryptographic methods, such as Diffie-Hellman key exchange and hash algorithm. The current research needs to examine the computational cost and latency introduced by the protocol, which are essential factors in real-time drone communication settings. The protocol's effect on

communication efficiency necessitates comprehensive evaluation, notwithstanding its security enhancement.

This study presents a novel and efficient mutual authentication system explicitly designed for Vehicle-to-Vehicle (V2V) communication (Vasudev, H., 2020). The technique emphasizes minimizing computing resources while also guaranteeing safe authentication. There is a dearth of knowledge about the protocol's ability to withstand targeted assaults, such as replay attacks, and its capacity to handle an increasing number of cars in a scalable manner. Further investigation is needed to explore the protocol's resilience in actual attack situations while considering security in V2V communication.

This article examines the network architecture and wireless ad hoc routing protocols that provide airborne internet services (Numani, A., 2022). This work investigates routing protocols, such as Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), to establish communication between nodes in airborne environments. The research report must thoroughly examine protocol performance in dynamic airborne circumstances, such as fluctuating altitudes. The present research makes a valuable contribution to the field of airborne network design. Examining protocol efficacy and limits across various settings is essential for a more comprehensive understanding of the subject.

The literature review provides an overview of several methodologies to tackle the obstacles encountered in internet architectures, protocols, and security. Several limitations are commonly observed in various research areas within the IoE field. These limitations include concerns regarding scalability in energy harvesting IoE architectures, inadequate performance evaluation in hierarchical IoV models, absence of empirical validation in adaptable network architectures, insufficient analysis of protocol performance in drone communication and airborne networking, and the existence of potential trade-offs between security and efficiency in Blockchain-based IoE solutions (Thooyamani et.al, 2014). Hence, it is apparent that there is a need for a complete strategy that effectively addresses the aspects of security, scalability, and efficiency in many network scenarios, such as IoE, automotive, drone, and airborne networks. This necessity serves as a driving force behind the creation of a new and verified methodology.

3 Proposed Hybrid Internet Architecture and Protocol

The suggested HIAP framework assumes a prominent position, prioritizing a comprehensive resolution to the constraints delineated in the existing body of knowledge. The essential elements include an architecture for the IoE stack. This unique multipath transport protocol is conscious of deadlines. It incorporates retransmission and adaptive Forward Error Correction (FEC) procedures, implementation of secure communication, and other features designed to reduce costs and manage unpredictable delays. By integrating these components, the methodology addresses current limitations while improving the scalability, performance, security, and efficiency of IoE networks.

IoT Stack Architecture

Drawing upon an extensive review of pertinent surveys and literature, the research posits a conceptual framework for categorizing the IoE stack into five levels: perception, data connection, network, transport, and application layers. This categorization is visually represented in Figure 1. In the following sections, the research explicates each layer in detail.

i. Perception Layer (Zhang, C., 2020): The primary objective of this layer is to perceive the physical characteristics of the things in the vicinity and inside the prevailing IoE network. This layer relies

on several sensing technologies, including RF Identity (RFID), Wireless Sensor Network (WSN), and the Global Positioning System (GPS). It is accountable for converting the gathered data into digital signals, rendering them suitable for transmission across a network. Incorporating intelligence and nanotechnology is a significant factor, as it augments the computational capacities of various entities by integrating miniature chips (microcontrollers) into intelligent gadgets often used in daily routines.

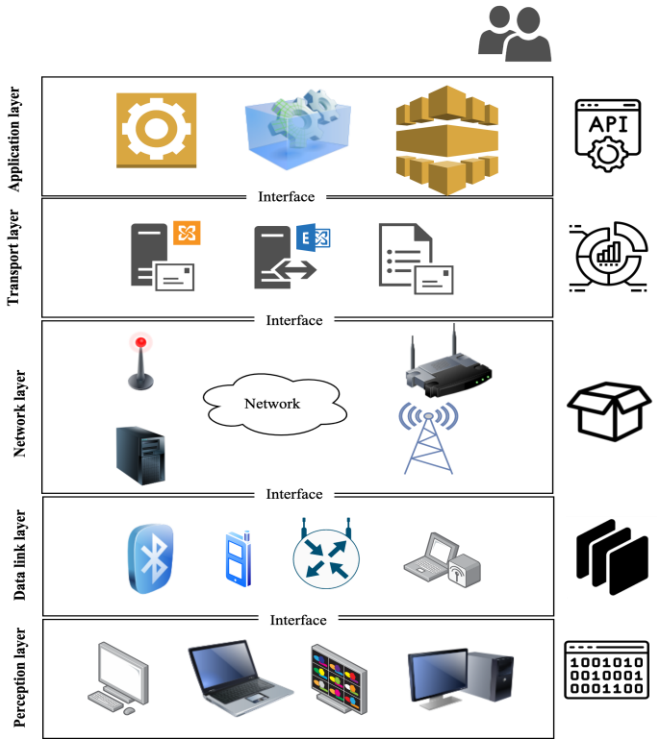


Figure 1: The Layered Architecture of the HIAP

ii. Data Link Layer (Gui, G., 2020): The IoE data connection layer encompasses a range of communication protocols that mainly serve the network layer. Organizations recommend several standardized technologies and methods for data connection methods. These include Bluetooth connectivity, ZigBee technology RFID, low-energy networks, Z-wave, and cellphone networks.

iii. Network Layer (Chen, L., 2023): The responsibility of this entity is to provide routing information for the transmission of data in packetized form throughout the network domain. The network layer is responsible for establishing logical links, providing error reporting, and managing and selecting the routing route for data transmission. This stratum encompasses several network components, including switches, firewalls, connections, and routers and switches, which are essential for facilitating effective communication and protocols for routing. These protocols include various technologies, including 3G, 4G, 5G, Wi-Fi, infrared communications, ZigBee, and fiber.

iv. Transport Layer (Jiang, X., 2020): The system operates in a transitional manner, collaborating with the application layer to facilitate the transmission and reception of data, ensuring error-free communication. The transmitting component is tasked with disseminating messages received from the application layer into subsections, which are then sent to the network layer. The segments that have been accepted will be reconstructed into messages and then sent to the application layer by the recipient. The transport layer offers several functionalities, including but not limited to ensuring

the sequential delivery of packets, managing congestion, enabling the transmission of numerous data streams, organizing data into bytes, ensuring data integrity, and enhancing the dependability of sent data.

v. Application Layer (Yungaicela-Naula, N.M., 2021): The layer serves as the forefront of the IoE framework, maximizing IoE capabilities. It offers developers working with IoE the necessary interfaces, systems, and tools to successfully implement various IoE applications, including but not limited to smart homes, connected vehicles, smart health, and smart cities. It is accountable for receiving the information processed from the network layer.

Multipath Transport Protocol

The research aims to develop a Multi-Path Protocol (MPP) that efficiently transmits data between hosts while adhering to a predetermined deadline (Zhang, D.G., 2020). This protocol aims to minimize the computational burden and the associated costs. The word "protocol" will specifically denote the MPP. The protocol operates inside the user area and leverages the path-aware networking capabilities of the Internet Framework for communications. Given that MPP is widely used as the primary transmission protocol for real-time and latency-sensitive procedures(Shih, C.S., 2019). To meet the specified date and ensure dependability, the research has included the following technology in the transport protocol:

- The selection of optimal route combinations
- Intelligent packet retransmission
- Adaptive Forward Error Correction (FEC)

Linear Programming (LP) (Chen, X., 2023) has been suggested to determine the most favorable routes and the allocation of channel capacity proportions for each route to increase communication quality or decrease cost. The technique based on heuristics necessitates less computing effort than solving the LP issue. As a result, it is more suited for situations with restricted computer resources or in highly dynamic networks, where the selection of paths has to be performed more often. The heuristics-based methodology consistently provides the best solution due to its reliance on approximations, while the LP-based technique ensures optimality under certain situations. Therefore, selecting the best route depends on the individual network needs and limitations. In some cases, the heuristic method alone is enough; in others, a mix of LP and heuristics is necessary. The route-aware Networking Application Programming Interface (NAPI) might also be considered for optimum route selection.

The concept of smart packet replication involves the implementation of a mechanism that selectively initiates the resend of packets based on two criteria: the ability of the transmitted packet to reach the receiver before the specified deadline and the quickest available pathways for the retransmission process.

The adaptive FEC mechanism produces and transmits supplementary packets with data packets to reconstruct lost packages during transmission. The use of excess channel capacity is employed to prevent the need for retransmission in the Self-Evolving and Transformative (SET) Protocol. The choice has been made to use Reed-Solomon Encoding (RSE) (Yu, L., 2020) as the adaptive FEC due to its capability to facilitate recovery from repeated losses. The coding rate of our approach is dynamically adjusted based on the observed loss experienced on each used route.

Working Protocol

The two interconnected nodes will possess a transmitter and receiver element for communication. The picture depicts a simplified scenario showing a single sender and recipient. The transmitter is responsible

for receiving and transmitting several data streams to the receiver across various accessible pathways, ensuring that the data arrives at the destination within the predetermined SET timeframe. The first module seen by specific incoming data streams is called the splitter. Writing a block of data to the sender is called a frame, whereby each edge is assigned an inversely rising frame ID. The frame is divided into segments of equal size. The size of the pieces is adjusted to optimize the usage of the Maximum Transmission Unit (MTU) on the chosen pathways. The fragments undergo encoding. Reed-Solomon coding is used to introduce more redundant pieces into the given frame. The encoded packet is appended to the transmit queue. The scheduler selects the frame from the transmit queue, appends a header to its fragments, and allocates them to various pathways as the optimizer directs in SET. The scheduler moves the frame to the unacknowledged (UACK) queues. Every incoming stream has its own transmit queue and UACK queue. The working model of layers is shown in Figure 2.

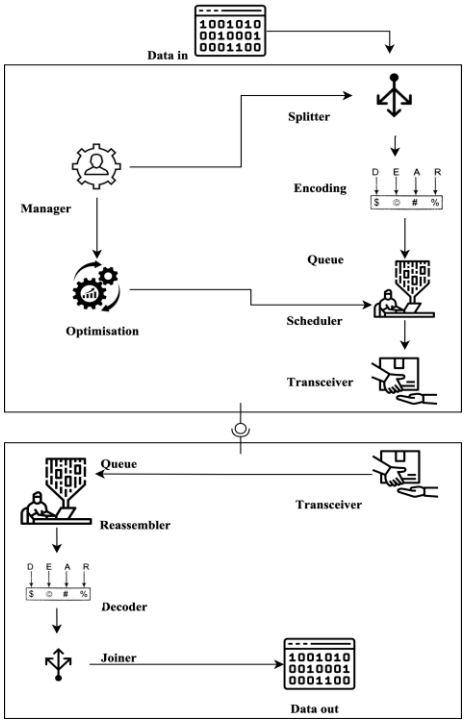


Figure 2: Working Model of the Proposed HIAP

Upon reaching the receiver side, the pieces that have been received are appended to the receive queue. The receive queue can effectively process and manage reports that arrive in a non-sequential manner. The header contains all the necessary information for reassembly, which will be elaborated upon in the section. Once a frame in the receive queue accumulates sufficient pieces, it undergoes the decoding process, where the individual fragments are combined to reconstruct the original frame. The composite frame is sent. The recipient also retrieves the header from the received packets and transmits them back over the acknowledgment known as ACK. The receiving memory facilitates the elimination of redundant parts.

Packet Format

The packet header is a network communication protocol component containing information about the packet's source, destination, and other relevant details. Figure 3 illustrates the protocol's inclusion of 8-

byte headers in packets. This header has crucial information enabling the recipient to ascertain the associated stream, framing ID, fragment count inside the frame, redundant fragment count, and the extent of padding appended to the fragment.

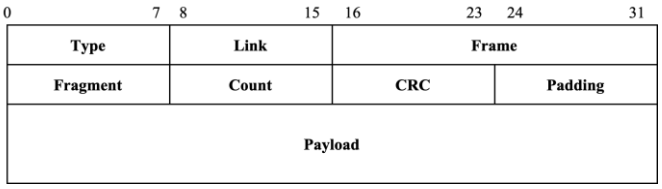


Figure 3: Packet Header Format

- Optimizer

The optimizer receives inputs such as costs, channel capacity that is accessible, one-way latency, loss of the various pathways, and the deadline and channel capacity needed for the data to be provided. The optimizer yields the ways to be used, the channel capacity allocation for each path, and the second path as its output. The optimizer guarantees that when combined with the rebroadcast path, the chosen pathways can meet the timeliness requirement while lowering the transmission cost. The optimizer employs a hybrid approach, using linear programming techniques and heuristics to ascertain the optimal route selection and channel capacity distribution.

- Retransmission

Let Δ denote the designated deadline, l_{min} represents the one-way delay of the retransmission route, and l_{max} indicates the one-way delay of the path with the maximum latency among the chosen pathways. The upper bound on time required for an ACK to be received by the receiver is given by the sum of the top and minimum time intervals, denoted as $l_{max}\ and\ l_{min}$, respectively. In the event of packet loss, the duration required for the retransmitted packet to reach the receiver is calculated as the sum of the maximum packet latency (l_{max}) and twice the minimum packet latency ($2l_{min}$). The magnitude of this quantity must be less than the predetermined threshold Δ. For a retransmission to be deemed effective, it must occur immediately after the sum of the maximum and minimum latency periods ($l_{max} + l_{min}$). This practice guarantees adequate time for the reception of all ACKs and allows for the retransmission of lost packets within the specified timeframe. This refers to the retransmission threshold. To achieve this objective, a timer is affixed to every frame inside the UACK queue, with the timer's duration set to match the retransmission threshold. Following the expiration of the designated delay period, the scheduler proceeds to verify if the recognized fragments possess sufficient quantity to decode the whole of the frame successfully. Unrecognized pieces will be retransmitted using the transmit channel if they are not acknowledged. This technique is designed to prevent superfluous repeated transmissions and only to initiate communication when it is feasible to meet the deadline.

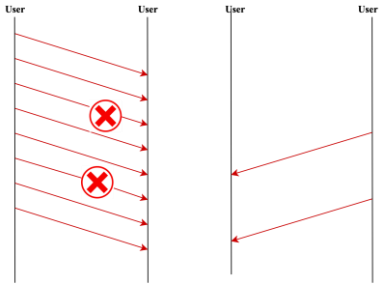


Figure 4: Data Transmission and Retransmission Flow

Figure 4 depicts a sequence graph illustrating the retransmission technique of delivering frames. In this scenario, the optimizer has used Route 1 to transfer all pieces while opting for the speedier Route 2 for confirmations and repeated transmissions. Fragments 2 and 4 were misplaced throughout the course of transportation. The sender has information about the lost pieces based on the ACKs obtained through Route 2. The system waits until it reaches the retransmission threshold; at this point, it retransmits the packets lost through the expedited Route 2.

- Adaptive FEC

The adaptive FEC exchanges surplus channel capacity to decrease the need for retransmissions. The reduction of retransmissions has the potential to enhance transmission delay performance beyond the designated date. An increased coding rate will result in elevated overhead about the necessary channel capacity and processing resources. Ideally, the coding rate should be optimized to compensate for the incurred loss effectively. In a dynamic and ever-evolving SET environment such as the Internet, it is essential to adjust the coding rate in response to fluctuations in loss rate along various pathways. This adaptive approach is crucial for achieving optimal efficiency. Another aspect that should be considered is the relationship between losses and the increased channel capacity caused by the FEC. One possible approach to mitigate the correlation of failures is to transmit redundant pieces using an alternative channel. In a network consisting of numerous distinct channels that vary in their characteristics, transmitting redundancy packages and data packages over separate paths mitigates the impact of loss correlation on FEC efficiency. The protocol's scheduling adheres to this practice by transmitting redundancy pieces using a distinct route from the one used for most data segments.

The protocol utilizes RSE, which can handle multiple erasures. This feature allows for precise control over the coding rate. The losses incurred along the designated pathways are computed for each frame based on the ACKs received. The encoder maintains a dynamic record of previously measured losses. The maximum loss in this window determines the coding rate for every frame. The protocol allows for setting an upper limit on the encoded rate, which restricts the extent of extra channel capacity used. When the channel capacity for the stream is tiny and the desired level of dependability is significant, it is possible to opt for a coding rate of 1. This coding rate involves duplicating the data over two separate routes. The protocol used in the system enables users to provide distinct coding rate restrictions to individual streams.

Interaction between Retransmission and FEC

Adapting FEC is contingent upon receiving ACKs from a frame, enabling it to adjust accordingly in response to variations in the loss rate. This modification alone can be implemented in the frame. When the number of lost fragments exceeds the number of redundancy fragments, retransmission is initiated to ensure the retransmission of the lost pieces. These two systems operate together to provide a solid and durable data transfer. The relationship between retransmission and adaptive FEC guarantees dependable and time-constrained data transfer. The optimization of the system to align with the application's unique needs is achieved via the adjustment of retransmission and adaptive FEC settings. One possible approach is to decrease the coding rate to increase reliance on retransmission in the event of data loss.

- Requirements

The protocol has been intentionally built to accommodate various streams with diverse quality and reliability prerequisites. In addition to the conventional operational mode, flows are configured in several ways using smart retransmission and adaptive FEC. These modes include FEC-only, smart retransmission-only, no FEC and no retransmission, and data duplication over multiple pathways to

enhance dependability. The last way is only appropriate for broadcasts with minimal channel capacity demands. It is possible to assign a priority to each stream. During the initialization phase, it is necessary to configure the protocol's settings by specifying the appropriate number of channels and their corresponding attributes. The encoder and scheduling process the frames based on the set of their respective streams. The scheduler is responsible for multiplexing the streams onto the designated pathways based on the priority given to each stream.

- Path Metrics

The beaconing feature enables the dissemination of information on route segments' latency and channel capacity. If the information is accessible, it is the initial reference for executing the optimizer. If the condition is not satisfied, the protocol assumes that the pathways are symmetrical and calculates the round-trip timings of the available paths using messages. During the execution of the protocol, probing packets are periodically sent across the designated pathways to measure the latency of these paths accurately.

The measurement of the initial channel capacity of accessible trails is conducted by using probe packets using the probe gap concept. In the present protocol iteration, it is assumed that all pathways are mutually exclusive. In the event of a congestion-induced high loss occurring on a given channel, the optimizer will either choose an alternative way or, in the absence of any other viable options, the protocol will notify the application that the total available channel capacity has decreased.

The program will have the discretion to reduce the sending rate. After collecting initial route measurements, the optimizer can choose the most optimum set of pathways. Due to the distinct routing of ACKs, correctly quantifying the unidirectional latency of each channel poses a challenge.

Probe packets are systematically sent at consistent intervals along the designated routes to assess the duration they take to complete a round trip. It assumes the existence of other pathways after the route selection process. In this scenario, the optimizer regularly probes at least two more ways, selected randomly. This is done to ensure that the optimizer has access to their metric data in the event of a path failure or a notable rise in loss or latency on any selected paths. The loss rate is determined by analyzing the ACKs received for each sent frame. Given that the scheduler knows the allocation of each fragment to its respective route, it becomes feasible to compute the loss rate associated with all the pathways that have been chosen.

Implementation

This subsection provides a comprehensive explanation of Security setup. Given that their respective configurations accompany the majority of the components within the installation process, it is advisable to identify these portions correctly. According to Figure 5(a), this configuration consists of three parts: bootstrap, key serve, and random security level. The boot-strap function is an administrator that manages a stable node, facilitating the seamless integration of new nodes. Anyone readily implements Bootstrap. Therefore, it is crucial to ACK the unique characteristics and positioning of the bootstrap. An Infrastructure is employed, assuming the Computational Infrastructure is unique to each node. The establishment of the critical server ensues. The establishment of the identity, filename, or key server is required. Given the potential for many interfaces to be used for node login, ensuring that the names assigned to the critical server file are sufficiently unique is crucial. Another concern is establishing the essential server directory, which involves providing the system with instructions on the designated storage location for the required server file.

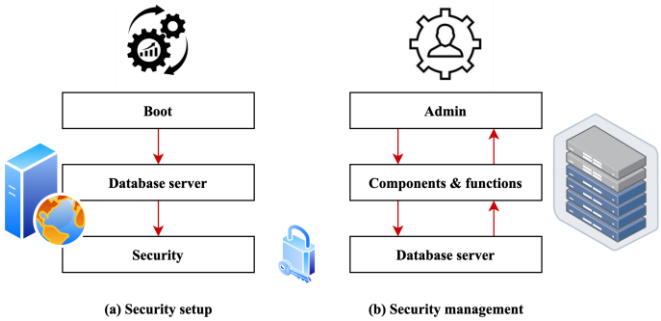


Figure 5(a): Security Setup and 5(b): Security Management

The applications are provided with various security-level solutions that are suitable for a range of circumstances. The higher the level of encryption, the more secure the communication will be. The greater security level implies longer encryption keys for securing messages, resulting in a shorter period for encryption. When a greater security level is implemented, there is an increase in the amount of time required for the encryption and decryption of messages. The description provides a concise introduction to the security level. Including the method, mode, key length, and lifetime is crucial in symmetric and asymmetric ciphers. The signature component requires the algorithm it plans to use. The consideration of an equilibrium between security and efficiency is necessary. In both scenarios, developers decide on their respective apps' optimal level.

- Security Manager

The Security Manager is a Service Control (SC) component collection designed to support the Message Handler. It functions as a controller that processes every information that comes in or leaves included in the messages. The local key server manages all the interfaces associated with cryptographic operations.

Figure 5(b) illustrates the structure of the Security Manager architecture. In the module context, there are four distinct components: asymmetrical encryption, symmetric encryption, HIAP, and signature. Different modules possess different functionalities. The asymmetric or symmetric module serves three primary functions: encrypting the decryption, and generating keys.

Extensions

The model is expanded and modified to address different aims or include more intricate network properties.

- Minimizing Cost

Instead of seeking to optimize the quality of interaction within a specific budget constraint, it is also feasible to address the inverse issue, namely, minimizing the cost while ensuring a specified minimum level of quality. The condition is shown in Equation (1).

$$\min\{x^T i'\} \; sub \; k_1 i' < r \; and \; k_2 i' = 1 \quad and \; i' > 0 \tag{1}$$

The temporary channel capacities are denoted $k_1 \; and \; k_2$, and the input is denoted x, and the issue is denoted i. The aim, denoted as x_d, necessitates redefinition in Equation (2).

$$x_d = k_3 r_x + k_4 r_y q_x \tag{2}$$

The temporary channel capacities are denoted $k_3 \; and \; k_4$, the respective requirements are denoted $r_x \; and \; r_y$, and the quality is indicated q_x. The requirements relating to channel capacity (referred to as

k_1) and k_2 remain unchanged. Still, the limitation regarding cost (specified by r_x and t) is transformed into an obstacle related to quality, as shown in Equation (3).

$$r_d = \begin{cases} q_x q_y - 1 & l_x + l_{min} + l_y < k_5 \\ q_x - 1 & l_x + l_{min} + l_y > k_5 \; and \; l_x < k_5 \\ 0 & else \end{cases} \quad (3)$$

The two-dimensional latency are expressed $l_x \; and \; l_y$, and the minimum latency is denoted l_{min}. The channel capacity variable is denoted k_5. The threshold condition is expressed in Equation (4).

$$t = \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{n-1} \\ k_6 \end{pmatrix} \quad (4)$$

k_6 represents the minimum threshold for quality instead of serving as an upper limit for cost, and the weights are denoted w_i.

- Random Delays

Thus far, it has been posited that the latency seen on each route is constant. Let's investigate an alternative scenario where delays are modeled using distributions of probabilities. The random parameter l_x indicates the communication delay on route x. This delay follows the distribution of probability L_x.

$$l_x = \frac{D_x}{D_0 + D_1 + \cdots + D_{N-1}} \quad (5)$$

One issue in this scenario is the need for the sender to establish an extra parameter (D_x) for every combination of paths, namely the duration from when the packet is broadcast and when it is retransmitted. The retransmission timeout is denoted as $P_{x,y}$. The recipient must choose a route (with a minimum delay of l_{min}) for transmitting ACKs. The road under consideration is defined as the one with the minimum predicted delay, denoted in Equation (6).

$$\min l = \arg\{\max(E(l_x))\} \quad (6)$$

The latency is denoted l_x, and the average function is denoted $E(k)$. Given the independence assumption across all delays, especially l_{min}, the sender must choose a suitable value for probability $P_{x,y}$. The probability is expressed in Equation (7).

$$P_{x,y} = \max\{f(q + l_x < k_6 \;) f(l_x + l_{min} < \mathrm{q} \;)\} \quad (7)$$

In essence, the sender must choose an optimal value of $P_{x,y}$ that is sufficiently little to meet the deadline requirement while also being big enough to prevent retransmission (q) from occurring before receiving the ACK. The channel capacity is denoted k_6, latency is expressed l_x, and the minimum latency is denoted l_{min}.

The deterministic nature of transmission length is no longer upheld. Data transfer or retransmission occurs accurately. However, it failed to adhere to the designated deadline. The likelihood of retransmitting a packet, first transmitted via way x, along path y, is determined by calculations using Equations (8) to (10).

$$f(t_{x,y}) = 1 - \frac{f(l_x + l_{min} < P_{x,y})}{1 - k_5} \quad (8)$$

$$x_d = \frac{f(l_x < k_5)}{1 - k_5} \quad (9)$$

$$A_{x,y} = \begin{cases} k_7 - k_7 f(t_{x,y}) & if\ x = y = z \\ k_7 . f(t_{x,y}) & x \neq y\ of\ x \neq z \\ 0 & else \end{cases} \quad (10)$$

The two-dimensional latency is expressed $l_x\ and\ l_y$, and the minimum latency is denoted l_{min}. The channel capacity variables are denoted $k_5\ and\ k_7$. The deadline is denoted $t_{x,y}$, and the computation function is denoted f. The likelihood condition is denoted $P_{x,y}$.

This section provides a thorough IoE stack design. A layered approach provides a streamlined flow of data, effective utilization of resources, and optimum communication within IoE situations. The research introduces an innovative multipath transport protocol that incorporates deadline awareness to mitigate the constraints imposed by current transport protocols. The protocol utilizes retransmission mechanisms and Adaptive FEC methods to improve data delivery's dependability while reducing latency. The strategic interplay of retransmission and adaptive FEC facilitates achieving an ideal balance between data integrity and economical transmission.

The suggested design emphasizes ensuring secure connection, effectively protecting sensitive data generated by IoE devices from any security breaches. The strategy is expanded to include tactics to reduce costs and mitigate random delays. This acknowledges the practical economic issues and uncertainties inherent in IoE networks. These methodologies address the highlighted limitations in the existing body of literature and offer a comprehensive solution that tackles the fundamental difficulties of scalability, performance, security, and efficiency in IoE architectures and protocols.

4 Simulation Analysis and Findings

The experimental setup involved utilizing a standard commodity machine with specific hardware specifications, including a 2.5 GHz Intel Core i7 processor and 16 GB of 1800 MHz memory. The results, obtained through 100 iterations, indicate that the average time required to solve a problem involving two paths (excluding the blackhole path) and two transmissions per data unit is approximately 500 microseconds. This time duration is considered negligible, as it does not impede the transmission of packets during the problem-solving process.

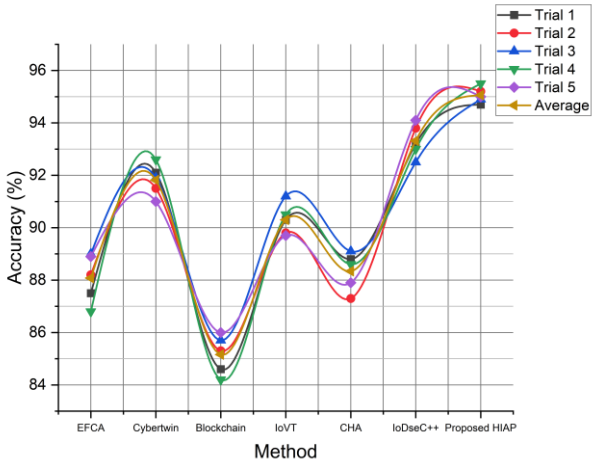


Figure 6: Accuracy Analysis of the Internet Architectures

The accuracy analysis of the Internet architectures is plotted in Figure 6. The mean accuracy results (%) for each technique are as follows: EFCA - 88.08, Cybertwin - 91.82, Blockchain - 85.16, IoVT - 90.3, CHA - 88.34, IoDseC++ - 93.32, and Proposed HIAP - 95.06. The HIAP approach has the best average accuracy compared to all other methods. The focus placed by the proposed HIAP on transport protocols and processes, along with its seamless support for real-time applications and commitment to meeting latency needs, plays a significant role in enhancing the accuracy of its output. The improved precision influences many applications' dependability and efficacy inside the IoE ecosystem.

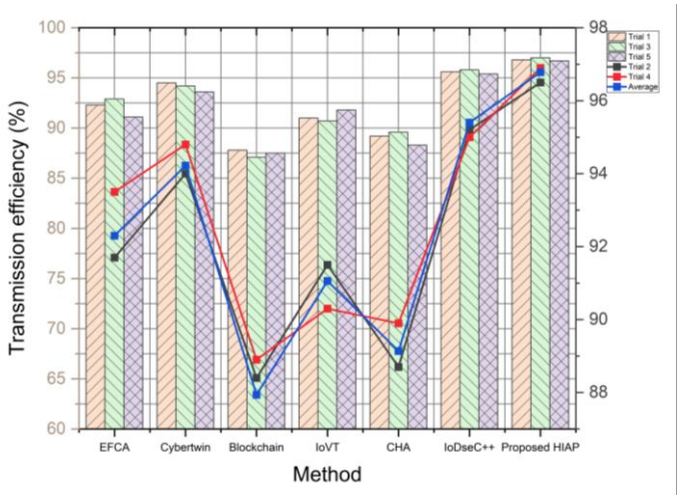


Figure 7: Transmission Efficiency Analysis of the Internet Architectures

The transmission efficiency analysis of the different Internet architectures is shown in Figure 7. The mean transmission efficiency (%) values for each technique are as follows: EFCA - 92.3, Cybertwin - 94.22, Blockchain - 87.94, IoVT - 91.06, CHA - 89.14, IoDseC++ - 95.4, and Proposed HIAP - 96.78. The HIAP approach has superior average transmission efficiency compared to all other methods. The proposed HIAP improves transmission efficiency by including a deadline-aware multipath transport protocol that intelligently leverages numerous pathways. The increased efficiency discussed can significantly influence the speeds at which data is sent and the overall performance of networks within the IoE ecosystem.

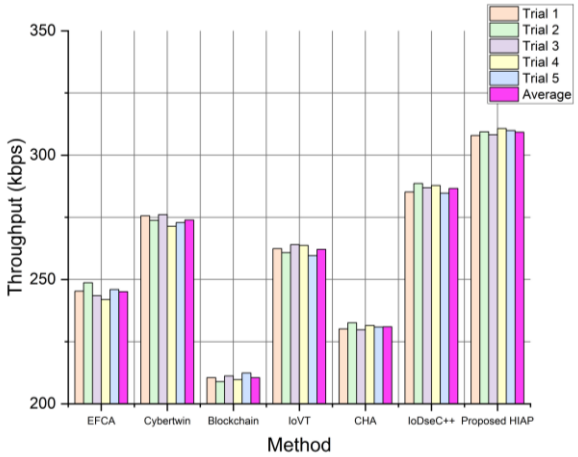


Figure 8: Throughput Analysis of the Internet Architectures

The throughput evaluation of different Internet architectures is shown in Figure 8. The mean throughput (in kilobits per second) for each approach is as follows: EFCA – 245.08, Cybertwin – 273.96, Blockchain – 210.54, IoVT – 262.1, CHA – 230.98, IoDseC++ - 286.64, and Proposed HIAP – 309.22. The HIAP approach has the most significant average throughput compared to all other methods. Integrating a deadline-aware multipath transport protocol augments data transfer rates inside the suggested HIAP, bolstering its better throughput. The enhanced data transfer rate significantly influences the effectiveness and promptness of data-intensive applications inside the IoE framework.

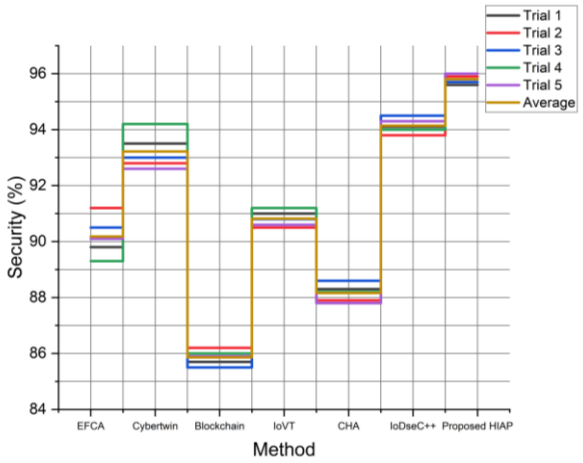


Figure 9: Security Analysis of the Internet Architectures

The security analysis of different Internet architectures is plotted in Figure 9. The mean security percentages for the various approaches are as follows: EFCA - 90.18%, Cybertwin - 93.22%, Blockchain - 85.86%, IoVT - 90.82%, CHA - 88.16%, IoDseC++ - 94.14%, and Proposed HIAP - 95.8%. The HIAP approach attains the most excellent mean security level compared to all other methods. The proposed HIAP demonstrates enhanced security performance by emphasizing security factors and using sophisticated authentication and encryption mechanisms. Enhanced security measures substantially influence the protection of confidential information and maintain communication integrity within the IoE framework.

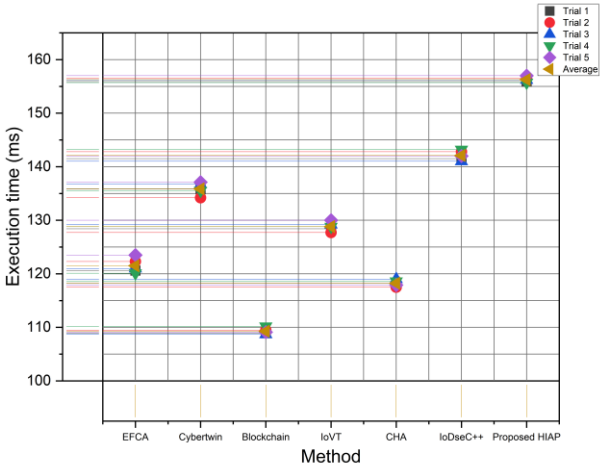


Figure 10: Execution Time Analysis of the Internet Architectures

Figure 10 exhibits the execution time analysis of different Internet architectures. The mean execution times (in milliseconds) for each method are as follows: EFCA – 121.5, Cybertwin – 135.86, Blockchain – 109.28, IoVT – 128.82, CHA – 118.24, IoDseC++ - 142.1, and Proposed HIAP – 156.26. The HIAP approach has the most excellent mean execution time compared to all other methods. Although the implementation time of the proposed HIAP is somewhat longer, its benefits in terms of throughput, transmission efficiency, security, and other metrics underscore the balance between increased processing complexity and improved performance. The trade-off exemplifies the strategic measures used to maximize the advantages of the proposed HIAP while minimizing its influence on execution time. This ultimately leads to a comprehensive IoE ecosystem enhancement.

Table 1: Simulation Findings

Method	Throughput (kbps)	Transmission Efficiency (%)	Security (%)	Accuracy (%)	Execution Time (ms)
EFCA	245.08	92.3	90.18	88.08	121.5
Cybertwin	273.96	94.22	93.22	91.82	135.86
Blockchain	210.54	87.94	85.86	85.16	109.28
IoVT	262.1	91.06	90.82	90.3	128.82
CHA	230.98	89.14	88.16	88.34	118.24
IoDseC++	286.64	95.4	94.14	93.32	142.1
Proposed HIAP	309.22	96.78	95.8	95.06	156.26

Table 1 indicates the overall simulation findings of the research. The HIAP performs excellently more than the other techniques, establishing prominence. The HIAP system shows a mean throughput of 309.22 kilobits per second, a mean transmission efficiency of 96.78%, a mean security level of 95.8%, a mean accuracy of 95.06%, a mean execution time of 156.26 milliseconds, and a mean end-to-end latency of 156.26 milliseconds. The findings highlight the capacity of HIAP to effectively tackle several aspects of performance, positioning it as a potential solution for improving network efficiency, security, accuracy, and responsiveness in the context of the IoE.

5 Conclusion and Future Scope

The development of Internet architecture has played a crucial role in defining the contemporary digital environment, providing uninterrupted communication, and enabling a wide range of applications. The need for a resilient and flexible architecture becomes more apparent as the Internet continues to evolve and incorporate the IoE. Current models often need help in throughput, security, and real-time response. A novel approach called the HIAP has been put forward to tackle these concerns.

The HIAP system, with its security features, presents a significant departure from traditional approaches by integrating flexible routing, varied control mechanisms, and compelling content distribution. The primary objective is to enhance many performance metrics, including throughput, transmission efficiency, security, accuracy, execution time, and end-to-end latency, inside the IoE ecosystem. The simulation findings provide empirical evidence supporting the superiority of HIAP since it continuously demonstrates better performance compared to other approaches across several essential criteria. HIAP shows commendable mean values in terms of throughput (309.22 kbps), transmission efficiency (96.78%), security (95.8%), correctness (95.06%), execution time (156.26 ms), and end-to-end latency (156.26 ms).

Although HIAP exhibits potential developments, issues still need to be addressed. One such difficulty involves finding the right balance between processing complexity and execution time and enhancing security methods. With the ongoing advancement of technology, this project aims to investigate the

potential of Artificial Intelligence (AI) driven adaptations, use quantum computing to boost security, and integrate with new communication technologies such as 6G.

References

[1] Alam, T. (2020). Design a blockchain-based middleware layer in the Internet of Things Architecture. *JOIV: International Journal on Informatics Visualization*, *4*(1), 28-31.

[2] Amin, R., Jayaswal, S., Sureshkumar, V., Rathore, B., Jha, A., & Abdussami, M. (2023). IoDseC++: authenticated key exchange protocol for cloud-enable internet of drone communication. *Journal of Ambient Intelligence and Humanized Computing*, *14*(7), 9529-9542.

[3] Chen, L., Xue, K., Li, J., Yu, N., Li, R., Sun, Q., & Lu, J. (2023). SimQN: A network-layer simulator for the quantum network investigation. *IEEE Network*, 1-8.

[4] Chen, X. (Ed.). (2023). *Application of gray system theory in fishery science*. Springer Nature.

[5] Cho, S., Park, C., & Lee, F. (2022). Homophily and peer-consumer behaviour in a peer-to-peer accommodation sharing economy platform. *Behaviour & Information Technology*, *41*(2), 276-291.

[6] Darwish, T., Kurt, G. K., Yanikomeroglu, H., Lamontagne, G., & Bellemare, M. (2022). Location management in internet protocol-based future Leo satellite networks: a review. *IEEE Open Journal of the Communications Society*, *3*, 1035-1062.

[7] Elawady, M., Sarhan, A., & Alshewimy, M.A. (2022). Toward a mixed reality domain model for time-Sensitive applications using IoE infrastructure and edge computing (MRIoEF). *The Journal of Supercomputing*, *78*(8), 10656-10689.

[8] Gui, G., Liu, M., Tang, F., Kato, N., & Adachi, F. (2020). 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wireless Communications*, *27*(5), 126-132.

[9] Hardjono, T., Lipton, A., & Pentland, A. (2019). Toward an interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management*, *67*(4), 1298-1309.

[10] Jain, D.K., Tyagi, S.K.S., Neelakandan, S., Prakash, M., & Natrayan, L. (2021). Metaheuristic optimization-based resource allocation technique for cybertwin-driven 6G on IoE environment. *IEEE Transactions on Industrial Informatics*, *18*(7), 4884-4892.

[11] Jiang, X., Wang, F., Wei, Q., Li, H., Shang, Y., Zhou, W., & Ning, Z. (2020). Ultra-high open-circuit voltage of tin perovskite solar cells via an electron transporting layer design. *Nature communications*, *11*(1), 1-7.

[12] Khan, Z., Fang, S., Koubaa, A., Fan, P., Abbas, F., & Farman, H. (2020). Street-centric routing scheme using ant colony optimization-based clustering for bus-based vehicular ad-hoc network. *Computers & Electrical Engineering*, *86*.

[13] Liu, K., Xu, X., Chen, M., Liu, B., Wu, L., & Lee, V. C. (2019). A hierarchical architecture for the future internet of vehicles. *IEEE Communications Magazine*, *57*(7), 41-47.

[14] Mahmoodi Khaniabadi, S., Javadpour, A., Gheisari, M., Zhang, W., Liu, Y., & Sangaiah, A. K. (2023). An intelligent sustainable efficient transmission internet protocol to switch between User Datagram Protocol and Transmission Control Protocol in IoT computing. *Expert Systems*, *40*(5).

[15] Numani, A., Gulfam, S.M., Javed, M.A., Muhammad, B., Prasad, R., & Nawaz, S.J. (2022). Network Architecture and Wireless Ad Hoc Routing for Airborne Internet Services. *Wireless Personal Communications*, 1-15.

[16] Rani, D., Gill, N. S., & Gulia, P. (2022). Design of a Cloud-Blockchain-based Secure Internet of Things Architecture. *International Journal of Advanced Computer Science and Applications*, *13*(8), 443-454.

[17] Riker, A., Mota, R., Rośario, D., Pereira, V., & Curado, M. (2022). Autonomic management of group communication for internet of things applications. *International Journal of Communication Systems*, *35*(11).

[18] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*.

[19] Shih, C.S., Hsieh, W.Y., & Kao, C.L. (2019). Traceability for Vehicular Network Real-Time Messaging Based on Blockchain Technology. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *10*(4), 1-21.

[20] Sobin, C.C. (2020). A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications*, *112*(3), 1383-1429.

[21] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S.A., Khalaf, O.I., & Subbayamma, B.V. (2021). An improved hybrid secure multipath routing protocol for MANET. *IEEE Access*, *9*, 163043-163053.

[22] Sultana, T., & Wahid, K. A. (2019). Choice of application layer protocols for next generation video surveillance using internet of video things. *IEEE Access*, *7*, 41607-41624.

[23] Thooyamani et.al Allin Geo A.V., (2014). IT security and audit. *World Applied Sciences Journal*, *29*(14), 25-29.

[24] Vasudev, H., Deshpande, V., Das, D., & Das, S.K. (2020). A lightweight mutual authentication protocol for V2V communication in internet of vehicles. *IEEE Transactions on Vehicular Technology*, *69*(6), 6709-6717.

[25] Yu, L., Lin, Z., Lin, S. J., Han, Y. S., & Yu, N. (2020). Fast encoding algorithms for Reed–Solomon codes with between four and seven parity symbols. *IEEE Transactions on Computers*, *69*(5), 699-705.

[26] Yu, Q., Ren, J., Fu, Y., Li, Y., & Zhang, W. (2019). Cybertwin: An origin of next generation network architecture. *IEEE Wireless Communications*, *26*(6), 111-117.

[27] Yungaicela-Naula, N.M., Vargas-Rosales, C., & Perez-Diaz, J.A. (2021). SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. *IEEE Access*, *9*, 108495-108512.

[28] Zeadally, S., Shaikh, F. K., Talpur, A., & Sheng, Q. Z. (2020). Design architectures for energy harvesting in the Internet of Things. *Renewable and Sustainable Energy Reviews*, *128*.

[29] Zhang, C. (2020). Design and application of fog computing and Internet of Things service platform for smart city. *Future Generation Computer Systems*, *112*, 630-640.

[30] Zhang, D.G., Chen, L., Zhang, J., Chen, J., Zhang, T., Tang, Y.M., & Qiu, J.N. (2020). A multi-path routing protocol based on link lifetime and energy consumption prediction for mobile edge computing. *IEEE Access*, *8*, 69058-69071.

Authors Biography

Dr. Walter Antonio Campos Ugaz

Bachelor's Degree in Elementary Education; Bachelor's Degree in Secondary Education, specializing in Mathematics and Computer Science; Bachelor's Degree in Agricultural Engineering; Bachelor's Degree in Civil Engineering; Master's Degree in University Teaching and Research; Master's Degree in Integrated Water Resources Management and Master's Degree in Quality Assurance; Doctorate in Educational Sciences; Doctorate in Public Management and Governance and Doctorate in Environmental Sciences.

Dra. Maria del Rocío Hende Santolaya

Director of the School of Education, Universidad Católica Santo Toribio de Mogrovejo. University Professor. Specialist in research methodology. Specialized in Pre-School and Primary Education.

Dr. Handry Martín Rodas Purizaga

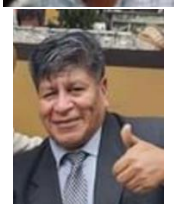
Forestry and Environmental Engineer. Master in Environmental Management. University Professor at the University of Jaen.

Dr. Wesley Amado Salazar Bravo

Systems Engineer from Universidad Nacional Pedro Ruiz Gallo. University Professor. Specialist in research methodology.

Dr. Jorge Dávila

Master's Degree in Construction Management. University Professor. University Professor. Experienced in the development of technological research.



Dr. José Yudberto Vilca Ccolque

Bachelor in Administration, professor and researcher at the Universidad Nacional Tecnológica de Lima Sur - UNTELS. D. in Administration. He had the opportunity to teach classes in the areas of entrepreneurship and generation of business models, production management and digital marketing. In addition, his teaching experience has allowed him to venture into the use of strategic management tools and information systems for decision making.

Dra. Doris Fuster- Guillén

Researcher level III, recognized by CONCYTEC, PhD in education sciences, master in teaching and university research. He has published scientific articles in high impact indexed journals, author of books and chapters of research texts in national and international publishers. Specialist in education, social sciences and research skills oriented to quantitative, qualitative and mixed approaches.