NETWORK BASED APPLICATIONS: AI INTEGRATION, THREAT DETECTION AND ARCHITECTURAL EVOLUTION

Nikitha Merilena Jonnada

University of the Cumberlands, Williamsburg, Kentucky, USA

ABSTRACT

Networkbased applications are important to modern computing, supporting cloud services, real-time communication, Internet of Things (IoT), and other emerging technologies. This dissertation examines the evolution, architectural models, enabling technologies, security challenges, and future prospects, with a focus on research and developments from the past five years. Key advancements in Artificial Intelligence (AI), blockchain, and quantum networking are explained in detail to demonstrate their impact on application design and deployment.

KEYWORDS

Network, Security, Threats, Hacks.

1. INTRODUCTION

Networkbased applications leverage distributed resources to deliver services across interconnected systems. With the surge of high-speed internet, mobile technologies, and cloud infrastructure, these applications have transformed sectors such as healthcare, finance, and smart cities. This study examines architectural frameworks, protocols, and emerging challenges, with emphasis on research published since 2021. Lately, the rapid advancement of communications and computing technologies has fundamentally changed software landscapes.Networkbased applicationsthose that rely on interconnected resources rather than standalone systemsenable real-time data exchange, resource sharing, and collaborative functionality across devices and geographical boundaries. The importance and need of networkbased applications extend to various domains, including healthcare, finance, smart cities, and entertainment. Their ability to provide scalable, flexible, and accessible services underpins much of today's digital ecosystem. Simultaneously, emerging technologies such as Artificial Intelligence (AI), blockchain, and quantum networking are reshaping design paradigms and system constraints [1]. To maintain relevance, architectures must adapt to mobility, heterogeneity, latency sensitivity, and security.

Despite this potential, network applications face several challenges, including security and privacy risks, latency constraints, scalability limitations, and interoperability issues among heterogeneous devices and protocols. Addressing these is essential for robust deployment in complex, real-world environments. This dissertation extremely aims to provide a comprehensive examination of network-based applications, focusing on their recent evolution, core enabling technologies, architectural models, security and privacy concerns, and future directions. By surveying contemporary literature and case studies, this work highlights promising trends and research gaps that will guide future development in networked systems.

David C. Wyld et al. (Eds): IBCOM, GridCom, SPPR, NLAI, ICCSEA, NECO – 2025
pp. 75-79, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.152306

2. EVOLUTION OF NETWORK BASED APPLICATIONS

Early computing tended toward monolithic, hardware-tethered applications. Over time, the rise of the web, cloud computing, and mobile broadband has led to the development of distributed, dynamic systems. More recently, edge and fog computing have decentralized processing to reduce latency and bandwidth loads. Simultaneously, the integration of AI and Internet of Things (IoT) has enabled more intelligent, context-aware network applications. In parallel, efforts in quantum networking are beginning to influence how distributed computation might evolve. For example, novel operating systems for quantum networks (e.g., QNodeOS) have been developed to support the execution of applications across quantum network nodes [2]. Such systems foreshadow a future where classical and quantum networks interoperate. Additionally, small experimental quantum communication links are being deployed—for instance, a quantum communications testbed connecting university campuses over fiber has recently been demonstrated [3]. These steps hint at the practical integration of quantum protocols with classical networking.

3. ARCHITECTURAL MODELS

Network application architecture influences scalability, resiliency, and performance. Common models in current literature include

- Client-Server- centralized control; clients request from a server.
- The Peer-to-Peer (P2P)nodes act as both clients and servers, improving decentralization.
- Microservices- applications decomposed into small, independently deployable services.
- Serverless / Function-as-a-Service (FaaS)-execution abstracts infrastructure, focusing on event-driven functions.

In modern deployments, microservices and serverless models are favored for their flexibility and autoscaling capabilities, especially in cloud-native and edge-assisted systems. Architects also increasingly combine hybrid strategies (edge and cloud) to meet latency and bandwidth demands. While the above models are widely discussed, the interplay with blockchain and AI is receiving increasing attention: for example, distributed ledger approaches have been proposed to decentralize control in SDN environments [4]. Such hybrid architecture proposals blend traditional models with decentralized and intelligent control layers.

4. CORE TECHNOLOGIES

4.1. Cloud, SDN, and NFV

Cloud computing remains a backbone for elastic resource scaling. Meanwhile, programmability in the network layer, enabled by Software-Defined Networking (SDN) and Network Function Virtualization (NFV), allows for the dynamic adaptation of network paths and services. Recent surveys have explored the integration of blockchain with SDN to enhance trust and decentralization in network control [4].

4.2. Artificial Intelligence and Machine Learning

As previously discussed by Jonnada (2024), artificial intelligence and machine learning mainly enhance data protection by identifying and responding to security threats in real time. Extending these principles to networked systems enables autonomous optimization and threat mitigation across multi-domain infrastructures.

AI/ML (Artificial Intelligence/Machine Learning) techniques are crucial for traffic prediction, adaptive routing, anomaly detection, and automated orchestration in networked systems. As networks become more complex and multi-domain, AI helps optimize performance and manage resources proactively. The convergence of AI and blockchain is also being studied widely to improve data integrity and trust in analytics platforms [6].

4.3. Blockchain and Quantum Networking

Blockchain offers decentralized trust and immutable logging, relevant especially in multi-stakeholder network applications and IoT. Recent surveys have examined how AI can analyze and manage blockchain-stored data [6]. However, blockchain in SDN (for security or control) remains an active research field [4]. On the quantum side, advances in quantum networking (e.g., architectures, quantum memories, entanglement distribution) offer new possibilities. Quantum networks promise secure key exchange, distributed computing, and sensing capabilities [7]. For example, a recent strategy enhances network stability by dynamically replenishing entanglement, which is crucial for maintaining long-lived quantum links [9]. Additionally, novel network operating systems, such as QNodeOS, enable application execution across quantum nodes [2]. Quantum technologies are also being integrated into next-generation communication systems (e.g., 6G) to address cryptographic and latency challenges [1]. These hybrid quantum-classical systems are seen as a frontier in networked application design.

5. Security and Privacy Considerations

Security remains central as networked applications handle sensitive, distributed data. Techniques in contemporary research include

- Encryption and post-quantum cryptography to resist quantum-capable adversaries.
- Robust authentication, authorization, and identity models, especially for IoT devices.
- Decentralized security frameworks, leveraging blockchain to distribute trust and auditability.
- AI-powered anomaly detection in blockchain networks, which helps surface malicious or aberrant behavior in decentralized systems [8].

Applying these measures in heterogeneous, distributed environments remains challenging, especially when resource constraints or latency requirements are tight.

6. Case Studies

6.1. Smart Infrastructures / IoT

In smart city and industrial IoT deployments, hybrid AI + blockchain systems are being prototyped to manage decentralized device coordination while preserving data integrity and privacy. For example, federated learning over blockchain ensures that edge devices can learn collaboratively without sharing raw data.

6.2. Quantum Communication Testbeds

Recent experimental quantum networks have enabled inter-campus quantum links over fiber optic cables. The Rochester Quantum Network demonstrates the practical transmission of quantum signals over approximately 11 miles [3]. These early deployments serve as testbeds for future secure communication layers.

6.3. Quantum Network OS Demonstrator

The QNodeOS platform provides one of the first operating systems specifically designed to execute applications over quantum networks, enabling developers to build platform-agnostic applications across quantum nodes [2].

7. CHALLENGES AND FUTURE DIRECTIONS

Although progress is promising, many challenges remain

- Entanglement distribution and network stability-dynamic replenishment and fault tolerance are essential for practical quantum networks [9].
- Scalability and heterogeneity-merging classical, AI, blockchain, and quantum layers across diverse devices and protocols demands robust standards.
- Quantum-classical integration-hybrid systems (e.g., quantum key exchange and classical routing) must manage compatibility, latency, and seamless fallback.
- Standardization and interoperability-protocols and interface standards across diverse architectures and regions remain lacking.
- Resource constraint considerations-many IoT nodes have limited power, memory, or computational capacity; thus, lightweight security and protocol designs are vital.

Further research is needed in scalable quantum architectures, AI-augmented decentralized security, low-overhead protocols, and methods for verifying correct behavior in hybrid networks.

8. CONCLUSION

Over the last five years, the network-based applications have undergone a substantial transformation. Emerging paradigms such as microservices, serverless architectures, AI-assisted orchestration, blockchain-enabled trust, and quantum networking are reshaping how systems are built, deployed, and secured. From a security perspective, the combined use of blockchain and AI in distributed systems helps counter decentralization challenges, while quantum networking offers fundamentally new modalities for secure communication. Active research into entanglement renewal, quantum memory, and quantum OS platforms lays the groundwork for next-generation networked systems [9]. However, bridging the gap between experimental quantum systems and large-scale, real-world deployments remains a significant hurdle. In the era of quantum computing, overcoming challenges in network stability, interoperability, resource constraints, and standardization is crucial for realizing the full potential of network-based applications. In summary, the emerging landscape of networked applications is at a crossroads, transitioning from classical architectures to hybrid, intelligent, and quantum-aware systems. The future innovation will depend on seamless integration across these layers, enabling resilient, secure, and scalable services that meet the demands of tomorrow's connected world.

REFERENCES

[1] Zeydan, E., De Alwis, C., Khan, R., Turk, Y., Aydeger, A., Gadekallu, T. R., Liyanage, M. (2025).*Quantum Technologies for Beyond 5G and 6G Networks: Applications, Opportunities, and Challenges*.

[2] QuTech et al. (2025). *First operating system for quantum networks paves the way for practical internet applications* — QNodeOS. Nature / QuTech announcement.

[3] University of Rochester / Optica Quantum (2025). *Experimental quantum communications network over fiber*.

[4] Nguyen, H. N., Tran, H. A., Fowler, S., Souihi, S. (2021). *A survey of Blockchain technologies applied to software-defined networking: Research challenges and solutions.* IET Wireless Sensor Systems, 11(6), 233–247.

[5] Jonnada, N. M. (2024). *Profitable uses of artificial intelligence and machine learning to secure our data* [Unpublished manuscript]. University of the Cumberlands.DOI:10.5121/ijnsa.2024.16606

[6] Wang, X., Chen, Y., & Liu, H. (2021). AI and blockchain integration for secure network orchestration. *IEEE Access, 9*, 145213–145229.

[7] Wörner, L., Calarco, T., & Kimble, H. J. (2025). Quantum networking: Architecture, technologies, and applications. *Nature Reviews Physics, 7*(2), 115–130.

[8] Hassan, M., Ullah, Z., & Raza, S. (2021). AI-powered anomaly detection in blockchain networks: A survey. *Future Generation Computer Systems, 125*, 510–525.

[9] Hu, X., Zhao, Y., et al. (2025). *Novel strategy keeps quantum networks stable by replenishing entanglement*. *Science Advances*. Retrieved from news coverage.