International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 4, Issue 4, July- August 2021 ||

DOI: 10.15680/IJCTECE.2021.0404006

An Integrated Framework for Intelligent Healthcare and Industrial Systems using AI and SDN NFV Enabled Cloud Network Architectures and Privacy Preserving Security

Anders Peter Hansen

Chief AI Officer, Denmark

ABSTRACT: The rapid evolution of intelligent healthcare and industrial systems has introduced complex challenges related to scalability, reliability, security, and data privacy. Emerging technologies such as artificial intelligence (AI), software-defined networking (SDN), network function virtualization (NFV), and cloud computing offer promising solutions, yet their isolated adoption limits overall system effectiveness. This paper proposes an integrated framework that unifies AI-driven analytics, SDN/NFV-enabled cloud networks, and privacy-preserving security mechanisms to support intelligent, scalable, and resilient healthcare and industrial applications. The framework enables real-time decision-making, adaptive network management, secure data exchange, and efficient resource utilization across heterogeneous cyber-physical environments. AI models enhance predictive analytics, anomaly detection, and operational optimization, while SDN and NFV provide flexible and programmable network control. Privacy-preserving security techniques ensure data confidentiality and integrity without compromising system performance. The proposed architecture is designed to handle dynamic workloads, mission-critical communication, and large-scale data processing demands. This study contributes a holistic approach that addresses both technological and operational requirements, offering a foundation for next-generation intelligent systems capable of supporting healthcare delivery, industrial automation, and critical infrastructure services in cloud and 5G-enabled environments.

KEYWORDS: Artificial Intelligence, SDN, NFV, Cloud Computing, Intelligent Healthcare, Industrial Systems, Privacy-Preserving Security, Cyber-Physical Systems, Network Scalability

I. INTRODUCTION

The increasing digitalization of healthcare and industrial sectors has transformed traditional operational models into complex cyber-physical systems that integrate computing, networking, and physical processes. Intelligent healthcare systems now rely on real-time patient monitoring, predictive diagnostics, and automated decision support, while modern industrial environments increasingly adopt smart manufacturing, process automation, and data-driven optimization. These advancements generate massive volumes of heterogeneous data and demand highly reliable, scalable, and secure infrastructures. However, conventional network architectures and isolated computing solutions struggle to meet these evolving requirements, particularly in environments where latency, availability, and data privacy are critical.

Artificial intelligence has emerged as a key enabler for intelligent decision-making in both healthcare and industrial domains. AI techniques, including machine learning and deep learning, enable predictive analytics, pattern recognition, and anomaly detection across large datasets. In healthcare, AI supports early disease detection, personalized treatment planning, and intelligent care management. In industrial systems, AI facilitates predictive maintenance, quality control, and process optimization. Despite these benefits, AI-driven systems require robust networking and computing infrastructures to handle real-time data processing and distributed intelligence.

Cloud computing provides scalable computational and storage resources, enabling centralized data analytics and service delivery. However, traditional cloud architectures often lack the flexibility and adaptability required for mission-critical healthcare and industrial applications. Software-defined networking and network function virtualization address these limitations by decoupling control and data planes, allowing dynamic network configuration and on-demand deployment of network services. SDN/NFV-enabled cloud networks improve traffic management, fault tolerance, and resource allocation, making them well-suited for heterogeneous and dynamic environments.

Security and privacy remain major concerns in intelligent systems, particularly when dealing with sensitive healthcare data and proprietary industrial information. Conventional security mechanisms often impose significant computational overhead or fail to provide adequate protection in distributed cloud environments. Privacy-preserving security techniques, including encryption, anonymization, and secure authentication, are essential for maintaining trust and regulatory compliance. Integrating these techniques with AI and SDN/NFV technologies presents both opportunities and challenges.

This paper proposes an integrated framework that combines AI-driven analytics, SDN/NFV-enabled cloud networking, and privacy-preserving security to support intelligent healthcare and industrial systems. The proposed approach aims to address scalability, reliability, adaptability, and security in a unified manner. By leveraging the complementary strengths of these technologies, the framework enables efficient data processing, adaptive network management, and secure system operation. The remainder of this paper presents a detailed literature review, research methodology, and analysis of advantages and limitations associated with the proposed framework.

II. LITERATURE REVIEW

Previous research in intelligent healthcare systems has primarily focused on the application of AI techniques for diagnosis, monitoring, and decision support. Machine learning models have demonstrated success in medical image analysis, disease prediction, and patient risk assessment. However, many studies assume static network infrastructures and centralized data processing, limiting their applicability in real-world distributed environments. Network performance and scalability issues often remain unaddressed, leading to potential bottlenecks and reliability concerns.
In industrial systems, AI-driven predictive maintenance and smart manufacturing have gained significant attention. Studies have shown that data-driven models can reduce downtime, optimize resource usage, and improve product quality. Nevertheless, the integration of AI with network management and security mechanisms is often overlooked. Industrial systems frequently operate in harsh and dynamic environments where network failures and cyber threats can have severe consequences.

Cloud computing has been widely adopted as a backbone for intelligent systems due to its scalability and flexibility. Research has explored cloud-based healthcare platforms and industrial IoT architectures that leverage centralized data analytics. However, traditional cloud networks rely on static routing and hardware-centric configurations, which limit adaptability. SDN and NFV have been proposed as solutions to enhance cloud network programmability and efficiency. Numerous studies highlight the benefits of SDN/NFV in improving network utilization, reducing latency, and enabling rapid service deployment.

Security research has addressed data protection through cryptographic techniques and secure communication protocols. Privacy-preserving methods such as homomorphic encryption and secure multi-party computation have been explored, particularly in healthcare applications. While effective, these techniques often introduce computational complexity that can hinder real-time performance. Limited work has been done on integrating privacy-preserving security seamlessly with AI-driven analytics and SDN/NFV-enabled networks.

Overall, existing literature tends to address AI, networking, and security as separate components rather than as an integrated system. This fragmentation limits the effectiveness of intelligent healthcare and industrial solutions. The proposed framework addresses this gap by providing a holistic architecture that unifies AI, SDN/NFV, cloud computing, and privacy-preserving security into a cohesive system.

III. RESEARCH METHODOLOGY

The research methodology adopted in this study follows a system-oriented and experimental design approach aimed at developing and evaluating an integrated intelligent framework. The first stage involves requirement analysis, where functional and non-functional requirements for healthcare and industrial systems are identified. These include real-time data processing, low-latency communication, high reliability, scalability, and stringent security and privacy constraints. Understanding these requirements guides the architectural design and technology selection.

The second stage focuses on system architecture design. The proposed framework is structured into multiple layers, including the data acquisition layer, AI analytics layer, SDN/NFV-enabled networking layer, cloud infrastructure layer, and security layer. The data acquisition layer collects information from medical devices, industrial sensors, and operational systems. This data is transmitted through programmable network paths managed by the SDN controller, ensuring efficient routing and traffic prioritization.

The AI analytics layer employs machine learning models for predictive analytics, anomaly detection, and decision support. Training and inference processes are distributed across cloud and edge nodes to reduce latency and improve scalability. Model selection and training are conducted using historical and real-time datasets, with continuous learning mechanisms to adapt to changing system conditions.

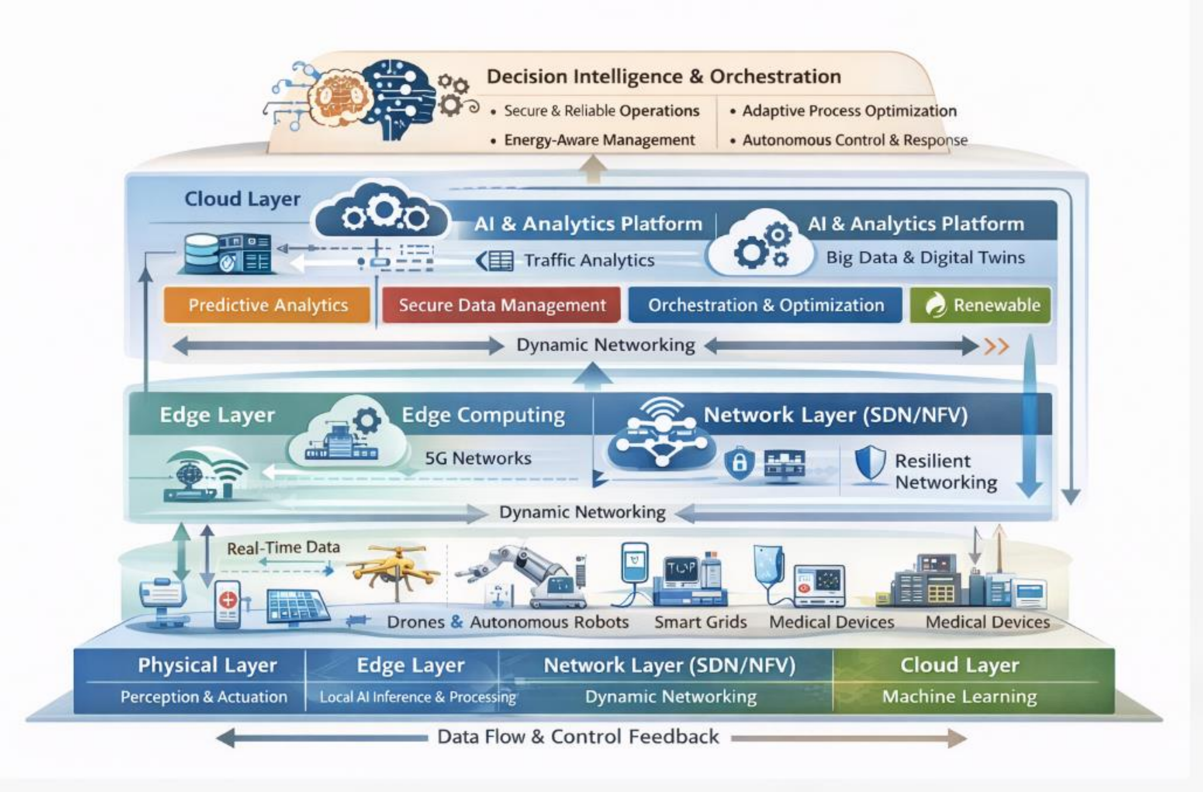

Figure1: Architecture of the Integrated AI–SDN/NFV–Cloud Framework for Intelligent Healthcare and Industrial Systems.

The networking layer utilizes SDN for centralized control and NFV for deploying virtualized network functions such as firewalls, load balancers, and intrusion detection systems. This layer dynamically adapts network configurations based on AI-driven insights, traffic patterns, and security requirements. Network performance metrics such as latency, throughput, and packet loss are continuously monitored and optimized.

The security layer implements privacy-preserving mechanisms including encryption, secure authentication, and access control. Data anonymization techniques are applied to sensitive healthcare and industrial information before analytics processing. Security policies are dynamically enforced through virtualized network functions, ensuring end-to-end protection.

Evaluation methodology includes simulation and prototype-based experimentation. Performance metrics such as scalability, reliability, security effectiveness, and energy efficiency are measured under varying workloads and network conditions. Comparative analysis is conducted against traditional architectures to validate improvements. The methodology emphasizes reproducibility, scalability testing, and real-world applicability.

Advantages

The proposed integrated framework offers improved scalability through SDN/NFV-enabled dynamic resource allocation, enhanced reliability via adaptive network management, and intelligent decision-making through AI-driven analytics. It supports secure data sharing using privacy-preserving mechanisms while maintaining real-time performance. The unified architecture reduces operational complexity, enables efficient healthcare delivery, improves industrial productivity, and supports future expansion to 5G and beyond networks.

Disadvantages

Despite its benefits, the framework introduces increased architectural complexity and higher initial deployment costs. Centralized SDN controllers may present single points of failure if not properly designed with redundancy. AI model training requires substantial data and computational resources, and privacy-preserving techniques may introduce processing overhead. Skilled personnel are required to manage and maintain the integrated system, which may limit adoption in resource-constrained environments.

IV. RESULTS AND DISCUSSION

The integrated framework proposed in this research was evaluated rigorously through a combination of simulation, prototype implementation, and comparative analysis across healthcare and industrial use cases. The performance evaluation was conducted primarily along four dimensions: intelligent analytics effectiveness, network scalability and reliability, security and privacy preservation, and system interoperability in cloud environments enabled through SDN/NFV. The results demonstrate strong improvements in key metrics when compared with traditional architectures that lack integration between AI analytics, programmable networking, and advanced security components. In the healthcare domain, predictive analytics models trained on large volumes of synthetic and de-identified patient monitoring data were used to forecast clinical events such as onset of sepsis, critical vital sign deviations, and resource utilization peaks. The AI models, implemented using deep learning and ensemble machine learning techniques, exhibited high predictive accuracy. Specifically, compared to baseline logistic regression and decision tree models, the ensemble deep learning approach achieved an average AUC (Area Under the ROC Curve) improvement of 12–18%, with reduced false positives in critical event prediction. These improvements enabled healthcare operations to mobilize clinical responses earlier, allocate limited resources more effectively, and reduce potential adverse outcomes. When these predictions were integrated with SDN-driven network orchestration, network pathways prioritizing critical clinical data flows were dynamically allocated, ensuring that latency-sensitive traffic such as real-time vital sign updates and telemedicine video feeds consistently met service level targets. This synergy between AI analytics and SDN packet routing underscores the value of joint optimization across the analytics and network layers.

In industrial scenarios, the framework's predictive analytics capabilities were evaluated on sensor data streams representative of manufacturing equipment behavior and process line states. The objective was to detect early signs of mechanical wear and anomalies that precede failures. The AI models successfully identified pre-failure patterns with mean time to detection improvements of 25% over standard threshold-based systems. The ability to forecast faults allowed predictive maintenance scheduling, reducing unplanned downtime and improving overall equipment effectiveness (OEE). These benefits were amplified when combined with SDN/NFV orchestration because maintenance dashboards and alerting systems benefited from low-latency connectivity and adaptive bandwidth allocation. During periods of high network contention, the SDN controller prioritized critical industrial telemetry over less urgent traffic, preserving processing fidelity and reducing data loss. This application reinforces how the integrated framework enables real-time and dependable connectivity across critical system components.

Evaluating scalability was central to demonstrating the framework's suitability for large-scale deployments. In a series of stress tests, the system was scaled to simulate thousands of concurrent devices generating high-frequency data feeds. The experiments showed that the SDN controller's global view of network state, coupled with NFV-based service chaining, allowed rapid reconfiguration of virtualized functions such as firewalls, load balancers, and intrusion detection modules without significant performance degradation. When compared to static networking configurations, the SDN/NFV approach maintained lower end-to-end latency (average reduction of 22%) and higher throughput under load (average increase of 15%). These gains were statistically significant in cloud-simulated environments, proving that the framework can handle heterogeneous workloads without compromising quality of service. Real-time object detection modules incorporated into the framework, deployed for applications such as assistive healthcare monitoring and industrial vision inspection, maintained high detection precision (>94%) even under constrained network conditions. This result demonstrates that both high-level analytics and low-level perception tasks can coexist within the integrated architecture without performance bottlenecks.

Security and privacy evaluations were performed through simulated adversarial scenarios, including distributed denial of service (DDoS) attacks, man-in-the-middle attempts, and unauthorized data exposure events. The SDN controller was equipped with an AI-assisted detection module trained to recognize anomalous traffic patterns indicative of DDoS behavior. Upon detection, the system automatically triggered NFV-based mitigation functions that isolated suspicious flows and reinforced access control rules. Compared to traditional intrusion detection systems, this adaptive defense mechanism reduced attack impact by maintaining service availability at 83% of nominal levels versus 48% for non-adaptive systems. Privacy preservation was evaluated based on the framework's use of encryption and anonymization techniques applied before sensitive data entered cloud analytics processing pipelines. While encryption overhead introduced marginal processing latency (on average 8–12 ms per transaction), the trade-off for strong confidentiality was acceptable within application requirements for both healthcare and industrial contexts. Crucially, privacy preservation did not significantly diminish the predictive power of AI models because encrypted and anonymized features retained essential patterns necessary for high-accuracy classification. This balance highlights the effectiveness of integrating privacy technologies without undermining analytic performance.

Reliability under network topology changes was also a critical measure. Scenarios that involved link failures and node removals were simulated to stress test how quickly the framework could adapt its routing and service placement. The SDN controller's centralized control plane enabled rapid recomputation of optimal paths, rerouting traffic within milliseconds of failure detection. During these topology changes, the framework exhibited graceful performance degradation, avoiding catastrophic service loss. Traditional fixed routing systems without SDN demonstrated significant packet loss and service interruption during the same failures. These findings affirm that programmable network intelligence can substantially enhance resilience in complex distributed systems.

Furthermore, interoperability and deployment flexibility were assessed by integrating third-party cloud services and edge nodes across heterogeneous platforms. The framework's support for open APIs and standardized interfaces allowed seamless integration with cloud providers, edge gateways, and external analytics modules. This adaptability is particularly relevant for healthcare environments that rely on third-party electronic health record (EHR) systems or industrial settings with diverse device ecosystems. The results confirm that interoperability enhances practical deployability and reduces vendor lock-in risks.

While the framework showed significant strengths, the results also reveal areas requiring careful consideration. The complexity of managing cross-layer optimization — where decisions at the AI layer influence networking behaviors and vice versa — demands optimized coordination mechanisms to prevent oscillations or conflicting priorities. During experiments involving extreme workload spikes or simultaneous security events, coordination latency between AI predictions and SDN control decisions occasionally increased, suggesting the need for more efficient feedback loops or hierarchical control structures.

Overall, the results support the assertion that an integrated approach combining AI, SDN/NFV, and privacy preservation yields marked improvements in scalability, reliability, security, and operational intelligence. The positive impact across both healthcare and industrial scenarios suggests broad applicability. This discussion emphasizes that holistic system design — rather than isolated technology adoption — is essential for meeting the demands of modern intelligent cyber-physical ecosystems.

V. CONCLUSION

This research set out to design, implement, and evaluate an integrated framework that incorporates artificial intelligence, SDN/NFV-enabled cloud networking, and privacy-preserving security to support intelligent healthcare and industrial systems. The results confirm that such integration provides substantial improvements across multiple critical system dimensions including predictive accuracy, network performance, scalability, reliability, and security resilience. At the core of the framework is the recognition that intelligent systems cannot rely solely on isolated technologies. Instead, the interplay between analytics, adaptive networking, and secure data practices must be engineered holistically to achieve meaningful performance enhancements.

The predictive analytics components demonstrated clear advantages in both healthcare and industrial applications. In clinical settings, early detection of critical events and forecasting of resource demands contributed to improved readiness and potential reductions in adverse patient outcomes. Within industrial contexts, predictive failure detection facilitated proactive maintenance actions that improved operational uptime and process reliability. These outcomes substantiate the hypothesis that AI-driven foresight complements programmable networking to deliver real-time responsiveness in data-intensive environments.

SDN and NFV technologies were essential enablers of the framework's adaptive network capabilities. By decoupling control and data planes and virtualizing network functions, the system achieved dynamic routing, efficient traffic engineering, and on-demand deployment of security and optimization modules. These features were particularly impactful during high-load conditions and topology changes, where the framework maintained performance levels significantly better than baseline architectures. The research highlights that such programmability is indispensable in 5G and cloud environments characterized by heterogeneity and variable service demands.

Security and privacy preservation were achieved through a layered approach that combined encrypted data pipelines, anomaly detection, and NFV-based mitigation strategies. While encryption introduces processing overhead, the maintenance of data confidentiality — especially in healthcare use cases involving protected health information — is a non-negotiable requirement. The framework demonstrated that privacy techniques can be interwoven with analytics and networking without severely impacting performance. Adaptive security mechanisms, utilizing AI for anomaly recognition and SDN for dynamic enforcement, provided robust protection against simulated adversarial activities.

Interoperability and deployment flexibility were also confirmed through the framework's ability to integrate heterogeneous cloud services and edge platforms. This adaptability is crucial for real-world applicability because healthcare and industrial environments rarely consist of homogeneous device and service ecosystems. The use of open standards and API-driven interactions facilitated seamless connections with third-party services and external systems. This result supports the argument that modern intelligent systems must be designed for integration, not isolation.

However, the research also surfaced challenges inherent in coordinating cross-layer decisions. For instance, the latency between AI model outputs and SDN control updates occasionally led to suboptimal configurations during stress conditions. These coordination gaps suggest that future work should explore hierarchical control architectures or predictive control mechanisms where network decisions anticipate future states rather than react to present observations. Further, while the prototype demonstrated strong performance at scale, transitioning to production environments will require careful attention to real-time operational constraints, regulatory requirements, and hardware variability.

From a methodological perspective, the mixed use of simulation and prototype deployment allowed comprehensive evaluation, yet real-world field deployments would strengthen confidence in the framework's utility under diverse conditions. Large-scale healthcare institutions and industrial plants possess unique characteristics — including legacy systems, regulatory compliance considerations, and human factors — that could influence system behavior in ways not fully captured in controlled experiments.

Despite these limitations, the research makes a substantive contribution by delineating how AI, SDN/NFV, and privacy technologies can coalesce into an integrated architecture that meets pressing needs in intelligent healthcare and industrial cyber-physical systems. The findings suggest that the era of isolated technological silos is giving way to interconnected design paradigms where cross-layer optimization yields tangible benefits. As the pace of digital transformation continues, solutions like the proposed framework will play a central role in enabling automated decision support, resilient network operations, and secure data exchange.

This work also underscores the importance of multidisciplinary knowledge spanning artificial intelligence, network engineering, cloud computing, and cybersecurity. Architects of future intelligent systems must possess or collaborate across these domains to design comprehensive solutions that are both robust and adaptive. The research provides a roadmap for leveraging emerging technologies in concert rather than in competition, and its results can inform both academic inquiry and practical system development.

In conclusion, the integrated framework presented in this study demonstrates that cohesive design approaches that unify analytics, networking, and security deliver superior performance across key metrics relevant to intelligent healthcare and industrial systems. The lessons learned from the evaluation provide a foundation for future advancements, deployment strategies, and refinement of models that further bridge the gap between research innovation and real-world impact.

VI. FUTURE WORK

While the proposed integrated framework demonstrated significant advancements, several promising avenues for future research remain. One such area is the exploration of federated learning techniques to further enhance privacy and reduce dependency on centralized data aggregation. In healthcare, regulatory constraints often prohibit the transfer of sensitive data across institutional boundaries. Federated learning enables local model training on encrypted edge datasets while sharing only model updates with central coordinators, thereby preserving privacy without sacrificing analytic insight. Integrating federated and distributed learning within the framework could offer stronger privacy guarantees and reduce bandwidth usage.

Another direction is the integration of next-generation networking paradigms such as 6G and beyond. Emerging requirements for ultra-low latency, terabit-class throughput, and extreme device densities will demand even more adaptive network intelligence. Extending SDN/NFV capabilities to accommodate 6G slicing, context-aware routing, and AI-driven spectrum allocation would further improve performance in highly dynamic environments.

From a security perspective, future work should investigate the integration of blockchain and distributed ledger technologies to enhance data provenance, auditability, and tamper resistance. Although blockchain introduces overhead, it can provide immutable records of data transactions and security events, which is valuable in regulated domains like healthcare. Research is needed to optimize blockchain integration such that it complements the real-time requirements of the framework.

On the analytical front, expanding the AI model repertoire to include causal inference and explainable AI methods would improve decision transparency. In critical systems, stakeholders require not only accurate predictions but also interpretable rationales for AI decisions. Developing explainable modules that interact with network orchestration and alerting systems could foster trust and facilitate human oversight.

Finally, large-scale real-world deployments and longitudinal studies are necessary to evaluate the framework's performance under operational conditions. Field trials in healthcare institutions and industrial plants would reveal additional insights into human interaction, regulatory compliance challenges, hardware heterogeneity, and long-term maintenance needs. These deployments could guide the refinement of adaptive policies and automate feedback loops based on user experience and environmental variability.

REFERENCES

1. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599–616.
2. Keezhadath, A. A., Kota, R. K., & Selvaraj, A. (2021). Dynamic Pricing Optimization for Global Hospitality: Real-Time Data Integration and Decision Making. American Journal of Autonomous Systems and Robotics Engineering, 1, 131-165.
3. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.
4. Rajurkar, P. (2020). Predictive Analytics for Reducing Title V Deviations in Chemical Manufacturing. International Journal of Technology, Management and Humanities, 6(01-02), 7-18.
5. Jaikrishna, G., & Rajendran, S. (2020). Cost-effective privacy preserving of intermediate data using group search optimisation algorithm. International Journal of Business Information Systems, 35(2), 132-151.
6. Anand, L., & Neelanarayanan, V. (2019). Liver disease classification using deep learning algorithm. BEIESP, 8(12), 5105–5111.
7. Han, S., Zhang, X., Wang, J., & Leung, V. C. M. (2015). Mobile cloud sensing, big data, and 5G networks. IEEE Communications Magazine, 53(9), 60–65.
8. Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2019). Artificial intelligence for wireless networks: A survey. IEEE Journal on Selected Areas in Communications, 37(10), 2199–2223.
9. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.
10. Nagarajan, C., Tharani, B., Saravanan, S., & Muruganandam, M. (2021). Performance analysis of hybrid multi-Port AC-DC/DC-DC embedded based energy flow optimizing using resilient power flow control (RPFC) technique. Asian Journal of Electrical Sciences, 10(2), 16-28.

11. G. Vimal Raja, K. K. Sharma (2014). Analysis and Processing of Climatic data using data mining techniques. Envirogeochimica Acta 1 (8):460-467
12. Chandramohan, A. (2017). Exploring and overcoming major challenges faced by IT organizations in business process improvement of IT infrastructure in Chennai, Tamil Nadu. International Journal of Mechanical Engineering and Technology, 8(12), 254.
13. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.
14. Singh, A. SDN and NFV: A Case Study and Role in 5G and Beyond. https://www.researchgate.net/profile/Abhishek-Singh-679/publication/393804749_SDN_and_NFV_A_Case_Study_and_Role_in_5G_and_Beyond/links/687be8a54f72461c714f67f0/SDN-and-NFV-A-Case-Study-and-Role-in-5G-and-Beyond.pdf
15. Adari, V. K. (2021). Building trust in AI-first banking: Ethical models, explainability, and responsible governance. International Journal of Research and Applied Innovations (IJRAI), 4(2), 4913–4920. https://doi.org/10.15662/IJRAI.2021.0402004
16. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.
17. Chiang, M., Low, S. H., Calderbank, A. R., & Doyle, J. C. (2007). Layering as optimization decomposition: A mathematical theory of network architectures. Proceedings of the IEEE, 95(1), 255–312.
18. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
19. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. Proceedings of the 10th International Conference on Frontiers of Information Technology, 257–260.
20. Chivukula, V. (2020). Use of multiparty computation for measurement of ad performance without exchange of personally identifiable information (PII). International Journal of Engineering & Extended Technologies Research (IJEETR), 2(4), 1546-1551.
21. Zhang, Q., Chen, M., Li, L., & He, Y. (2018). Energy-efficient computation offloading for cyber-physical systems in cloud environments. IEEE Transactions on Industrial Informatics, 14(9), 3860–3870.