iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62313

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Real-Time Video Streaming Applications in Military 5G Networks: A Technical Review

Nitesh Bhardwaj[1], K Tony Joseph[2]
Military College of Telecommunication Engineering Mhow, India

Abstract: ***The integration of advanced telecommunications technologies into military operations marks a pivotal evolution in modern warfare strategies. With the advent of military-grade 5G networks, there arises an unprecedented capacity for real-time data streaming and enhanced operational transparency on the battlefield. This literature review critically examines the deployment of real-time streaming applications within such networks, focusing on a technology stack comprising React Native, Node.js, MongoDB, Docker, and WebRTC. These technologies collectively form the backbone of a system designed to leverage the full capabilities of 5G's high throughput and ultra-low latency, essential for the demands of contemporary military engagements.***

Index Terms: 5G, military applications, real-time streaming, React Native, Node.js, MongoDB, Docker, WebRTC.

I. INTRODUCTION

Tactic decision-making procedures can be altered by the use of 5G technology in military applications, which enables operations based on real-time data analytics and information gathered from sensors positioned at the front edge of the battle field. Building responsive cross-platform applications that easily adjust to the many hardware and software ecosystems found in military tech contexts requires the use of React Native and Node.js. For managing the diverse and copious amounts of data produced in military environments, MongoDB's adaptable schema-less data structure is essential for enabling speedy data retrieval and storage. Docker ensures uniform operation across various military computer settings by encapsulating software into standardized units for development. In delicate or compromised operating circumstances, WebRTC offers a strong framework for secure peer-to-peer communication, which is essential for real-time data sharing. [1], [2].

II. 5G TECHNOLOGY IN MILITARY APPLICATIONS

The deployment of 5G technology in military contexts represents a strategic advancement, offering not just enhanced communication capabilities but also foundational changes in operational tactics due to its high data throughput and minimal latency. This section provides an in-depth analysis of key technical features of 5G that are pivotal to military applications, emphasizing network slicing, advanced security measures, and the criticality of ultra-reliable low-latency communications (URLLC).

A. Network Slicing

Military 5G networks can leverage network slicing to create isolated slices for classified communication, logistics management, and real-time battlefield intelligence. This compartmentalization helps minimize the propagation of cyberattacks and ensures the continued functionality of critical operations even if one slice is compromised [3].

B. Enhanced Security Protocols

Military 5G networks require robust security measures beyond traditional commercial solutions. Quantum-resistant cryptography and post-quantum cryptography algorithms can safeguard against future threats from advancements in codebreaking techniques. Additionally, integrating hardware-based security modules can provide an extra layer of protection for sensitive data at rest and in transit [4].

C. Ultra-Reliable Low-Latency Communications (URLLC)

URLLC in 5G is crucial for mission-critical military operations where immediate response is required. The capability to transmit data with latency as low as 1 millisecond transforms how the military can utilize technology, facilitating real-time remote control of battlefield assets and near-instantaneous data analysis. Mitigating these risks requires implementing techniques like time-hopping and frequency-hopping spread spectrum communication to minimize signal interception.

Additionally, robust authentication protocols are essential to ensure only authorized devices can access the network [5].

III. TECHNICAL INTEGRATION OF CORE TECHNOLOGIES IN MILITARY 5G APPLICATIONS

This section provides a detailed analysis of how React Native, Node.js, MongoDB, Docker, and WebRTC are technically integrated and utilized within military 5G networks to achieve superior operational efficiency and security.

A. React Native

React Native is used for building high-performance applications that must operate under diverse environmental conditions. Its compatibility with third-party plugins and native modules allows for integration with complex security features such as biometric authentication and encrypted storage, safeguarding sensitive military data [6]. Leveraging secure enclaves on mobile devices can isolate sensitive data and cryptographic operations, and integrating multi-factor authentication ensures robust user access control.

B. Node.js

Node.js is pivotal for building scalable network applications that manage simultaneous connections across vast networks. Its non-blocking I/O models allow the processing of high volumes of ISR data without lag, ensuring real-time information processing and relay [10]. Implementing vulnerability management practices to identify and patch software dependencies promptly, along with enforcing role-based access control, restricts unauthorized access to sensitive data within the Node.js environment.

C. MongoDB

MongoDB's schema-less nature allows military databases to incorporate an array of unstructured data types such as realtime video feeds, sensor data, and tactical logs. Its replication facilities ensure data redundancy and high availability, critical in combat scenarios where data integrity and timely access can be a matter of life and death [11]. Utilizing access control lists and encryption at rest safeguards data stored within MongoDB, and regularly backing up databases with disaster recovery procedures ensures data availability in case of cyberattacks.

D. Docker

Docker's container technology is strategically important for deploying and managing software in a secure, isolated, and consistent manner across diverse computing environments. It facilitates rapid deployment and scaling of applications across multiple cloud environments or bare-metal setups [7]. Enforcing strict image signing and content trust policies prevents unauthorized modifications to containerized applications, while network segmentation isolates Docker container traffic and minimizes the attack surface.

E. WebRTC

WebRTC is instrumental in establishing secure realtime communication channels without reliance on traditional telecommunication infrastructures. It facilitates direct encrypted peer-to-peer exchanges, crucial for covert operations and real-time tactical communication [8]. WebRTC connections should be encrypted using Secure Real-time Transport Protocol (SRTP) to protect against eavesdropping and data tampering. Additionally, implementing techniques like DTLSSRTP can ensure connection integrity and prevent man-in-themiddle attacks.

IV. SYSTEM ARCHITECTURE AND INTEGRATION IN MILITARY 5G REAL-TIME STREAMING APPLICATION

This section outlines the cohesive system architecture that binds React Native, Node.js, MongoDB, Docker, and WebRTC into a comprehensive solution, providing a detailed view of how these components interact within a military 5G network to support real-time streaming and communication capabilities.

A. System Overview

The application utilizes React Native to create a responsive and adaptable user interface, crucial for real-time operational awareness and command control functionalities. Node.js acts as the nerve center for backend services, managing realtime data processing and communication. MongoDB stores all operational data, including real-time video streams, sensor data, and logs. Docker encapsulates the Node.js environment and MongoDB in separate containers, providing a consistent and isolated runtime environment. WebRTC handles real-time communication needs, including live video streaming, audio communication, and secure data transfers [1], [2], [10].

V. OPERATIONAL IMPACT AND STRATEGIC VALUE OF 5G REAL-TIME STREAMING APPLICATIONS IN MILITARY OPERATIONS

This section evaluates the significant operational impacts and strategic advantages provided by deploying a 5G realtime streaming application, detailing how these technological advancements translate into enhanced military effectiveness and readiness.

A. Enhanced Situational Awareness

The integration of real-time video streaming and sensor data aggregation facilitated by 5G technology offers unprecedented situational awareness. Commanders and field units receive up-to-the-minute visual and data-driven insights, allowing for more informed decision-making and rapid response to changing battlefield conditions [9].

B. Improved Operational Efficiency

With the low latency and high reliability of 5G connections combined with the direct communication channels provided by WebRTC, military operations can benefit from faster communication and decision-making processes. Node.js and MongoDB work together to automate the processing and analysis of large volumes of data [11].

C. Increased Scalability and Flexibility

The use of Docker and 5G network slicing allows for dynamic resource management, making it possible to scale operations quickly and efficiently in response to mission requirements. The microservices architecture facilitated by Docker ensures that the system is modular and scalable [7].

D. Security and Reliability

The application employs cutting-edge encryption and security protocols, ensuring that all transmitted data remains secure against interception and cyber threats. The robust architecture ensures that communication links remain stable and reliable even in challenging environments [8].

E. Security Considerations for Operational Deployment

While real-time streaming applications offer significant advantages, their effectiveness hinges on maintaining a secure communication channel. Continuous monitoring of network activity for suspicious behaviour is crucial, with intrusion detection and prevention systems (IDS/IPS) deployed to identify and mitigate potential threats in real-time. End-to-end encryption should be leveraged whenever possible to safeguard data not only in transit but also at rest and in use, minimizing the potential impact of a data breach even if an attacker gains access to a specific network segment. Enforcing strong password policies, conducting regular security awareness training for personnel, and implementing vulnerability management practices are essential for maintaining a robust security posture. Simulating cyberattacks through red teaming exercises can help identify vulnerabilities in the system and assess the effectiveness of implemented security measures.

VI. CONCLUSION: IMPLICATIONS AND FUTURE OUTLOOKOF REAL-TIME STREAMING APPLICATIONS ON MILITARY 5G NETWORKS

This literature review has extensively explored the integration of React Native, Node.js, MongoDB, Docker, and WebRTC within military 5G networks, highlighting how each technology contributes to enhancing real-time streaming applications that are pivotal for modern military operations. The deployment of these technologies offers substantial improvements in communication, decision-making processes, and operational efficiency.

A. Key Takeaways

The real-time capabilities provided by these technologies enable faster and more accurate decision-making, crucial in dynamic battlefield environments. The integration of 5G networks ensures that data is processed and communicated with minimal latency. The use of WebRTC for secure realtime communications facilitates direct and reliable tactical communication across military units [10].

B. Strategic Implications

The deployment of these technologies strengthens the tactical capabilities of military forces and has strategic implications for national security. Enhanced real-time data processing and communication capabilities ensure that military forces are better prepared and more capable of responding to threats swiftly and effectively [2].

C. Future Outlook

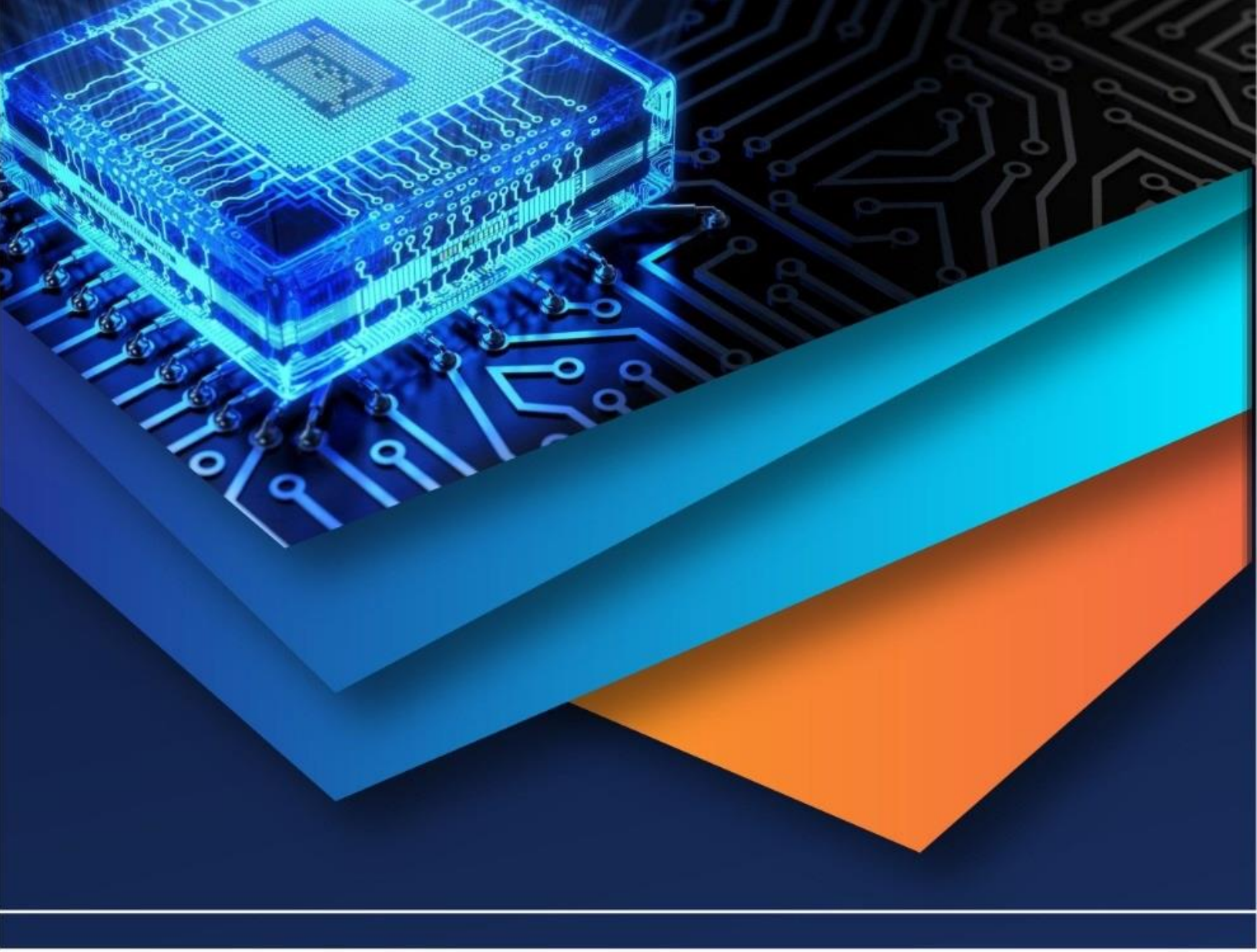
As the battlefield landscape continues to evolve, so too will the need for even more sophisticated and secure real-time communication solutions. Integration of Artificial Intelligence (AI) powered analytics can be integrated into real-time data streams to extract valuable insights and expedite decision-making processes, though the security implications of incorporating AI algorithms into military networks need careful consideration. Advancements in quantum computing pose a significant threat to current encryption standards, making the adoption of quantum-resistant cryptography algorithms crucial for safeguarding sensitive military communications. The development of self-healing and adaptive networks can further enhance the resilience of military communication infrastructure in the face of cyberattacks.

D. Considerations for Continuous Improvement

Maintaining a secure and effective 5G-based real-time streaming application ecosystem necessitates ongoing research and development efforts. Regular vulnerability assessments should be conducted to identify and address potential weaknesses in the system. Promptly deploying security patches for identified vulnerabilities is essential to minimize the window of opportunity for attackers. Collaboration and information sharing among military forces and cybersecurity experts can provide valuable insights into emerging threats and facilitate the development of more effective countermeasures. By continuously evaluating, adapting, and implementing robust security measures, military forces can leverage the full potential of real-time streaming applications in 5G networks to gain a decisive advantage on the modern battlefield.

REFERENCES

[1] P. Salva-Garcia, J. M. Alcaraz-Calero, Q. Wang, M. Barros, and A. Gavras, ”Self-Restoring Video User Experience in 5G Networks Based on a Cognitive Network Management Framework,” IEEE Trans. Broadcast., vol. 64, no. 2, pp. 621–634, 2019, doi: 10.1109/LCN44214.2019.8990815.
[2] K. Sayrafian and K. Yekeh Yazdandoost, ”Toward 5G Emerging Technologies: Selected Papers from IEEE PIMRC 2014,” Int J Wireless Inf Networks, vol. 22, no. 3, pp. 295–297, 2015, doi: 10.1007/s10776-0150289-5.
[3] J. Fletcher, D. Doria, and D. Bruno, ”Android Video Streaming,” Army Research Laboratory, Aberdeen Proving Ground, MD 210055067, ARL-TR-6947, May 2014.
[4] M. Repetto, ”Service Templates to Emulate Network Attacks in CloudNative 5G Infrastructures,” IEEE NetSoft, pp. 498–503, 2023, doi: 10.1109/NetSoft57336.2023.10175505.
[5] S. Ahmed, ”Enhancing Extended Reality(XR) By Using Mobile Devices Emphasizing Universal Usage,” Journal of Network and Systems Management, vol. 32, no. 1, pp. 1, 2023, doi: 10.1007/s10922-023-09778-5.
[6] T. Bokareva, W. Hu, S. Kanhere, B. Ristic, N. Gordon, T. Bessell, M. Rutten, and S. Jha, ”Wireless Sensor Networks for Battlefield Surveillance,” IEEE PIMRC, USA, 2006.
[7] T. Andras, ”The Use of 5G in Military Cloud of Things Solu-´ tions,” AARMS – Academic and Applied Research in Military and Public Management Science, vol. 21, no. 3, pp. 5–20, 2022, doi:10.32565/aarms.2022.3.1.
[8] A. Baretto, N. Pudussery, V. Subramaniam, and A. Siddiqui, ”Real-Time WebRTC based Mobile Surveillance System,” International Journal of Engineering and Management Research, vol. 11, no. 3, pp. 2976–2980, 2021, doi: 10.22214/ijraset.2019.5490.
[9] C. Togay, ”WebRTC technology for mobile devices,” IEEE SIU, pp. 256–259, 2014, doi: 10.1109/SIU.2014.6830214.
[10] G. Shen, J. Dai, H. Moustafa, and L. Zhai, ”5G and Edge Computing Enabling Experience Delivery Network (XDN) for Immersive Media,” IEEE HPSR, pp. 1–7, 2021, doi: 10.1109/HPSR52026.2021.9481809.
[11] D. Fang, Y. Qian, R. Q. Hu, and H. Wang, ”Security for 5G Mobile Wireless Networks,” IEEE Access, vol. 6, pp. 4850–4874, 2018, doi: 10.1109/ACCESS.2018.2810843.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY