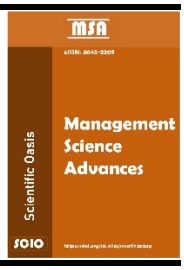
SCIENTIFIC OASIS

Management Science Advances

Journal homepage: www.msa-journal.org
eISSN: 3042-2205



Modern Information and Communication Technology Platforms: Advancing SecuDroneComm Management

Rexhep Mustafovski[1,*]

[1] Ss. Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Rugjer Boshkovikj, Skopje, Republic of North Macedonia

ARTICLE INFO

Article history:
Received 10 August 2025
Received in revised form 24 September 2025
Accepted 20 November 2025
Available online 24 November 2025

Keywords:
Information and Communication Technology Platforms; Management Communications; Unmanned Aerial Vehicles; Communication Advances; Communication Systems

ABSTRACT

The rapid advancement of information and communication technology (ICT) solutions has significantly changed the landscape of secure communication systems, especially in scenarios involving unmanned aerial vehicles (UAVs) and real-time data exchange. SecuDroneComm, a hybrid platform created for secure, low-latency communication between drones and command centers, represents an innovative management approach to tackling issues related to data security, latency, and scalability. This paper provides a thorough comparative analysis of SecuDroneComm alongside leading ICT platforms, including ITU-T X.805 frameworks, SmartNet architecture for energy systems, and federated global identity frameworks for mobile and wireless communications. By exploring these systems, we pinpoint essential design principles and innovations that have influenced secure management communication platforms, with a focus on encryption, data integrity, server architecture, and hybrid deployment strategies. The findings highlight the platform's flexibility in managing critical situations like battlefield intelligence, disaster response, and public health monitoring. Additionally, the analysis investigates possible improvements, such as the integration of 5G technologies, blockchain for data validation, and enhanced access control systems. SecuDroneComm's cutting-edge architecture, which merges security with real-time responsiveness, provides notable benefits compared to both traditional and modern platforms, meeting the changing demands.

1. Introduction

In today's fast-paced technological landscape, secure communication systems are essential for modern infrastructure, facilitating everything from personal devices to extensive industrial and military operations. The rapid expansion of drone technology and its integration into critical infrastructures has increased both the complexity and the importance of these systems [1]. Unmanned aerial vehicles (UAVs) are no longer limited to niche applications but are now essential in fields such as surveillance, humanitarian relief, logistics, and military operations. This wider use also

* *Corresponding author.*
E-mail address: rexhepmustafovski@gmail.com

https://doi.org/10.31181/msa31202627

© The Author(s) 2026| Creative Commons Attribution 4.0 International License

raises new concerns about how to maintain secure and reliable channels of communication between the drones, their command centers, and the broader network environment [2].

SecuDroneComm offers a comprehensive response to these concerns. It is a hybrid platform specifically designed to enable safe and dependable information exchange between UAVs and their operational control units. The system draws on the capabilities of modern ICT by incorporating AES-256 encryption, TLS 1.3, and hybrid server configurations that protect the confidentiality, integrity, and availability of transmitted data. While existing approaches have addressed some of these requirements, many still struggle with issues of scalability, adaptability, and seamless integration into fast-changing operational contexts [3].

1.1 Role of Secure ICT Platforms in Modern Communication

Secure ICT platforms form the backbone of many critical operations, as they are responsible for safeguarding sensitive information during transmission and processing, ensuring protection against interception and unauthorized access [4]. This requirement is particularly important in drone communication, where activities rely on distributed networks and wireless links that are highly exposed to security risks. Although solutions such as ITU-T X.805 and SmartNet have advanced the development of secure ICT infrastructures, they continue to face limitations when addressing the current demands for mobility, real-time responsiveness, and global scalability [5].

The SecuDroneComm platform has been developed to overcome these challenges by combining the reliability of established approaches with the flexibility of new technologies [6]. It incorporates hybrid server architectures that balance the scalability offered by cloud resources with the low-latency performance of localized servers. In addition, the use of logical coordination units, comparable to software-defined networking (SDN) controllers, supports efficient data management and resource distribution across the platform [7].

1.2 Importance of Real-Time Communication for Drones

The effective operation of drones depends on uninterrupted information exchange. Tasks such as collecting surveillance data or executing autonomous maneuvers can only be achieved when secure and dependable communication links are maintained. In high-stakes scenarios like battlefield monitoring or disaster relief, even brief interruptions or delays in data transfer can significantly affect mission outcomes [8]. Traditional ICT systems often struggle to deliver the speed and low latency that these situations require, which highlights the importance of platforms such as SecuDroneComm [1,2].

1.3 Bridging the Gap: Comparing SecuDroneComm with Existing Platforms

Modern ICT platforms have contributed greatly to the development of secure communication systems. For example:

i. The ITU-T X.805 framework provides a structured approach to ICT security, although it was primarily designed for fixed infrastructures, which limits its usefulness in highly mobile or rapidly changing environments.
ii. The SmartNet architecture, which was developed for energy systems, shows the potential of distributed ICT frameworks, but it does not provide the level of real-time responsiveness required for UAV applications.

iii. Federated identity systems for mobile and wireless communications have improved authentication and access control, yet they frequently encounter challenges with scalability and interoperability, particularly when implemented in hybrid server settings.

Building on these lessons, SecuDroneComm incorporates mechanisms such as OAuth-based access management and TLS-secured channels, while being tailored to the unique requirements of UAV communication. Its hybrid configuration allows it to operate reliably across both local and cloud infrastructures, supporting continuous data transmission even when connectivity is unstable or restricted.

1.4 Key Features of SecuDroneComm Platform

i. *Hybrid server structure* – SecuDroneComm integrates both local and cloud servers in order to meet diverse operational requirements. Local servers are used to provide rapid responses for time-sensitive tasks, while cloud servers support scalability and long-term data storage with redundancy features [9];
ii. *Enhanced security mechanisms* – Security is a central element of the platform. It applies AES-256 encryption for safeguarding information, TLS 1.3 to ensure secure transmission, and OAuth protocols for reliable user authentication. Together, these mechanisms protect data across all stages of its use [10];
iii. *Logical coordination* – Inspired by software-defined networking, the logical coordinator manages routing and optimizes the distribution of resources between servers. This functionality is particularly important in hybrid infrastructures, where data often shifts between local and cloud environments [11];
iv. *Timely data handling* – The system is designed to satisfy the speed requirements of UAV communication. Its refined architecture minimizes latency and ensures that information is transmitted and processed without delay [9];
v. *Capacity for growth* – SecuDroneComm supports expansion from small tactical missions to large-scale, distributed networks. Its modular structure allows new drones, servers, or nodes to be added seamlessly without affecting ongoing activities [10].

1.5 Applications and Use Cases

i. *Military operations* – In defense scenarios, drones often function in environments where communication security is critical. SecuDroneComm enables continuous data exchange between UAVs and command centers, ensuring that reconnaissance and tactical planning are based on reliable and current information;
ii. *Disaster response* – During natural disasters, drones play an essential role in mapping affected areas and locating survivors. With SecuDroneComm, this information can be transmitted securely to emergency teams, supporting fast and coordinated interventions;
iii. *Public health applications* – The platform can also contribute to health-related monitoring, for instance by measuring air quality or detecting pathogens in populated areas. Through its connection with cloud servers, it provides large-scale analysis while maintaining responsive performance at the local level;

iv. *Industrial use* – In fields such as pipeline inspection or emissions monitoring, UAVs operating with SecuDroneComm ensure that sensitive industrial data is transmitted safely and remains protected against unauthorized access or manipulation.

1.6 Challenges and Opportunities

The deployment of SecuDroneComm is not without obstacles, particularly when integrating its diverse components across different operational contexts. Establishing the necessary infrastructure, such as hybrid servers and logical coordinators, requires both strategic planning and significant resources [9]. In addition, the system must remain flexible enough to respond to evolving cybersecurity threats and the rapid pace of technological innovation [10,11]. At the same time, these challenges create opportunities for further development. Incorporating tools such as blockchain to ensure data authenticity and artificial intelligence to strengthen threat detection could greatly enhance the platform's performance. Partnerships with established ICT systems and industry stakeholders may also accelerate both its adoption and continuous refinement [12].

2. Literature Overview

This section reviews recent progress in ICT platforms that support secure communication and compares these developments with the SecuDroneComm framework. By drawing on the referenced sources, it provides a comprehensive overview of existing approaches and highlights the aspects where further enhancement is needed.

2.1 Overview of SecuDroneComm Platform

SecuDroneComm is an advanced hybrid ICT platform designed to ensure secure and responsive communication between drones and their command centers. Its structure integrates both local and cloud servers, providing low-latency performance in constrained environments while also supporting scalability for wider deployments. The platform employs AES-256 encryption to safeguard information, TLS 1.3 to secure data transmission, and OAuth for user authentication. A logical coordinator, functioning similarly to an SDN controller, manages data flow and allocates server resources efficiently [9-11].

The system is particularly suited for critical fields such as defense, disaster relief, and public health monitoring, where timely and protected communication is indispensable. Through its modular structure and the use of modern technologies, SecuDroneComm offers the adaptability required to operate effectively across diverse mission contexts [10].

2.2 Overview of Other ICT Platforms

Several ICT platforms illustrate different methods for achieving secure communication, each addressing specific requirements and limitations (Table 1):

i. *ITU-T X.805 framework* – It provides a structured approach to end-to-end protection in networked systems. It introduces a three-layer model (infrastructure, services, applications) supported by eight distinct security dimensions. While it establishes a strong foundation for distributed environments, its design is rooted in conventional IP-based networks, which reduces its suitability for highly dynamic contexts such as UAV communication [13];
ii. *SmartNet architecture* – It was developed for secure communication in energy infrastructures, relying on distributed ICT frameworks including IoT and 5G. Its smart grid

architecture model (SGAM) ensures effective alignment of data flows within smart grids. Although it demonstrates flexibility and integration strength, its emphasis on energy systems restricts its usefulness for UAV communication that requires low-latency and real-time performance [14];

iii. *Trust-ME federated framework* – Trust-ME addresses authentication and access control across multiple systems through federated identity management. Features such as single sign-on (SSO) and integrated intrusion detection systems (IDS) improve both security and usability [15];

iv. *Spread secure communication* – Spread is intended for secure group communication, relying on dynamic key management protocols to maintain confidentiality and integrity. It performs well in collaborative scenarios that require scalability, but its reliance on predefined networks and complex group setups makes it less practical for UAV-focused applications [16].

Table 1
Overview of the SecuDroneComm and other platforms

Platform	Core focus	Applications
SecuDroneComm	Real-time UAV communication	Military, disaster response, public health monitoring
ITU-T X.805	End-to-end security	Traditional IP-based systems, networked environments
SmartNet	Energy system communication	Smart grids, energy management
Trust-ME	Federated identity management	Identity management, secure authentication
Spread	Group communication security	Collaborative environments, enterprise communication

3. Comparison of SecuDroneComm with Other Platforms

SecuDroneComm introduces a unique approach to secure communication for UAVs by combining strong encryption, hybrid server infrastructure, and adaptive routing mechanisms. While platforms such as ITU-T X.805, SmartNet, Trust-ME, and Spread have contributed significantly to the field of secure ICT communication, they are not fully aligned with the demands of real-time UAV operations. The following section provides a comparative evaluation, emphasizing the ways in which SecuDroneComm distinguishes itself while also drawing relevant insights from the strengths and limitations of these existing systems [17]. Table 2 outlines the main strengths and limitations of each platform, offering a clear perspective on how SecuDroneComm stands in relation to its peers.

3.1 In-Depth Comparison

SecuDroneComm features a hybrid architecture that allows for smooth integration of both local and cloud servers. This design guarantees low latency for operations that are time-sensitive and offers scalability for long-term data storage [11]. In comparison, platforms such as ITU-T X.805 utilize traditional layered frameworks, whereas SmartNet employs a distributed model specifically designed for energy systems, making them less flexible for UAV communication requirements [18].

SecuDroneComm uses AES-256 encryption and TLS 1.3 to ensure comprehensive data protection. This robust security framework keeps sensitive UAV data safe, even in high-risk situations [54]. On the other hand, Trust-ME is strong in identity management but does not prioritize the security of data transmission. Similarly, while Spread is effective in group communication, it lacks encryption

protocols that are tailored for hybrid systems [19].

Table 2
Comparison of SecuDroneComm with other platforms

Platform	Strengths	Limitations
SecuDroneComm	Hybrid server architecture, AES-256 encryption, TLS 1.3, SDN-like logical coordinator	Requires advanced infrastructure, initial setup complexity
ITU-T X.805	Comprehensive layered framework adaptable to multiple network scales	Focused on traditional IP-based systems, limited support for mobile and hybrid environments
SmartNet	IoT and 5G integration; highly flexible distributed architecture	Tailored for energy systems, lacks emphasis on UAV and real-time responsiveness
Trust-ME	Single sign-on, intrusion detection, seamless user access	Geared toward authentication and access management, less focus on data routing or scalability
Spread	Dynamic group key management, scalability for collaborative networks	Complexity in managing group configurations; not optimized for hybrid server architectures

Real-time communication is essential for UAV operations, and SecuDroneComm effectively addresses this with its logical coordinator, similar to an SDN controller. This capability manages data flow dynamically, ensuring that latency is kept to a minimum. Other platforms, like ITU-T X.805 and Trust-ME, focus more on security and authentication but fall short in optimizing real-time responsiveness [20].

SecuDroneComm's hybrid server setup offers built-in scalability, enabling the system to grow as new drones, servers, or nodes are introduced [11]. SmartNet also boasts strong scalability, but its emphasis on energy grids restricts its adaptability for UAV applications. On the other hand, Spread is scalable for group communication but lacks the hybrid integration for broader applications.

SecuDroneComm is designed for military operations, disaster response, and public health surveillance, where the need for security and real-time functionality is critical. In contrast, platforms like SmartNet and ITU-T X.805 are more appropriate for static or semi-dynamic settings, such as energy systems or established network infrastructure.

3.2 Effectiveness Comparison

Evaluating the performance of SecuDroneComm requires an analysis of several core indicators, including latency, security, scalability, adaptability, and ease of use. This part compares SecuDroneComm with established ICT platforms such as ITU-T X.805, SmartNet, Trust-ME, and Spread, using these benchmarks as reference points (Table 3). The purpose of this comparison is to demonstrate the advantages of SecuDroneComm, highlight the areas where it provides superior results, and identify opportunities for further refinement.

SecuDroneComm achieves low latency by utilizing local servers for quick data processing and cloud servers for added scalability. ITU-T X.805 and Trust-ME experience moderate latency due to their emphasis on layered security and authentication, respectively. SmartNet performs well in static environments but may face challenges in mobile scenarios like UAVs.

SecuDroneComm’s implementation of AES-256 encryption and TLS 1.3 provides strong data protection, outpacing the more generalized multi-layered security approach of ITU-T X.805. SmartNet uses blockchain technology to enhance security, while Trust-ME focuses more on user authentication than on data encryption.

Table 3
Effectiveness comparison of SecuDroneComm with other platforms

Metric	SecuDroneComm	ITU-T X.805	SmartNet	Trust-ME	Spread
Latency	Real-time with hybrid servers	Moderate	High in static environments	Moderate	Depends on group size
Security	AES-256, TLS 1.3, OAuth	Multi-layered framework	Blockchain-based encryption	Federated authentication	Group key management
Scalability	Highly scalable (hybrid model)	Limited to network scope	Flexible in distributed grids	Limited to authentication	Scalable in group settings
Adaptability	Dynamic routing with SDN-like logic	Rigid for IP-based systems	Focused on energy systems	Limited to access control	Limited to preconfigured groups
User accessibility	Modular design for easy integration	Structured but static	Advanced IoT integration	SSO for seamless access	Complex group configurations

SecuDroneComm is built for scalability, allowing for easy expansion to support more drones or servers. SmartNet offers similar scalability but is specifically tailored for static energy grids. In contrast, Spread's scalability is restricted to collaborative groups, and ITU-T X.805 faces challenges with large-scale dynamic deployments.

With its hybrid server architecture and logical coordinator, SecuDroneComm can easily adjust to various operational requirements. On the other hand, ITU-T X.805 and Trust-ME are less flexible, concentrating on static or pre-configured systems.

SecuDroneComm's modular design guarantees user-friendliness and seamless integration, providing adaptable interfaces for a variety of users. Trust-ME improves accessibility with SSO, while Spread's dependence on group configurations can hinder its user-friendliness.

By examining both the advantages and limitations of comparable systems, SecuDroneComm incorporates their most effective elements while addressing unresolved challenges, establishing itself as a strong candidate for secure UAV communication. Besides, SecuDroneComm distinguishes itself from existing platforms through several critical features that are central to UAV communication:

i. its hybrid design supports real-time processing with very low latency;
ii. advanced security mechanisms ensure robust protection of data while allowing the system to expand when needed;
iii. the inclusion of adaptive routing enables effective operation across diverse and changing environments.

4. Issues and Potential Solutions with the Implementation of the SecuDroneComm Platform

SecuDroneComm provides a strong and innovative solution for secure communication between drones, but there are challenges to consider when implementing this platform. Tackling these issues is crucial to ensuring the platform functions effectively and achieves its objectives in practical scenarios.

4.1 Infrastructure Requirements

SecuDroneComm depends on sophisticated infrastructure, which includes hybrid servers, secure gateways, and high-performance drones outfitted with sensors and communication modules. Establishing and maintaining this infrastructure can be resource-heavy, particularly in remote or resource-constrained areas. Solutions are:

i. adopt modular deployment strategies, beginning with essential regions;
ii. utilize portable, energy-efficient hardware for locations with limited infrastructure.

4.2 Cybersecurity Challenges

While SecuDroneComm employs robust encryption protocols such as AES-256 and TLS 1.3, new cybersecurity threats like quantum computing or advanced malware could take advantage of system vulnerabilities. Solutions are:

i. consistently update and patch encryption algorithms to stay ahead of technological advancements;
ii. incorporate real-time IDS to oversee and counteract potential cyber threats.

4.3 Scalability Concerns

While the platform's scalability is a notable advantage, overseeing numerous drones, servers, and users at the same time can get complicated, particularly during large-scale operations. Solutions are:

i. utilize the SDN principles to manage resources dynamically;
ii. create a strong data coordination system to efficiently handle high traffic.

4.4 Latency in Real-Time Operations

In time-sensitive scenarios such as military missions or disaster response, even slight delays in data transmission can lead to serious repercussions. Solutions are:

i. focus on using local servers for tasks that are sensitive to latency;
ii. enhance data routing through an SDN-like logical coordinator to reduce delays.

4.5 Integration with Existing Systems

Integrating SecuDroneComm with the legacy systems utilized in tactical operations centers or current drone communication frameworks can present challenges due to compatibility issues. Solutions are:

i. create middleware APIs to ensure seamless compatibility with legacy systems;
ii. offer customizable modules to tailor the platform to various operational requirements.

4.6 Environmental and Operational Limitations

The platform needs to operate effectively in a range of challenging environments, including those with extreme weather conditions, limited connectivity, or physical obstructions. Solutions are:

i. design rugged drones and hardware components that can endure environmental challenges;
ii. establish redundancy systems for connectivity, such as dual communication channels.

4.7 User Training and Operational Knowledge

SecuDroneComm offers advanced features that operators might not be familiar with. Without adequate training, the platform's effectiveness could be diminished. Solutions are:

i. implement comprehensive training programs for operators and technical staff;
ii. create user-friendly interfaces along with clear documentation and support systems.

4.8 Cost of Deployment and Maintenance

The deployment and upkeep of SecuDroneComm can be expensive due to the requirement for high-end technology and ongoing updates. Solutions are:

i. utilize a phased implementation strategy to spread costs over time;
ii. consider forming partnerships with industry leaders or government agencies to share funding and resources.

5. Conclusion

The SecuDroneComm platform represents a significant advancement in secure communication systems tailored for real-time UAV operations. It brings together a hybrid server structure, robust encryption protocols such as AES-256 and TLS 1.3, and a routing mechanism inspired by SDN concepts. This combination addresses core challenges, including latency reduction, system scalability, and operational adaptability. Its modular construction and capacity to connect with other infrastructures make it suitable for a variety of applications, ranging from defense missions to disaster response and public health monitoring.

In comparison with ICT frameworks such as ITU-T X.805, SmartNet, Trust-ME, and Spread, SecuDroneComm demonstrates stronger responsiveness, enhanced security, and greater versatility when operating in complex and rapidly changing conditions. Nonetheless, its successful deployment requires careful consideration of infrastructure demands, the evolving landscape of cyber threats, and the training of users. Approaches such as phased implementation, the integration of technologies like artificial intelligence and blockchain, and backward compatibility with existing systems can help strengthen its performance.

As UAV technologies and secure communication continue to progress, SecuDroneComm is positioned to set a new standard among ICT platforms. Its innovative design not only addresses gaps in earlier systems but also creates a foundation for future developments, ensuring reliable and secure communication in increasingly interconnected environments.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors received no external funding for this research.

References

[1] Kumar, R., & Khan, R. A. (2024). Securing communication protocols in military computing. N*etwork Security, 2024*(3). https://doi.org/10.12968/S1353-4858(24)70011-7.
[2] Aldossary, M., Alzamil, I., & Almutairi, J. (2025). Enhanced intrusion detection in drone networks: a cross-layer convolutional attention approach for drone-to-drone and drone-to-base station communications. *Drones, 9*(1), 46. https://doi.org/10.3390/drones9010046.
[3] Shamshad, S., Belguith, S., & Oracevic, A. (2025). Securing the Skies: A Cutting-Edge Authenticated Key Establishment Protocol for the Internet of Drones. *IEEE Internet of Things Journal, 12*(14), 27113-27125. https://doi.org/10.1109/JIOT.2025.3562117.

[4] Latif, S., Djenouri, D., Idrees, Z., Ahmad, J., & Zou, Z. (2025). Hardware Security Modules for Secure Communications in the Industrial Internet of Things. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2025.3600161.

[5] Rahouti, M., Xiong, K., & Xin, Y. (2020). Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends. *IEEE Access, 9*, 12083-12113. https://doi.org/10.1109/ACCESS.2020.3047996.

[6] Mustafovski, R., Risteski, A., & Shuminoski, T. (2025). Challenges and solutions for enhancing Drone-to-TOC communication performance in military and crisis operations. *ETIMA, 3*(1), 148-156. https://doi.org/10.46763/ETIMA2531148m.

[7] Darwish, T., Alhaj, T. A., & Elhaj, F. A. (2025). Controller placement in software defined emerging networks: a review and future directions. *Telecommunication Systems, 88*(1), 18. https://doi.org/10.1007/s11235-024-01252-0.

[8] Mandloi, D., Arya, R., & Verma, A. K. (2024). Internet of drones. In *Recent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors* (pp. 353-373). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-6790-8_13.

[9] Mustafovski, R., Risteski, A., & Shuminoski, T. (2025). State-of-the-Art Comparison of the SecuDroneComm Platform with Existing Secure Drone Communication Systems. *Proceedings of the International Conference "Annual conference on Challenges of Contemporary Higher Education*, Kopaonik, Serbia, 3-7 February.

[10] Mustafovski, R. (2025). Evaluating the Operational Impact of SecuDroneComm: Simulation-Based Assessment of Secure UAV Communication in Military Environments. *Scientific Technical Review, 75*(1), 11-18.

[11] Mustafovski, R. (2025). Formula-based Architectural Framework of the SecuDroneComm Platform for Unmanned Aerial Vehicle Communications. *Management Science Advances, 2*(1), 288-303. https://doi.org/10.31181/msa21202525.

[12] Tiron-Tudor, A., Deliu, D., & Ndou, V. (2025). Shaping the future: ethical, legal and social implications (ELSI) of digital innovation ecosystems (DIEs) amid the Twin Transition. *European Journal of Innovation Management*, 1-45. https://doi.org/10.1108/EJIM-12-2024-1524.

[13] Martín Toral, I., Calvo, I., Villar, E., Gil-García, J. M., & Barambones, O. (2024). Introducing security mechanisms in OpenFog-compliant smart buildings. *Electronics, 13*(15), 2900. https://doi.org/10.3390/electronics13152900.

[14] Saleem, M. U., Usman, M. R., Yaqub, M. A., Liotta, A., & Asim, A. (2024). Smarter grid in the 5G era: Integrating the internet of things with a cyber-physical system. *IEEE Access, 12*, 34002-34018. https://doi.org/10.1109/ACCESS.2024.3372379.

[15] Xu, B., Zhang, Z., Sun, A., Guo, J., Wang, Z., Li, B., et al. (2023). T-FIM: transparency in federated identity management for decentralized trust and forensics investigation. *Electronics, 12*(17), 3591. https://doi.org/10.3390/electronics12173591.

[16] Ni, J., Fang, G., Zhao, Y., Ren, J., Chen, L., & Ren, Y. (2024). Distributed Group Key Management Based on Blockchain. *Electronics, 13*(11), 2216. https://doi.org/10.3390/electronics13112216.

[17] Vogt, F. G., Rothenberg, C., Lopes, V. H., Luizelli, M. C., Rodriguez, F., Papagianni, C., & Pongrácz, G. (2025). SmartNet: Bridging Performance and Realism in Network Emulation with SmartNICs. In *Proceedings of the ACM SIGCOMM 2025 Posters and Demos* (pp. 184-186). https://doi.org/10.1145/3744969.3748449.

[18] Poorvi, J., Kalita, A., & Gurusamy, M. (2025). Reliable and efficient data collection in uav based iot networks. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2025.3550274.

[19] Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. *Multimedia Tools and Applications, 80*(14), 21165-21202. https://doi.org/10.1007/s11042-021-10723-4.

[20] Campagna, G., & Rehm, M. (2025). A Systematic Review of Trust Assessments in Human-Robot Interaction. *ACM Transactions on Human-Robot Interaction, 14*(2), 1-35. https://doi.org/10.1145/3706123.