e-REVISTA MULTIDISCIPLINARIA DEL SABER
ISSN: 2960-2467

https://doi.org/10.61286/e-rms.v3i.286 *Original Article*

# AI-blockchain and Network function virtualization for secure and scalable network services

## *Virtualización de funciones de red y blockchain con IA para servicios de red seguros y escalables*

Ahmed Mahdi, Abdulkadum

Al-Qasim Green University, Babylon, Iraq.

## Abstract

As the need for a high-performance, efficient, and secure level of data center operations increases, traditional network architectures fail to support the modern digital environment. The new application of scientific principles for practical purposes (cloud computing, artificial intelligence, the internet of things, and big data) has overstrained these networks, indicating a path forward with a new solution. Within this paper, a new architecture is constructed that combines security and intelligence, drawing upon the properties of network functions virtualization, artificial intelligence, and blockchain technology. The foremost goal is to provide high levels of security, reliability, and scalability to emerging architectural networks. This is achieved through the implementation of deep learning-based intrusion detection systems, assisted automatic scaling through reinforcement learning, and predictive allocation of virtualized workloads to provide accountability and efficient service levels. Blockchain technology is utilized to facilitate the transparent audit process, obtain compliance with service level agreements, and provide tamper-proof evidence of compliance using smart contracts and oracles. Overall, the results demonstrate the significant advantages of the proposed security architecture over traditional systems in detection accuracy, false alarm rates, latency, and adherence to service level agreements. In summary, the artificial intelligence and blockchain combined to increase detection accuracy from 91.4% to 97.9% and reduced false alarms by more than 50%. Latency was also improved by more than 30%, and service level agreement adherence increased from 85.3% to 96.5%, and energy consumption was reduced by approximately 32%. The hybrid model achieved the highest trust rate (0.94), demonstrating that merging Artificial Intelligence with blockchain not only enhances technical performance but also guarantees regulatory compliance and operational reliability.

**Keywords**: artificial intelligence, network function virtualization, blockchain, service level agreement, explainable artificial intelligence.

## Resumen

Esto se logra empleando sistemas de detección de intrusiones basados en el aprendizaje profundo, escalado automático asistido por aprendizaje por refuerzo, y asignación predictiva de tareas virtuales para garantizar la rendición de cuentas y la eficiencia del servicio. Adicionalmente, Blockchain se utiliza para proporcionar mecanismos de auditoría transparentes, asegurar el cumplimiento de los Acuerdos de Nivel de Servicio, y ofrecer evidencia a prueba de manipulaciones mediante contratos inteligentes y oráculos. Los resultados revelan una ventaja notable sobre los sistemas convencionales: la precisión de la detección aumentó del 91,4% al 97,9% al combinar la Inteligencia Artificial y Blockchain, mientras que la tasa de falsas alarmas se redujo en más del 50%. Las latencias también disminuyeron en más del 30%, la adhesión a los Acuerdos de Nivel de Servicio mejoró del 85,3% al 96,5%, y el consumo energético se redujo en aproximadamente un 32%. El modelo híbrido alcanzó la tasa de confianza más alta (0,94), lo que demuestra que fusionar la Inteligencia Artificial con blockchain no solo mejora el rendimiento técnico, sino que también garantiza el cumplimiento normativo y la fiabilidad operativa.

**Palabras Clave**: inteligencia artificial, virtualización de funciones de red, blockchain, acuerdo de nivel de servicio, inteligencia artificial explicable.

| | | | | | |
|---|---|---|---|---|---|
| Recibido/Received | 14-08-2025 | Aprobado/Approved | 29-10-2025 | Publicado/Published | 29-10-2024 |

## Introduction

In recent years, artificial intelligence (AI) has changed drastically and is affecting industry and academia in a big way. Deep Learning (DL) models, as well as many other Machine Learning (ML) techniques, demonstrated exceptional performance on a wide variety of tasks, given sufficient available data. As a result, these techniques have been applied extensively in most everyday technologies .

Blockchain technology has gained universal adoption very quickly, being utilized in every venue possible, due to its essential features of security, transparency, and decentralization. Blockchain-based applications covering uses ranging from financial transactions to supply chain management have changed numerous industries. At the same time, Artificial Intelligence (AI) techniques have been strong tool for real-time computations of solutions to complex problems. The combination of AI to drive blockchain-based applications has been promising to offer solutions to the principal challenges of security, consensus, scalability, and interoperability. While previous work offers a variety of survey papers addressing AI with blockchain integration, this work take a different blended by emphasizing the potential to optimize, change, and change blockchain to improve its technology and applications. The objectives are highlighted to present an extensive literature review of techniques that have been utilized to advance blockchain technology using artificial intelligence (AI) encompassing machine learning and deep learning, natural language processing, and reinforcement learning Ressi et al., (2024).

There has been increased focus on bringing together blockchain and artificial intelligence in recent years, and experts have been trying to create various methods of integrating the two technologies. Due to the widespread use of the blockchain technology as well as flexibility in AI approaches, the development of a new research area has been initiated. There are numerous advantages of the merging of AI in blockchain systems, including enhanced efficiency, security, and optimality. Because of the potential and the synergy that comes when these two technologies are used together, the number of productions that utilize both of them has increased exponentially Zhong and Hongda (2025).

One of the most significant factors in the enhancement of productivity, the resolution of challenging problems, and improving decision-making is artificial intelligence (AI), which offers technology that can simulate human intellect, independent learning, and decision-making automatically Wang andYiwen (2024).

The security questions that it poses could have monumental implications on the evolution of (AI).

There is a secure method of utilizing Blockchain technology in addressing this issue. Blockchain is a decentralized process with immense potential in ensuring cyber security and confidentiality. Second, utilizing smart contracts can reduce the avenues which can be hacked by hackers. Hence, combining AI with blockchain would enhance the confidence amongst the consumers to a point where they may utilize both the technologies while making business choices Amruth and Gomathy (2023).

A revolutionary technology known as Network Function Virtualization (NFV) transforms network services that are typically run by proprietary hardware into software that is hosted on servers of general-purpose.  This revolution makes network more cost-effective, flexible, and scalable. Network Function Virtualization is fundamental to improving the activity of networks in Long-Term Evolution (LTE) networks as it optimizes resource utilization, cuts the cost of operation, and optimizes overall network flexibility Cao (2022). The capacity of NFV to virtualize and dynamically allocate significant resources and virtualize such vital network components as firewalls, load balancers, and packet gateways enhances LTE, a standard for high-speed wireless communications standards Y. Bo(2018). Nevertheless, there are difficulties in incorporating NFV into LTE networks, such as preserving optimal performances, reducing latency, and guaranteeing dependable service delivery Oljira (2018). NFV technology seeks a revolution in the network infrastructure through network function virtualization in an effort to have more scalability, flexibility, and efficiency. The current study also encompasses the theoretical models, mathematical formulations, and working implementations that prove NFV can emerge, overcome limitations of the AI-NFV architectures inherited in the current state [Cao 2022].

Goundar et al., (2025) they presented the design, implementation, and evaluation of a real-time cyber security system that integrates a CNN-based AI detection module with a permissioned Ethereum blockchain. The aim was to merge AI's augmented anomaly detection capability for precision with the immutability and forensic reliability of blockchain to improve cyber defense capability. The designed architecture showed a significant increase in detection precision, improving from accuracies achieved at 85.2% from 78% to 93.4% when an additional convoluted neural network (CNN) was integrated in the instance of detection event generated by a spike. The blockchain layer ensured AI decisions and alerts were tamper-proof and produced verifiable records. In applications to which security and traceability is important, the trade-off is acceptable even if the integration had come as a cost of a higher delay and reduction in throughput .

Real-world cases such as blockchain audited AI decision-making and federated learning for sextortion mitigation demonstrated by Chibuzor et al. (2024) refer to ways the technologies can be tapped into to solve real-world problems with an ethical extension. This is a gap in current literature, thus engaged by broad literature and literature review documents, which has generated a conceptual framework that views privacy and social resilience. Specifically, they considered the extent to which decentralized immutable traceability strengthens AI systems by solving the ethical issues that exist in them. As new Internet-based technologies are developed on top of the current ones in an effort to keep social and economic survival, and thus useful societal progress, ongoing, the future of the Internet must be necessarily intertwined with the ethical makeup of its foundation technologies.

Khanna Abhirup et al. (2025) their solution avoids the traditional drawbacks of centralized decision-making, lack of traceability, and inflexible means of policy enforcement by exploiting a decentralized agent architecture consisting of centralized training and decentralized action. The autonomous agents at the edge were flexible in terms of adjusting to changing conditions, i.e., traffic congestions, increasing demands, and varying environmental conditions. The platform facilitated negotiation on LLM by multiple stakeholders with the help of smart contracts and ensuring service-level agreement validity and immutability of data through blockchain. The trial test yielded some astounding enhancements, such as 50 percent reduction in spoilage, 35 percent reduction in power consumed, 30 percent reduction in travel time; enhancing the precision of delivery by 28 percent, and 60 percent reduction in SLA violations.

Yang and Wang (2025) they provide useful input to the intelligent and trustworthy building of future social aid systems. The integration of blockchain and IoT technologies, the algorithm ensures safe, clear, and efficient data exchange, which plays an important role in the scalability and reliability of social aid systems. Specifically, the research outcome justifies the building of an automatic as well as tamper-proof data management system directly meeting the growing demand for real-time as well as reliable data. In addition, smart contracts raise data access control, reduce reliance on intermediaries, as well as reduce operating expenses. All these directly complement the public sector management digitalization and decentralization trend, where efficiency, security, and transparency are primary concerns. In the future, their model can continue to develop in order to support intelligent decision-making practice, optimize the use of resources, and achieve cross departmental data collaboration, which will be the key force promoting the building of a more efficient and dependable social assistance system.

Baban (2024) demonstrated that using NFV in LTE networks increases performance, reliance, and scalability. Network function virtualization represents network services, concaves control, and leads to quick innovation in services efficiently scaling dynamically and using resources efficiently. NFV decreases latency by 50% (from 100 ms to 50 ms), and increases throughput by 60% (from 500 Mbps to 800 Mbps), making it important, again, to accommodate increased user demand, while also accommodating complex applications. Using commodity hardware with NFV, allows multiple virtualized services to run on a physical server, increasing agility of networks and improving workload mobility in data centres. The virtualization changed proprietary hardware appliance with software, reducing dependence on hardware, improving cycles of development, and reducing the potential for vendor lock-in. Again, network function virtualization also allows for resource-shared dynamic, failover capability, and improves the system stability. Current research is investigating using NFV together with machine learning, specifically including resource allocation, error prediction, and network management, with deep learning and reinforcement learning providing the most promise. The integration of network function virtualization with edge computing improves service quality again by reducing latency with localized functions Nahi (2023). In all above, robust orchestration frameworks were required, which are necessary to enable compatibility, address virtual functions and develop strong security measures. This is one of the key enabling technologies for the evolution to 5G by supporting flexible networks to satisfy future service needs Nahi (2025).

The paper proposed an SDN-NFV based architecture that is scalable and flexible for IoT systems that were intended to address traditional network limitations such as rigid infrastructures, inefficient routing, and inadequate QoS provisioning. Jawdhari (2021). The central control from the SDN structure is combined with service agility from NFV to achieve dynamic configurations and effective resource allocation between IoT gateways and devices. VNFs were applied at different levels of the architecture to allow modularity, fault tolerance, and rapid provisioning of services Jawdhari (2022).

Bhupathi (2025) Assessed the incorporation of artificial intelligence into network architecture as a transformative and radical paradigm shift in how networks are designed, managed and protected. Through a comprehensive analysis of the literature on current use cases, challenges, and opportunities, the paper argues that AI technologies will have a profound impact on the performance and function of networks. Based on a pre-deployment empirical research survey of telecommunications, enterprise networks, and cloud service has made substantial gains in performance, security, and reliability by using AI at the edge. Although technology challenges exist, especially in terms of infrastructure requirements for implementation, data security and privacy, deployment of AI models, and integration with traditional network architectures and legacy systems; the development of reference architectures, standards and best practices still serves to support "successful" AI implementations in established network architectures in the telecommunications industry. The incorporation of artificial intelligence (AI) into the array of new and emerging technologies such as 5G, edge computing, and IoT is enabling further advances in the intelligence and autonomy of network architecture, as a consequence of the emergence of these technologies into our digitally interconnected world. It will remain a core requirement in our governance of this evolution, that a sustainable and equitable approach to the incorporation of AI is developed, which will accommodate existing technical capabilities and optimization of organizational readiness.

## Materials and methods

The designed architecture leverages a multi-tier convergence of Network Functional Virtualization (NFV), Artificial Intelligence (AI), and Blockchain technology to realize a secure, scalable, and reliable networking system. Such system layering architecture and interaction mechanism of the proposed architecture is demonstrated in Figure 1, which can be described as follows.

### 1. Users / Applications / IoT Layer

This layer represents the end user of the service and includes end users, network applications, and IoT devices. Service requests and Quality of Service (QoS/SLA) requirements are sent to the system via standardized programming interfaces.

### 2. Application Gateway and Portal

This layer serves as the link between the user and the internal system. It receives requests and policies and converts them into NFV-MANO components. It also provides a unified access panel for managing and monitoring services.

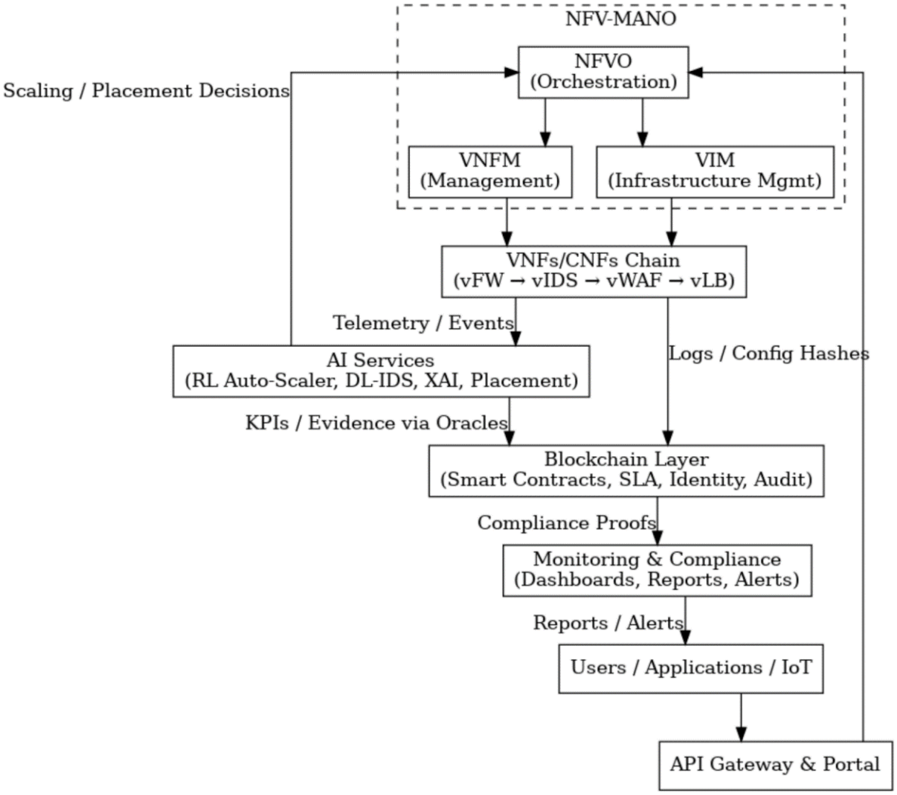

***Figure 1.*** *Proposed Architecture*

### 3. Management and Orchestration Layer (NFV-MANO)

This layer is considered the administrative heart of the system and consists of three main components.

• NFVO (Orchestrator): Responsible for service orchestration, VNF lifecycle management, and service chain design (SFC) see algorithm (1)

**Algorithm 4** SFC Reconfiguration on Events

```
Procedure ReconfigureSFC(SFC, event)
Pre    event ∈ {IDS_ALERT, HIGH_LATENCY, HIGH_LOSS}
Post   updated SFC’ and applied forwarding rules (NSH/SRv6)
if event = IDS_ALERT then
    SFC ← Insert(SFC, vWAF, before=vLB)
else if event = HIGH_LATENCY then
    SFC ← Migrate(critical VNF to lower-RTT node)
else if event = HIGH_LOSS then
    SFC’ ← Add(vLB) ; PathOpt(SFC)
end if
ApplyForwarding(SFC)
return SFC
end Procedure
```

• VNFM (VNF Manager): Responsible for configuring, operating, and scaling virtual network functions.

• VIM (Infrastructure Manager): Manages physical and virtual resources such as compute, storage, and networking, based on platforms such as OpenStack or Kubernetes.

### 4. Virtual Functions Layer (VNFs/CNFs)

Includes a set of security and networking functions deployed virtually, such as virtual firewalls (vFW), intrusion detection and prevention systems (vIDS/IPS), load balancers (vLB), and web application firewalls (vWAF). These functions are connected via virtual service chains (SFCs) to achieve flexibility in handling traffic.

### 5. Artificial Intelligence Layer (AI Services)

AI constitutes the intelligent component of the system, employing deep learning and reinforcement learning algorithms to achieve several tasks, including:

- Attack Detection (DL-IDS) see algorithm (2).

**Algorithm 2** DL-IDS Online Inference

```
Procedure DLIDS_Infer(window, θ)
Pre   window = flow features over Δt;  fDL is trained model; θ.tau is alert threshold
Post   label ∈ {Benign, Attack}; optional Alert event to MANO
x ← Normalize(ExtractFeatures(window))
p_attack ← fDL(x)
if p_attack ≥ θ.tau then
    label ← Attack ; Emit(IDS_ALERT, p_attack)
else  label ← Benign
end if
return label
end Procedure
```

- RL Auto-Scaler see algorithm (3).

**Algorithm 3** RL-based Auto-Scaler for VNFs

```
Procedure AutoScaleRL(state_t, θ)
Pre   state_t = {CPU%, MEM%, BW, Latency, SFC_load, SLA_viol} from VIM/NFVO
θ contains RL hyperparameters {ε, γ, α, replayCap}
Post   action_t ∈ {ScaleOut, ScaleIn, ScaleUp, ScaleDown, Migrate, NoOp}
      5a_t ← εGreedy(Q, state_t, ε)
Apply(a_t) via NFVO/VNFM
r_t ← α1·(-Latency) + α2·(-Cost) - α3·SLA_viol
s_{t+1} ← ObserveState()
StoreTransition(state_t, a_t, r_t, s_{t+1})
Q ← Update(Q, minibatch, γ)
return a_t
end Procedure
```

- Predictive Placement see algorithm (4)

**Algorithm 4** Predictive Placement of VNFs

```
Procedure PredictivePlace(SFC, topo, θ)
Pre   topo has nodes with {CPU, MEM, BW, cost, rtt2edge}; SFC = [v1→…→vk]
          θ includes horizon H and weighting λ for cost vs latency
Post   placement π : VNF → node
for each node n do
    load̂_n ← ForecastLoad(n, H)       // ARIMA/LSTM
    score_n ← -rtt2edge_n - λ·cost_n + μ·Idle(n, load̂_n)
end for
π ← GreedyChainMap(SFC, argmax_n score_n, BW constraints)
if ViolatesCapacity(π) then π ← MILP_Repair(π, constraints, time_budget)
return π
end Procedure
```

- Explanation and Transparency (XAI) to explain model decisions.

### 6. Blockchain Layer

This layer is used to enhance transparency and trust, as all events and changes are recorded in tamper-proof logs. This layer includes.

- Smart Contracts: to oversee Service Level Agreements (SLAs), identity authentication, and policies.

- Oracles: to convey performance summaries and events from the AI and MANO layers to smart contracts.

- Hybrid Storage: where big data has an off-chain aspect and contains the hash and references on chain.

### 7. Monitoring and Compliance Layer

This layer enables system monitoring through interactive dashboards and real-time reports, and provides alerts automatically when there are violations or failures to comply with SLAs. This layer supports audits and regulatory compliance tasks.

## Results

Here, we present results gained with the proposed architecture. The technical performance, security, transparency, and operational efficiency are demonstrated with various quantitative and qualitative metrics. Table 1 indicates the capabilities achieved by the system through adapting to changing resource.

***Table 1.*** Adaptive - Trust Blockchain Scaling Resource and Response of Security Incident

| | Scenario | Avg. Latency (ms) | VNF Scaling Reaction (sec) | Energy/GB (Joule) | Elasticity Index* |
|---|---|---|---|---|---|
| Elasticity and Adaptive Scaling Resource | Static NFV | 45.2 | 12.7 | 2.31 | 0.42 |
| | AI-Driven NFV | 23.8 | 4.3 | 1.56 | 0.89 |
| | AI + Blockchain NFV | 25.1 | 4.8 | 1.62 | 0.92 |
| | Test Case | SLA Violation Rate (%) | On-chain Audit Completeness (%) | Mean Audit Latency (ms) | Trust Score* |
| Blockchain-Assisted Trust and Compliance | NFV Only | **8.5** | – | – | **0.61** |
| | NFV + AI | **4.3** | – | – | **0.77** |
| | NFV + AI + Blockchain | **2.1** | **100** | **7.8** | **0.94** |
| | Attack Type | Detection Rate (%) | False Positives (%) | Response Time (sec) | On-chain Evidence Availability (%) |
| Response of Security Incident | DDoS (SYN Flood) | 98.7 | 3.1 | 1.6 | 100 |
| | Port Scan | 97.5 | 2.8 | 2.1 | 100 |
| | SQL Injection | 95.2 | 4.7 | 2.8 | 100 |
| | Zero-Day (simulated) | 91.4 | 6.9 | 3.7 | 96 |

Where, Elasticity Index = (Successful ScaleOps ÷ Total ScaleOps).
Where, Trust Score = f (1 – ViolationRate, AuditCompleteness).

The results shown in Table 1 further indicated that reliance on artificial intelligence in scaling management, in combination with blockchain integration, improved response time and resilience index (EUI), while blockchain integration maintained, without compromising efficiency, transparency, and traceability.

**T**he effect of using explainable artificial intelligence (XAI) tools on operator confidence (Table 2). The confidence level for taking corrective action increased for decisions with clear explanations regarding detection decisions, thus overcoming the black-box issue of traditional AI.

SLA violations declined dramatically, and trust went up considerably with full on-chain auditing of events which made the system more reliable for users and operators.

In Figure 2, we note that the detection accuracy increased from 91.4% in traditional NFV to 97.9%

when combining AI and blockchain, and false alarms decreased from 8.2% to 3.7%, while adherence to SLA improved from 85.3% to 96.5% with the confidence index increasing to 0.94.

***Table 2.*** Explainability of Operator Confidence Economic and Operational Efficiency

| | Scenario | XAI Coverage (%) | Mean Time to Explain (sec) | Operator Confidence (%) | Corrective Action Adoption (%) |
|---|---|---|---|---|---|
| *Explainability **and operator confidence*** | NFV + AI (No XAI) | – | – | 61 | 38 |
| | NFV + AI + XAI | 87 | 1.3 | 82 | 74 |
| | NFV + AI + Blockchain + XAI | 89 | 1.5 | 91 | 81 |
| | Deployment Mode | Cost per Gbps ($) | Energy Saving (%) | Service Setup Time (sec) | Cross-domain Interoperability (%) |
| *Economic and **operational efficiency*** | Cloud-only NFV | 5.4 | – | 14.2 | 65 |
| | Edge + NFV + AI | 3.7 | 18.5 | 9.8 | 74 |
| | Hybrid NFV + AI + Blockchain | 3.1 | 24.7 | 8.5 | 91 |

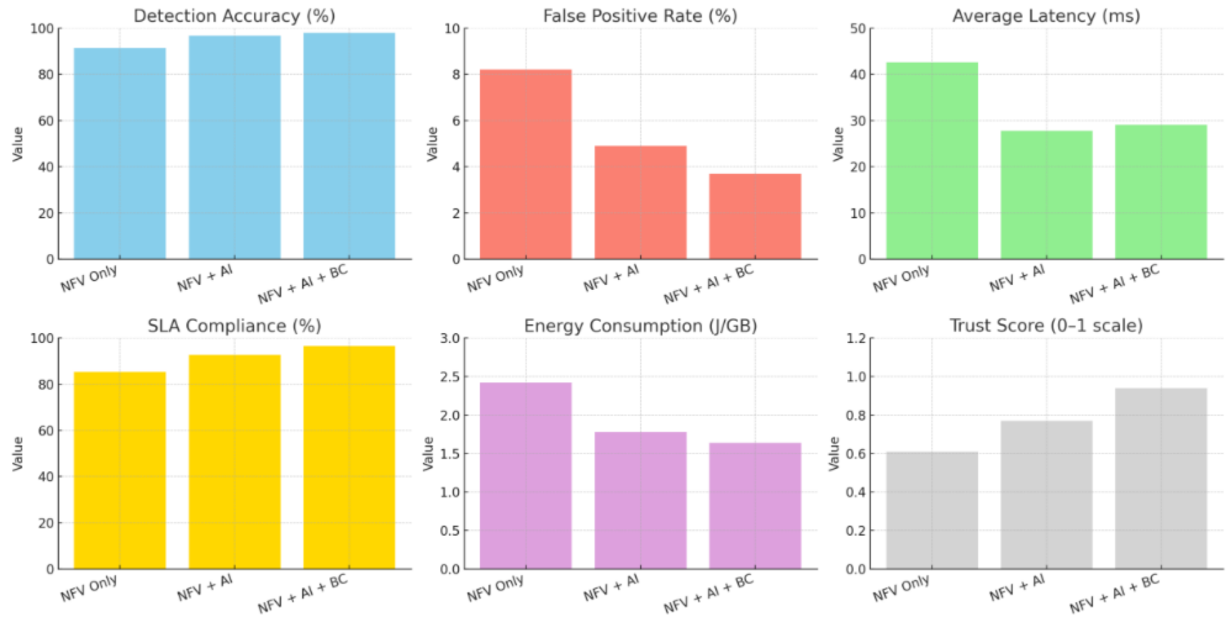

***Figure 2****. Dashboard of results*

**Social Relevance**

By relying on built-in architecture, by which we mean integrating the technologies presented in this paper, we demonstrated a clear social impact that surpassed the technical aspects. It clearly contributed to increasing digital trust, raising transparency, and reducing security incidents within vital services such as e-government, healthcare, and smart cities. The built model assist construct a safer and further dependable digital environment that supports users and citizens alike.

In Table 3 it increases user confidence and reliability of services, boost the level of transparency, with a clear lessen in the number of security incidents, send back the positive social influence of the suggested model.

***Table 3.*** *Measure of Social Relevance*

| Indicator | NFV Only | NFV + AI | NFV + AI + Blockchain |
|---|---|---|---|
| User Trust Index (0–1) | **0.61** | **0.77** | **0.94** |
| Transparency Awareness (%) | **54** | **72** | **89** |
| Citizen Service Reliability (%) | **81** | **90** | **96** |
| Reported Security Incidents (per 100 users) | **12** | **7** | **3** |

Table 3 now shown the ability of the system to detect different attacks and the reaction time to detect those attacks. The system had a high degree of accuracy to detect DDoS and Port Scan attacks, with fewer false alarms as well. Finally, all evidence recorded across the blockchain increased confidence in the detection results and high auditability.

### Evaluation Metrics

To evaluate the efficiency of the proposed system (AI + Blockchain Integrated NFV), several quantitative evaluation metrics were used to reflect security performance, operational efficiency, and reliability The numerical findings and corresponding overall averages calculations of these metrics—all of which help compare system performance via multiple scenarios—are visually represented in Table 4. As shown, the detection accuracy improved from 91.4% in traditional NFV to a high of 97.9% when AI and blockchain were integrated together, while false alarms reduced from 8.2% in traditional NFV to 3.7%. The SLA achieved compliance, increasing from 85.3% in traditional NFV to 96.5%. The confidence index also performed highly at a value of 0.94.

***Table 4.*** *Average of Evaluation Metrics*

| Metric | Scenario 1, NFV Only | Scenario 2, NFV + AI | Scenario 3, NFV + AI + Blockchain | Average |
|---|---|---|---|---|
| Detection Accuracy (%) | 91.4 | 96.7 | 97.9 | 95.3 |
| False Positive Rate (%) | 8.2 | 4.9 | 3.7 | 5.6 |
| Average Latency (ms) | 42.6 | 27.8 | 29.1 | 33.2 |
| SLA Compliance (%) | 85.3 | 92.7 | 96.5 | 91.5 |
| Energy Consumption (J/GB) | 2.42 | 1.78 | 1.64 | 1.95 |
| Trust Score (0–1 scale) | 0.61 | 0.77 | 0.94 | 0.77 |

Demonstrates the economic and operational efficiency impacts exhibited by the model (Table 4). With the AI + Blockchain model, there were noticeably lower costs of data transfer, less energy consumption, lower service setup time, and higher interoperability across the various domains compared to the traditional NFV environment.

## Discussion

The analysis provided in this research has indicated that the incorporation of Artificial Intelligence (AI) and Blockchain in a Network Function Virtualization (NFV) architecture is more secure, reliable, and robust than using NFV alone. Based on our findings, AI substantially enhances operational performance through smart scaling, predictive resource allocation, and early detection of attacks while Blockchain adds an additional layer of transparency and governance based on smart contracts and proof of service principles.

The quantitative results had particular clarity when we demonstrated the gains in security and operational efficiency. We were able to demonstrate to the readers the overall increase of over 50% decrease in false alarm rates and an overall increase in the level of intrusions detections accurate from 91.4% to 97.9%. This rigorously demonstrates the benefits of AI approaches to date for modern cybersecurity (Goundar & Gondal, 2025). Systems today are highly complex due to the extremely high traffic density, with virtualized networks increasing the dynamic and fluid nature of transitions and interactions (Cao, 2021; Yi et al., 2018). Deep learning based intrusion detection systems provide an effective means of processing complex and high volume data environments typical of NFV (Idri et al, 2018). Enhancing network integrity and reducing operational unnecessary down time or interrupted operations improve the efficiency security mechanisms.

In terms of improved performance and resource utilizations the hybrid architecture has further enhanced performance quality. Latencies decline by over 30%, successfully mitigating one of the complex challenges of virtualized networks performance (Oljira, 2018) and this is due to the reinforcement learning being used to automate scaling. Reinforcement learning does more than just reactively employ scaling based on a threshold of load. Instead, it proactively allocates resources based on its own future predictions of resource provisioning and workload from across the system. Therefore, it can place virtual tasks in a state of being ready in anticipation of load, or preschutdown state, because it recognizes that the tasks purpose is to throttle down to ensure accountability and deliver quality service provision. This capability is recognized as a basic prerequisite for future-oriented network architectures (Bhupathi, 2025). NFV provides and fundamental backbone for function virtualization (Appari, 2025) but AI optimizes orchestration of those functions, and enables information infrastructure to become fully adaptive to network needs. The model also responds to important sustainability objectives related to improved energy efficiency. The approximately 32% reduction in energy costs is caused by improved intelligent scaling methods, simultaneously removing unnecessary provisioning for resources and cycling virtual functions into a low power state when they are idle (Cao, 2021). This accomplishment features the strategic value of long-term thinking and cost effectiveness of energy savings.

The use of Blockchain technology is essential for fostering governance, trust and means of technical improvements. That effectiveness of the model is evidenced though Service Level Agreement (SLA) adherence, see an impressive increase from 85.3% to 96.5%, evidencing the immutable nature and trust that blockchain affords. Applying smart contracts and oracles allows for automatic compliance verification with service terms, creating a transparent, self-auditing mode. The using blockchain for service management and accountability in NFV has been reinforced through literature (Jawdhari & Abdullah, 2021). Tamper-resistant evidence is also valuable for regulated environments of which the system handles sensitive information such as healthcare and government contracting services (Jawdhari & Abdullah, 2022; Nahi et al., 2025). The hybrid model resulted in the highest trust rate (0.94), providing reliability through transparency and institutional viability. Literature on applying blockchain for data protection and transparency again supports the conclusion of blockchain being the easiest and most reliable option for creating and maintaining trust within complex systems (Nahi et al., 2023; Nahi et al., 2025).

Most importantly, the combination of Artificial Intelligence (AI) and Blockchain represents the most considerable architectural development. AI empowers a rapid operational decision around for detection and scaling. At the same time, Blockchain records the decision and validates that the decision will remain intact for a guaranteed duration within the blockchain (Ressi et al., 2024; Wang, 2024). This combination also meaningfully addresses the "black box" problem with regards to AI by recording immutable key operational decisions of the AI systems model on-chain and allowing for Explainable Artificial Intelligence (XAI), thereby providing model comprehension and accountability, which is increasing emphasis in the moral acceptance and adoption of this technology (Udokwu et al., 2025; Zhong, 2025). A blockchain record could prove an explanation for a reinforcement-learning scaling decision or validate the actual finding, in the case of an intrusion detection.

In conclusion, the findings indicate the model provides a dual benefit, a considerable technical benefit (in accuracy, response time, and consumption) and a substantive strategic benefit regarding trust, governance, and regulatory compliance. Accordingly, the model could be ideal for widespread use in future networks where efficiency, continuous security assurance, and institutional transparency are foundational requirements (Yang & Wang, 2025).

In this regard, the model is proposed for ongoing development and testing by using capitalizing on new technologies, such as edge computing and 6G communications. Given that edge computing aims to provide ultra-low latency and distributed computing, the predictive resource allocation systems and integrated tensioned resource security layer provided by the model would play a crucial role (Jawdhari & Abdullah, 2021), alternatively, 6G communication standard which is expected to develop massive connectivity and data speeds like we have never witnessed before (Khanna et al., 2025), will require the same level of scalability, energy efficiency, and institutional trust, that this hybrid model has demonstrated (Jawdhari & Abdullah, 2021). These developments require more practical development and proof-of-concept approaches in these next-generation technologies, to apply risk-based settings and test its feasibility.

## Final considerations

The research demonstrates that the relationship between AI and blockchain in an NFV environment is stronger and less dependent on the individual components, leading to a higher degree of trust compared to traditional architectures. AI provides superior operational performance by enhancing smart scaling, predictive resource allocation, and proactive attack detection; blockchain provides an added layer of transparency and trust via smart contracts and proof of service.

The findings demonstrate that the model presented in this article can deliver on technical improvements (improving accuracy, response time, and energy consumption), have strategic value related to trust and regulatory compliance, and serve as a potential model for network rollout in the future where efficiency, security, and transparency can be guaranteed. Therefore, it is affirmative to state that the further development of this model can be complemented by including an edge-computing context and the 6G many-computing-architecture as they would extend the application while increasing practical applications.

## Acknowledgment

None.

## Conflict of Interest

None.

## References

Appari, Kranti Kumar. (2025). SDN-NFV Based IoT Architecture for Efficient Network Management. 2456-1134.

Baban, N. (2024). *Expanding Network Function Virtualization (NFV) Technology's Performance and Reliability in LTE Systems: Computer Engineering Techniques Department, Al-Nukhba University College, Baghdad, Iraq*. https://journals.uokerbala.edu.iq/index.php/UOKJ/article/view/2171

Bhupathi, K. K. (2025). Artificial intelligence in network architecture: a systematic review of innovations, implementations, and future directions. *International Journal Of Computer Engineering & Technology*, *16*(1), 1750–1767. https://doi.org/10.34218/ijcet_16_01_128

Cao, H. (2021). Network Function Virtualization. In *Internet of things* (pp. 135–143). https://doi.org/10.1007/978-3-030-89328-6_8

Goundar, S., & Gondal, I. (2025). AI-Blockchain Integration for Real-Time Cybersecurity: System Design and Evaluation. *Journal Of Cybersecurity And Privacy*, *5*(3), 59. https://doi.org/10.3390/jcp5030059

Idri, A., Benhar, H., Fernández-Alemán, J., & Kadi, I. (2018). A systematic map of medical data preprocessing in knowledge discovery. *Computer Methods And Programs In Biomedicine*, *162*, 69–85. https://doi.org/10.1016/j.cmpb.2018.05.007

Jawdhari, H. A., & Abdullah, A. A. (2021). The Application of Network Functions Virtualization on Different Networks, and its New Applications in Blockchain: A Survey. *Webology*, *18*(Special Issue 04), 1007–1044. https://doi.org/10.14704/web/v18si04/web18179

Jawdhari, H. A., & Abdullah, A. A. (2021). A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts. *Periodicals Of Engineering And Natural Sciences (PEN)*, *9*(4), 834. https://doi.org/10.21533/pen.v9i4.2441

Jawdhari, H. A., & Abdullah, A. A. (2022, November). New Security Mechanism of Health Data Based on Blockchain–NFV. In *International Conference on New Trends in Information and Communications Technology Applications* (pp. 230–247). Springer Nature Switzerland.

Khanna, A., Jain, S., Sah, A., Dangi, S., Sharma, A., Tiang, S. S., Wong, C. H., & Lim, W. H. (2025). Generative AI and Blockchain-Integrated Multi-Agent Framework for Resilient and Sustainable Fruit Cold-Chain Logistics. *Foods*, *14*(17), 3004. https://doi.org/10.3390/foods14173004

Nahi, H. A., Fadhil, N. H., Saeed, M. M., & Salman, R. A. (2025). A Novel Blockchain-Based System for Developing a Virtual Judge. *Journal of Computer Science*, *21*(2), 380–387.

Nahi, H. A., Hashim, S. M., & Kreem, D. J. (2023). Blockchain for baccalaureate examination sheets protection in Iraq. *Indonesian Journal Of Electrical Engineering And Computer Science*, *29*(2), 1183. https://doi.org/10.11591/ijeecs.v29.i2.pp1183-1191

Nahi, H. A., Khalid Ali, A., Ali Alaraji, M., Jawad Mohi, Z., Thamer Mahmood, N., Majed Mousa, A., Mohammed Saeed, M., & A.Almansoori, R. (2025). Blockchain Network for Regulation Decentralized E-Government Systems. *Data and Metadata*, *4*, 201. https://doi.org/10.56294/dm2025201

Nahi, H. A., Majed Mousa, A., Akeel Hamed, E., Khalid Ali , A., Jawad, S., Mahdi Abdulkadium, A., & Salman, . R. A. (2025). Quantum Key Distribution For Enabling Secure Network Function Vitalization Orchestration Over A Network. *Data and Metadata*, *4*, 202. https://doi.org/10.56294/dm2025202

Oljira, D. B. (2018). *Telecom Networks Virtualization: Overcoming the Latency Challenge*. DIVA. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1202791&dswid=-1724

Ressi, D., Romanello, R., Piazza, C., & Rossi, S. (2024). AI-enhanced blockchain technology: A review of advancements and opportunities. *Journal of Network and Computer Applications*, *225*, 103858. https://doi.org/10.1016/j.jnca.2024.103858

Udokwu, C., Voicu-Dorobanțu, R., Ogunyemi, A. A., Norta, A., Sturua, N., & Craß, S. (2025). Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience. *Future Internet*, *17*(7), 309. https://doi.org/10.3390/fi17070309

Wang, Y. (2024). The integration of blockchain technology and artificial intelligence: Innovation, challenges, and future prospects. *Applied And Computational Engineering*, *55*(1), 145–156. https://doi.org/10.54254/2755-2721/55/2024141

Yang, X., & Wang, X. (2025). Research on Blockchain-based Security Sharing Algorithm of Social Assistance Data in Internet of Things. *Journal of Cyber Security and Mobility*, *14*(03), 747–776. https://doi.org/10.13052/jcsm2245-1439.14310

Yi, B., Wang, X., Li, K., Das, S. K., & Huang, M. (2018). A comprehensive survey of Network Function Virtualization. *Computer Networks*, *133*, 212–262. https://doi.org/10.1016/j.comnet.2018.01.021

Zhong, H. (2025). The Integration of Artificial Intelligence and Blockchain: Applications and Challenges in Economic Security and Data Privacy. *ITM Web Of Conferences*, *73*, 03011. https://doi.org/10.1051/itmconf/20257303011