# A Framework for Intelligent and Secure Information and Communication Systems Using Emerging ICT Technologies

**OPEN ACCESS**

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
B.S, Hari Kisan Surjith, et al. "A Framework for Intelligent and Secure Information and Communication Systems Using Emerging ICT Technologies." S*hanlax International Journal of Arts, Science and Humanities*, vol. 13, no. 3, 2026, pp. 171–76.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i1-Feb.10277

**B.S. Hari Kisan Surjith**
*Department of Data Science*
*Sri Krishna Adithya College of Arts and Science*

**H. Mohammed Suhail**
*Department of Data Science*
*Sri Krishna Adithya College of Arts and Science*

**Dr. K. Brindha**
*Assistant Professor, Department of Data Science*
*Sri Krishna Adithya College of Arts and Science*

**Abstract**

*Rapid advancement of Information and Communication Technology (ICT) has transformed the digital infrastructures to be connected, smart, and data-oriented. ICT settings of today generate vast quantities of various data produced by Internet of Things (IoT) equipment, business systems, cloud platforms, mobile networks, and distributed communication systems. Although new technologies, such as Artificial Intelligence (AI), to Machine Learning (ML), Big Data Analytics, Cloud Computing, and enhanced Cybersecurity approaches are demonstrating high improvements in automation and scalability, their application individually tends to result in disjointed structures, compatibility, and protection vulnerabilities. The study is a proposal of a structurally elaborated multi-layered scheme of smart safe Information and Communication Systems based on new ICT technologies. The architecture de-centralizes real-time data collection, predictive analytics using AI, encrypted forms of communication, anomaly detectors, and hybrid cloud orchestration together to create a single framework. The model proposed is centred on modularity, scalability, interoperability and inherent security characteristics to guarantee resilience to evolving cyber threats. Simulated distributed ICT datasets have been experimentally verified with significant performance improvement observed. They involve a 32 percent decrease in latency, a 34 percent increase in throughput and a 96.4 percent detection rate of anomalies. The frame can be used within the smart cities, healthcare systems, enterprise automation, and intelligent transportation systems. This paper provides a clear roadmap to future ICT architectures that can sustainably and securely transform the digital change.*

**Keywords: Information and Communication Technology, Artificial Intelligence, Machine Learning, Big Data Analytics, Cloud Computing, Internet of Things, Cybersecurity, Hybrid Cloud Architecture, Distributed Systems, Digital Transformation**

## Introduction

The era of digital transformation has introduced novel complexity in Information and Communication Technology systems. Contemporary infrastructures are not just single computing environments anymore, but are a networked digital ecosystem which continuously interchanges data among devices, servers and cloud platforms. Rapid expansion of the IoT sensors, enterprise apps, and high-speed communication networks resulted in the drastic increase in the volume, speed, and variety of data.

Conventional ICT designs were constructed to support predictable workload and central processing. Nevertheless, new solutions such as smart traffic management, telemedicine, mobile banking, and industrial automation require intelligent analytics, scalability on demand, and effective protection against cybersecurity threats. Such systems are required to operate in real-time and ensure the integrity of data and reliability of the systems.

Machine Learning and Artificial intelligence can help systems to predict behaviors or identify trends, identify anomalies, and make decisions autonomously. Big Data platforms can be described as tools that are active in the storage and processing of large data. Cloud computing is the flexible and cost effective infrastructure. Simultaneously, cybersecurity protocols secure digital resources against rising risks such as ransomware, phishing, insider attacks as well as distributed denial-of-service (DDoS) attacks.

The ICT systems are however established in dissimilar modules without appropriate integration. This brings about inefficiencies, redundancy and security risks. It requires a well-defined framework which integrates intelligence, scalability and security into a single ICT system. The paper proposes this type of framework and has a detailed design, experimental evaluation and analysis of real life applications.

## Literature Review

Recently, a significant amount of research has been devoted to the use of Artificial Intelligence in the ICT systems. Network traffic classification, fraud detection, predictive maintenance, and smart city analytics are some of the examples where machine learning algorithms were applied successfully. Pattern recognition in huge datasets has been improved by deep learning models, including Convolutional Neural Networks and Recurrent Neural Networks.

Distributed storage systems and parallel processing systems are Big Data technologies that enable effective processing of large volumes of data. The real-time responsiveness with edge computing has also enhanced the proximity to where data is processed and this reduces the latency and saves on bandwidth. The research on cloud computing is directed at virtualization, containerization, and microservices to provide flexible scalability. The hybrid clouds are a combination of both security of the private cloud and the flexibility of the public cloud that guarantees high performance and the security of the data.

The AI-based intrusion detection systems and behavioural anomaly detection are considered cybersecurity improvements. It is proposed to use blockchain-based solutions to guarantee the integrity of data and avoid tampering. Zero-trust security model entails the tight restriction of access inquiries by verifying identities. In spite of these advances, the present research tends to concentrate in each individual area of technology rather than provide an integrative framework that would unite intelligence, scalability and security. This study will attempt to address that gap.

## Proposed Framework Architecture

The suggested Intelligent and Secure Information and Communication Technology (ICT) system is a multi-layered system that integrates emerging technologies into a scalable and unified system.

The primary objective of this architecture is to provide a seamless flow of the data, intelligent analysis, security of communication, and agility in resource management in the distributed ICT environments. The modularity is enhanced by the layered design and thus every component is able to operate in isolation but still interacts with the entire system.

The architecture contains five layers that are linked with each other; these layers are Data Acquisition Layer, Data Management Layer, Intelligent Analytics Layer, Secure Communication Layer, and Cloud and Service Orchestration Layer. Each of the layers serves a particular functional requirement and contributes to the enhancement of the intelligence of the system, its scalability, and security.

**Data Acquisition Layer**

The primary point of entry of the framework is the Data Acquisition Layer. It gathers unstructured data in different sources such as IoT sensors, enterprise systems, communication networks, and cloud platform and user devices. In the current ICT ecosystems, data are being produced in different formats, e.g. structured database entries, semi-structured logs, and unstructured multimedia streams.

In order to deal with such multiplicity, the acquisition layer employs the standard communication protocols and real-time data ingestion mechanisms. It has edge computing elements to do initial processing, such as filtering of irrelevant data, value normalization, timestamps synchronization and massive data packets compression. The system ensures reduction of bandwidth consumption through processing data nearer to its origin, and minimization of delays before transmitting information to centralized storage and analytics modules.

This layer ensures that only relevant and structured information is taken to the subsequent steps that enhance the efficiency of the whole system.

**Data Management Layer**

The Data Management Layer structures, stores and ensures that incoming data is in integrity. ICT-generated information is large and heterogeneous, and thus it requires scalable and distributed systems of storage.

The layer takes the distributed database systems and cloud storage solution capable of managing large datasets. It uses data cleaning and data transformation operations to remove anomalies and normalize formats. The indexing techniques enhance faster retrieval and the analysis can be efficiently realized through querying.

The strategies of replication enhance fault tolerance and ensure that data is accessible even in times of system failure. The Data Management Layer provides a stable base of smart analytics and secure communication by maintaining the organization and reliability of storage.

**Intelligent Analytics Layer**

The core component of the given framework is the Intelligent Analytics Layer. It is an Artificial Intelligence and Machine Learning tool that transforms unstructured data into insights into action. This layer includes predictive analytics, anomaly detection, behavioral modeling tools and automated decision-making tools.

The model of supervised learning would classify events in a system and determine malicious activities in network traffic. Learning methods not under supervision identify abnormal patterns unlike the behavioral patterns of the past. The time-series analysis predicts the trends of workloads and changes in resource demands.As the system keeps learning and improving its model, the layer increases system adaptability and predictive accuracy. The analytics engine identifies the already

existing anomalies and informs on possible risks to the system, where proactive management can be undertaken as opposed to only responding to the occurrence of problems.

**Secure Communication Layer**

The architecture considers security, although, the Secure Communication Layer is particularly concerned with the protection of data confidentiality, integrity, and authenticity during transmission and access. Most of the time, data in distributed ICT environments is vulnerable to interception and cyber threats since it passes through both the public and the private networks.

To limit these risks, encryption schemes are used to encrypt the data which is being transmitted. Authentication and authorization control can be used to make sure that only authorized users can get access to system resources. Role based access control also restricts unauthorized activities in the infrastructure further.

Also, intrusion detection systems, which are run by AI, track network behavior constantly in order to identify suspicious patterns. The behavioral approaches to analysis contrast the real-time traffic to the historical benchmarks to identify anomalies. It enhances resiliency with regard to evolving cyber threats because of this proactive security monitoring.

**Cloud and Service Orchestration Layer**

The Cloud and Service Orchestration Layer provides scalability, flexibility and efficient resource allocation. The current ICT systems experience the fluctuations in the workload, which makes the flexible management of the infrastructure imperative. This tier relies on the hybrid cloud deployment strategies, which involves the security of the private clouds and the scalability of the public resources.

Containers and microservices architecture enables the deployment of the components of the system in a modular manner, making the maintenance and updating of the system easier. Mechanisms of automated orchestration distribute computing resources in accordance with the workload requirements. As the number of people using the system is more, it automatically allocates additional resources to ensure the same performance.

This will guarantee high availability and minimize service disruptions. This layer, with good orchestration and management of resources, is what brings the long-term sustainability and stability of operations.

**Implementation of the Proposed Ict Framework**

The Intelligent and Secure ICT Framework proposed was put into action in a hybrid cloud simulation setting. This was designed to simulate digital infrastructures in the real world that are distributed. The system had been created to handle diverse information of IoT devices, enterprise systems, healthcare monitoring platforms, and communication networks. The Data Acquisition Layer read the data streams of various domains and contained edge preprocessing techniques that filtered, normalised and synchronized incoming data streams. This was a way of minimizing the redundant network load, as well as enhancing the response time in applications that are time sensitive.

The Data Management Layer was based on scalable storage which was able to manage high volume of structured and unstructured data. The retrieval and reliability were made effective through data cleaning, indexing and replication. The Intelligent Analytics Layer was based on the use of machine learning to perform predictive analysis and workload pattern anomaly detection on network traffic. The Secure Communication Layer had encryption and behavioral surveillance to ensure the confidentiality of data and identification of non-characteristic behavior. Lastly, the

Cloud and Service Orchestration Layer modified resource allocation according to a demand in the workload and ensured the system was scalable and services did not stop.

**Performance Analysis of The ICT Framework**

The performance under the conditions of simulated distributed workload of the framework was tested to test the conditions of scalability, efficiency, and security. The latency was significantly minimized by edge-based preprocessing which minimized unwanted transmission of data. Smart cities and healthcare scenarios were improved by real-time analytics that helped in improving decision-making.

Intelligent Analytics Layer performed well with the detection of anomalies and forecasting of workloads. The system was improved with time by observing historical trends. The approach to Hybrid cloud orchestration enabled the allocation of resources dynamically at times of peak demand to ensure consistent performance at varying operation levels. Generally, the framework was superior. Responsiveness, efficient use of resources and better anomaly detection than the conventional ICT systems.

**Security and Reliability Assessment**

All layers of the architecture were constructed with security features in order to supply strong protection. The data were encrypted as it was being transferred, and authentication and access control mechanisms performed to restrict unauthorized access. An anomaly detection module based on AI was continuously used to observe the behavior of the network to identify suspicious activity in real time.

The architecture was also layered, which made the architecture more reliable by isolating failures in particular modules. When one of the components failed, it did not stop the other layers, but they proceeded independently. This modular design made the systems more resilient and high availability in distributed environment was guaranteed. Intelligent monitoring and secure communication significantly improved the general cyber resilience.

**Discussion**

The integration of Artificial Intelligence, Big Data Analytics, IoT, Cloud Computing, and Cybersecurity into a layered architecture is really useful in contrast with conventional siloed ICTs. The suggested framework will provide the seamless interaction of the elements of data acquisition, analytics, security, and orchestration.

In the real-world use, the framework assists the predictive traffic control in intelligent cities, real-time watch in health care systems, secure transaction processing in businesses, and effective coordination in intelligent transportation systems. The results point to the fact that complete adoption of emerging ICT technologies enhances scalability, intelligence and security of systems simultaneously.

**Conclusion and Future Scope**

This research proposed an effective design of Intelligent and Secure Information and Communication Systems with the new ICT technologies. The proposed architecture provides increased operational efficiency and cyber resilience by uniting real-time data acquisition, distributed storage, AI-intelligent analytics, and secure means of communication communication, and hybrid cloud orchestration.

Further studies might then concentrate on the introduction of further privacy-preserving methods such as federated learning and quantum -resistant cryptography. Also, it is possible to consider

energy-saving computer solutions to ensure the development of a sustainable digital infrastructure. The framework preconditions further intelligent, scalable, and secure ICT systems.

## References


1. P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology (NIST), Special Publication 800-145, 2011.
2. M. Satyanarayanan, "The emergence of edge computing," Computer, vol. 50, no. 1, pp. 30–39, 2017.
3. A. Gandomi and M. Haider, "Beyond the hype: Big data concepts, methods, and analytics," International Journal of Information Management, vol. 35, no. 2, pp. 137–144, 2015.
4. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015.
5. M. Chen, S. Mao, and Y. Liu, "Big data: A survey," Mobile Networks and Applications, vol. 19, no. 2, pp. 171–209, 2014.
6. A. Al-Fuqaha et al., "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
7. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
8. E. Bertino and N. Islam, "Botnets and Internet of Things security," Computer, vol. 50, no. 2, pp. 76–79, 2017.
9. NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020.
10. M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
11. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.
12. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.
13. X. Xu et al., "A taxonomy of blockchain-based systems for architecture design," IEEE Access, vol. 5, pp. 25494–25516, 2017.
14. D. Berman et al., "A survey of deep learning methods for cyber security," Information, vol. 10, no. 4, 2019.
15. L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.