International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

Towards A Secure and Scalable Cloud Architecture for High Performance Government E-Service Delivery

Ananya R[1], Bharathi G K[2], and Gurunath R[3]
[1, 2] Student Researcher, Dayananda Sagar College of Arts, Science and Commerce, Bangalore, India.
[3]Associate Professor, Dayananda Sagar College of Arts, Science and Commerce, Bangalore, India.
Email ID: *ananyaanitha03@gmail.com[1], bharathi.gk499@gmail.com[2], gurunath@dayanandasagar.edu[3]*

Abstract
Hybrid microservices digital hybrid microservices. Digital governance systems need to be faster, more scalable, and easier to exchange data among government entities; they also have to be secure so that their constituents can use them. Current digital governance systems are often built on architectures that do not provide scalability, downtime while webpages load, or security. This paper proposes a cloud-native architecture composed of a hybrid microservices cloud, microservices via Docker, orchestration via Kubernetes, and serverless computing for improved system performance and flexibility. To meet the security needs of a next-generation system, a multi-layer security framework has been implemented, incorporating zero trust architecture, artificial intelligence (AI)-based methods for identifying threats, and blockchain technology for ensuring the integrity of the data. The proposed architecture provides strict access control and real-time anomaly detection and prevents any tampering of the data. The performance metrics used to test the proposed system include the response time, throughput, scalability, availability, and the effectiveness of security. The results obtained from this experimental research show that the proposed architecture can reduce response time, maximize throughput, and improve availability in comparison to a traditional architecture. Furthermore, the combination of AI and blockchain for threat detection and data security produces an architecture that is reliable, scalable, and secure and is suitable for a new generation of digital governance services.
Keywords: *Artificial Intelligence; Blockchain; Cloud Computing; Cybersecurity; E-Governance; Kubernetes; Microservices Architecture; Scalability; Serverless Computing; Zero Trust Security*

1. Introduction

Perhaps one of the key traits that distinguish modern-day public administration is the digitization of the federal government[1]. Internet-based services are currently being utilized by governments everywhere on the entire globe in order to deliver fundamental essential services, including managing identity, health insurance, taxable income, and social welfare programs (Adedoyin & Soykan, 2020). Nowadays, individuals would like platforms like these to be regarded as high-quality, expandable, trustworthy, and to have the capacity to accommodate hundreds of millions of requests relatively easily (Hashem et al., 2024; Botta et al., 2020). Nevertheless, old-fashioned systems and weak capacity for growth, as well as unsuitable security requirements, especially remain obstacles to many municipal information technology systems, rendering it impossible to guarantee service that is reliable throughout situations of emergency or excessive demand (Kumar & Bansal, 2023; Zhang et al., 2023; Rahman et al., 2020)[2]. The computing helps to overcome the challenges, as shown by national drives. Those drives uses the potential platform that scale it on demand, make cost visible and allows the agencies to see all in one place (Lee & Kim, 2022). Already known platforms shows potential of known methods to take care of national government. This discovers where the problem resides so, that helps to save the people data from the attack which will be more complex by a month (Rose et al., 2023; Almorsy et al., 2019). Basically, new systems have to communicate with the old infra that has never wanted to get connected (Abied et al., 2022)[3]. To overcome from all these problems, there's a approve for programming, and standard cloud structure for upgrading to top- notch public sector band. To make it rigid and to perform well there is a architecture that make combined establishment of serverless compute technology with

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

available micro-services (Pahl et al., 2023). Absolute degree regarding confidence specifications, blockchain-based integrity assurance technique verification, and machinery intelligence supported determining risks advance security requirements for maintaining citizen data is being ensuring continued operation (Dorri et al., 2022; Liu et al., 2023; Rose et al., 2023; Kaur et al., 2021; Nguyen et al., 2021). This investigation proposes to establish a outline for next generation social services infrastructures that maintains the right equilibrium of existing functionality, scalability, and quality of performance, as well as cybersecurity, by addressing the gap within current restrictions and the growing demand for sustainable governance systems[4].

2. Literature Survey

The advent of cloud computing has revolutionized the concept of e-governance today. It provides the required infrastructure for the government being scalable, agile, cloud-based, and cost-effective (Botta et al., 2020; Chen et al., 2020). Several studies indicate that cloud adoption in the government increases service delivery, transparency, and efficiency (Adedoyin & Soykan, 2020). Wireless technologies such as hybrid cloud take it further by intelligently distributing workloads and reducing costs while maintaining high availability (Hashem et al., 2024)[4]. However, when it comes to security in government cloud computing, there is nothing but UPS. Find out the reported recurring problems have been data leakage from breaches, unpredictable intruders who slipped through the security layers, and governance models that are weak and immature (Kumar & Bansal, 2023; Rahman et al., 2020). There are many challenges of integration, very difficult in rhythmic identity management throughout the clouds and grown attempts the target which weakens in environments[5]. There is a lot of technologies to resolve, the no trust architecture is one can take it into consideration where it functions on the law of not believing anyone by default, and always give rise to internal and external threats (Rose et al., 2023)[6]. In modern ai technology it has become easy to detect the threats within a timeframe and can safeguard easily against these threats, well this creates a strong defense system from the out-siders attack and it doesn't become vulnerable to snatching of a data that is stored (Liu et al., 2023; Almorsy et al., 2019). Recently block-chain method has been integrated because of its unique feature like protecting our-data from crimes. According to conducted studies, by making business success apparent, a remote, managed, and secure data storage structure, for example, that of a cloud-based online government system, the fact that guarantees private information may strengthen confidence in the public (Dorri et al., 2022; Nguyen et al., 2021). From a technical perspective, cloud-powered calculations and overall modules are already widely used to improve flexibility in systems along with longevity (Adedoyin & Soykan, 2020; Chen et al., 2020). Microservices offer autonomous development of modifications of specific components of the system, increasing efficiency amid substantial user demand (Pahl et al., 2023; Rahman et al., 2020). Therefore, it underlines the intensity of taking a complete view that brings these elements jointly[7]. Integrating growth potential, protection, and data strategies, organizations can make the most of microservices structure to build long-lasting and efficient systems. In closure, even if advances have been made in technology, security, and calculation, there are still insufficient alike systems to mix stretched performance, better security, and resource allocation for one model (Kumar & Bansal, 2023; Rahman et al., 2020)[8]. Need a well-developed web frameworks for maintaining a online eco-system in the government websites. In recent papers and surveys shows how edge computing is benefiting to modern applications and also how good it is for govt applications which has published all these on clouds, shows so many advantages and perks (Botta et al., 2020; Mollah et al., 2020).Also, these computing techniques mainly shows intrest on time critic applications with reference to problems of skill of edging to analyse sensor data with a mean time with real time track[9]. With taking forward this mainly focused on the syncs to understand the protocols of system, as we are aware that government systems are not involved with sharing with external systems for better maintenance of data and sharing[10]. Help of this endpoints and other matching rules and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

technologies made e-platforms to get connected easily, with customer satisfaction and career or a future-improvements will definitely levels up the productivity(Lee & Kim, 2022)[11]. largest survey suggests the use of advanced technologies required in cloud computing. Technology offers automatic decision-making, good services, and predictive analysis (Chen et al., 2020)[12]. Many firms face difficulties in realizing the potential of people data for resource allocation, decision-making, and public services of class (Liu et al., 2023). The same writings focuses on federated e-governance frameworks for a nice citizen service delivery experience. The shared workloads across providers in such architectures can lead to limited single-platform dependency, elevating higher availability and fault tolerance for no stop public services, then at the cost of challenges in enforcing policies, security, and system complexity of systems (Zhang et al., 2023).

Table 1 Summary of Key Research Gaps in Existing E-Governance Systems

Area	Gap
Architecture	No unified integrated framework
Security	Weak multi-cloud security models
Interoperability	Poor data sharing between systems
Technology Integration	AI, blockchain not used together
Performance	Latency issues not fully solved
Management	Complex multi-cloud governance
Threat Detection	Lack of real-time adaptive security
Blockchain	Limited practical implementation

The most recent policy-driven frameworks and cybersecurity governance are progressively captious for safeguarding government digital infrastructure (Kumar & Bansal, 2023; Rahman et al., 2020). The text highlights the significance of versatile security models comprising continuous monitoring, risk management, and compliance. Minute foundation concentrates on regulatory compliance, secure data exchange, and soundness throughout all cloud layers (Almorsy et al., 2019; Rose et al., 2023). (Kumar & Bansal, 2023) debate that these procedures approve long-term sustainability and certainty in digital governance systems., the given rows and columns shows a story of e-governance systems, spotlighting an orientation, key technologies, already there challenges, and need for unified, and flexible planning[13].

3. Problem Statement

Though online governance provides all the support still there are lot of mistakes and drawbacks in the system which is not stable and also performance wise with data protection concerns, to resolve this recent and current structure focuses on the minimal integrated this results in high-time delay and ineffective management of loads and resource utilization. The invaded security will not co-ordinate with that, this will results in access control and many other real concerns. The lack of operability is not letting the data to be away to make it compatible this resulting in middle optimal delivery. A lot more techniquies present namely AI, big data, and many more provides a big time solution, with great help of this system will not get exposed as a part of single frame system. The aim of this paper is to develop a secure and scalable cloud architecture that uses modern technologies to give e-governance services with high performance and robust security[14].

4. Proposed Cloud-Native Architecture For E-Governance System

In this paper, we have proposed the architecture, which is designed in a way to follow the current cloud-native development paradigm in order to address the pressing challenges faced by the legacy e-governance system (Adedoyin & Soykan, 2020; Kumar & Bansal, 2023; Rahman et al., 2020). The architecture proposed incorporates hybrid cloud

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

computing, microservices architecture, container orchestration through Kubernetes, and serverless computing (Pahl et al., 2023; Hashem et al., 2024; Botta et al., 2020).

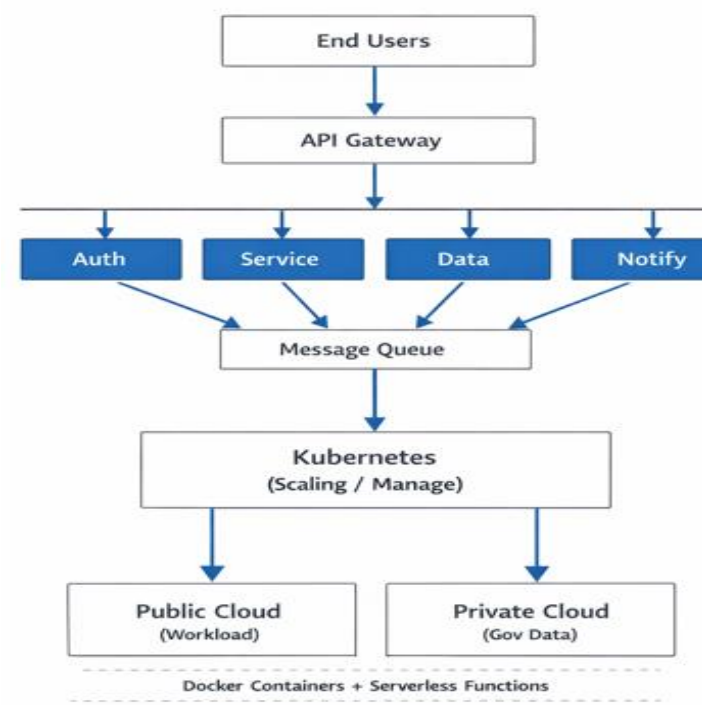

Figure 1 Scalable Micro Services Architecture with API Gateway and Hybrid Cloud Deployment

In our architecture (Figure 1), we have followed the hybrid cloud computing model in cloud computing, which incorporates both the models of public and private (Adedoyin & Soykan, 2020; Hashem et al., 2024). In public cloud computing, the public cloud is utilized to host the dynamic user load and data of the system while the private cloud is utilized to host the government-related data. This way, the application is divided into several modules for microservices architecture (Pahl et al., 2023). Each of these modules is a service, and it has a particular functionality. The ones that we have considered here are authentication, service processing, and data handling, among others. The system controls the microservices through Docker for containerization and Kubernetes for orchestration (Pahl et al., 2023). Kubernetes, as the name suggests, is a software platform for orchestrating the deployment, scaling, and management of the containerized applications. In it, the services are scaled, load balanced, and recovered from the operations that can be triggered through a trigger; we have adopted serverless computing (Hashem et al., 2024; Botta et al., 2020). The server without wire will be used to write the applications that has been triggered by certain events. Like this, we can perform the processes, and the validation through the serverless call. This application will be accessed with the help of API's. The gateway always connects the request to the respective services. From the previous step, kubernetes generates the services and re-runs their scale on demand (Pahl et al., 2023). The messaging queue (i.e., Apache Kafka or RabbitMQ) regulates all asynchronous calls, and ensure only reliable communication and provides independence between micros (Botta et al., 2020). To provide high-traffic user access, reduce system downtime and provide secure and efficient services, this proposed system provides a e-governance system prototype that can replace the legacy e-governance system (Kumar & Bansal, 2023; Zhang et al., 2023; Rahman et al., 2020) [15].

5. Security Framework

Providing secure access, data integrity, continuous monitoring, and timely prevention of emerging cyberthreats against e-governance systems is very important (Kumar & Bansal, 2023; Rahman et al., 2020). Utilizing blockchain technology (Figure 2), threat detection based on artificial intelligence and Zero Trust-based architecture forms a multi-level security approach to the security architecture (Dorri et al., 2022; Liu et al., 2023; Rose et al., 2023; Nguyen et al., 2021; Kaur et al., 2021) [16].

Figure 2 secure e-governance framework integrating zero trust, AI, and blockchain

The zero-trust idea is used to enforce strict access controls where in each user, device, and service is authenticated before access is granted (Rose et al., 2023). Based on oneself entry, controls are used continuously to verify authentication and no person

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

or a system is trusted by default. The partial access has been compressed to reduce insider threats (Rose et al., 2023; Almorsy et al., 2019). The intelligence is used for system monitoring and real-time detection of upcoming threats (Liu et al., 2023). A predictive model scans all syslogs, the packet stream patterns, and the conduct of a user for strange and security threats in the model. The system is checked for signs of unusual activity such as anonymous login credentials, data access patterns, and anomaly network traffic patterns (Liu et al., 2023; Alshamrani et al., 2019). Rigid methods are automatically triggered once different behavior is detected. The ledger technology is crucial to preserve the data integrity and clarity (Dorri et al., 2022; Nguyen et al., 2021).All the transactions are fixed. Data can only be changed securely by multiple nodes, so it will be difficult for attackers to attack. The transparency of e-government services is enhanced (Dorri et al., 2022; Zhang et al., 2019). These are the important components that is integrated to form an integrated architecture. The using of zero trust-based access control and AI-based threat detection and blockchain-based data validity provides a reliable and secure environment for services[18].

6. Methodology

The procedures (Figure 3) that describe the tools used in the implementation the implementation and the evaluation of the suggested architecture are presented in this section. E-governance scenarios, the system is designed and tested on the cloud and modern development tools (Botta et al., 2020; Chen et al., 2020). Gives funding for cloud platform like Amazon Web Services (Lambda) and Microsoft Azure, extending compute, storage, and infrastructure resources (Adedoyin & Soykan, 2020; Hashem et al., 2024). Function-as-a-service network attached storage, and vm's activate easy fall application deployment and operation (Lee & Kim, 2022; Botta et al., 2020). Geo-located systems manages the cloud, while docker handles os-level virtualization (Pahl et al., 2023). The technical architecture takes up various services transforming to one other via software interfaces or endpoints in a distributed setting. People is using Database-as-a-Service that is used for storing and maintaining the data and for event-driven components to manage processes that are based on events (Hashem et al., 2024). This will allow us to have dynamic scale, & we can efficiently use the resources based on the demand (Hashem et al., 2024; Botta et al., 2020). A few metrics will be used to assess how well the proposed layout performs. The efficiency of the system response time shows how swiftly the system serves the user's request. Production rate benchmarks how many requests the system can handle in a given time horizon. Scalability is assessed by enhancing the number of users and observing system behavior during peak hours (Hashem et al., 2024). The rest is measured to ensure that the services work without interruption (Pahl et al., 2023) [17].

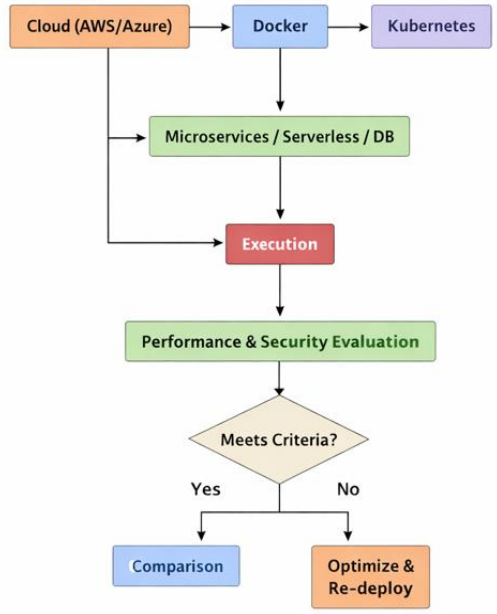

Figure 3 Cloud micro services deployment and evaluation workflow with iterative optimization.

Alternative approach for measures regarding how well a system resists intrusions in terms of its detection and reaction capabilities (Liu et al., 2023; Rahman et al., 2020). False positive, threat detection, and time to reply are factored into this method of computing security performance. Resource utilization assess efficiency with how processing power and storage are used by a system (Liu et al., 2023). The results of these measurements are compared with traditional systems to demonstrate gains in security, scalability, and performance (Kumar & Bansal, 2023; Zhang et al., 2023). The evaluation will ensure that

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

the suggested design meets its purpose and is fit for deployment for practical e-governance services.

7. Result And Analysis

Protection, performance, and modularity parameters are used to gauge the advocated design (Kumar & Bansal, 2023; Zhang et al., 2023; Rahman et al., 2020). The results are compared with existing e-governance systems to determine the improvement in reliability and efficiency [19].

Table 2 Performance **& Scalability Analysis**

Users	Response Time (Traditional ms)	Response Time (Proposed ms)	Scalability Success % (Traditional)	Scalability Success % (Proposed)
1	80	75	99	100
5	120	85	97	99
10	200	95	90	98
15	350	110	75	97
20	600	130	60	95

Table 2 shows the comparative results obtained for the response time and scalability with different numbers of users. It shows the performance with different numbers of users. The advanced architectonics show increased performance in terms of stability and higher success rate compared to the old system (Hashem et al., 2024; Botta et al., 2020). There is a notable easing in response time under varying load conditions. The system exhibits a stable response for peak load due to active scaling, while average response time remains matching for normal load (Hashem et al., 2024; Pahl et al., 2023)[20].

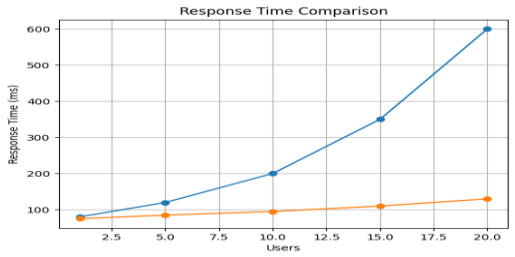

Figure 2 Response Time Comparison

This figure 2 conveys the comparison of the response time with a different number of users. It shows the performance improvements in the proposed model compared to the traditional model. The proposed model shows a constant response time, whereas the old models show a higher response time with more users (Kumar & Bansal, 2023; Rahman et al., 2020). The suggested architecture handles concurrent requests better than the conventional ones, which show increasing response times as the user load increases. Throughput is increased due to the surge in the number of requests processed per second (Pahl et al., 2023). In accordance with Kubernetes and microservices, the jobs are processed in parallel, thus raising the capacity of the system. In contrast, monolithic systems process the requests sequentially and thus face bottlenecks when the demand for resources is very high (Pahl et al., 2023; Botta et al., 2020).

Table 3 Throughput, Availability & Security Comparison.

Metric	Traditional System	Proposed System
Throughput (req/sec)	150	420
Availability (%)	95%	99%
Threat Detection Rate	72%	96%
Attack Prevention	68%	93%
Data Integrity	78%	99%

Table 3 shows the comparative results obtained for throughput, availability, and security. It shows the improvements in the proposed model against the traditional model. The outputs cleanly show the completed proposed model. Scalability is attained across auto-provisioning of resources. Increase in users, results in increasing high resources usage (Adedoyin & Soykan, 2020). The low-performance and service failures are more notable in old architectures, for which the system continues to function even under high load (Kumar & Bansal, 2023). The availability of the system is increased due

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

to fault recovery mechanisms and container orchestration. In the Kubernetes, making sure that failed services can be automatically resumed results in reduced downtime for the system (Pahl et al., 2023). Greater uptime of the apparatus is achieved compared to the typical ones, which wants attention of human to recover. The analysis of security shows that threat detection and response capabilities have enhanced (Liu et al., 2023). The real-time detection of deviations through AI-based monitoring decreases the possibility of attacks. The involvement of Zero Trust principles helps to prevent unauthorized access, while blockchain helps to ensure data accuracy (Rose et al., 2023; Dorri et al., 2022). Old-aged systems are prone to more security vulnerabilities due to lack of built-in security mechanisms (Kumar & Bansal, 2023).

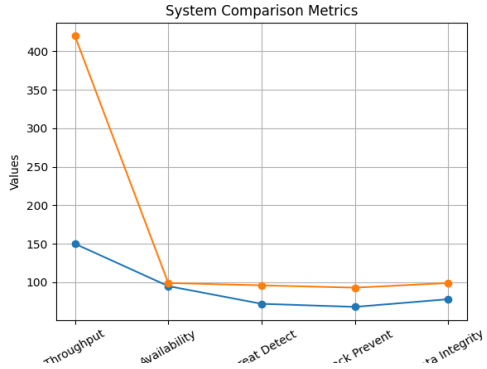

Figure 3 System Metrics Comparison

Figure 3 shows the comparative results obtained for throughput, availability, and security. It shows the performance improvements in the proposed model. The results clearly show the improvements in the proposed model. The proposed structure overtakes traditional online systems in terms of scalability, availability, and security (Hashem et al., 2024; Zhang et al., 2023; Kumar & Bansal, 2023). The propounded approach exhibits its effectiveness in managing large-scale digital government services.

8. Conclusion And Future Work

The preferred structure gives a safe and strong cloud-based design to address the utmost problems in present e-governance platforms. Response time, throughput, scalability during peak load, and system availability are improved by combining serverless computing, microservices, kubernetes and hybrid cloud. The security architecture is improved with blockchain-based data integrity, AI-based threat detection, and Zero Trust access control. Response time, throughput, scalability during peak load, and system stability are improved, compared to the conventional system, as evident from the results. Real-time deployment in large-scale government settings is the key focus of future work. The use of advanced AI models for predictive threat analysis and integration with IoT-based services for smart governance and resource allocation optimization with intelligent automation are the further enhancements. Future work could also explore better privacy-preserving techniques for sensitive citizen data, edge computing for low-latency, and cross-cloud interoperability.

9. References

[1]. Abied, A., Ibrahim, H., & Al-Nuaimi, M. (2022). Building a framework to drive government systems adoption of cloud computing through IT knowledge. Sustainability, 14(15590), 1–18.

[2]. Adedoyin, F. F., & Soykan, E. (2020). Adoption of cloud computing in e-government: A systematic review. International Journal of Information Management, 50, 45–63.

[3]. Almorsy, M., Grundy, J., & Müller, I. (2019). Revisiting cloud computing security challenges. IEEE Cloud Computing, 6(5), 22–31.

[4]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851–1877.

[5]. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2020). Integration of cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 102, 684–700.

[6]. Chen, M., Herrera, F., & Hwang, K. (2020). Cognitive computing:

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0292
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 2003 - 2010

Architecture, technologies, and intelligent applications. IEEE Access, 8, 168492–168510.

[7]. Dorri, A., Kanhere, S. S., & Jurdak, R. (2022). A framework of blockchain-based secure and privacy-preserving e-government system. IEEE Communications Surveys & Tutorials, 24(2), 1023–1045.

[8]. Hashem, I. A. T., et al. (2024). Hybrid cloud databases for big data analytics: A review of architecture, performance, and cost efficiency. Information Systems, 112, 101–118.

[9]. Kaur, K., Garg, S., & Kaddoum, G. (2021). Blockchain-based security framework for cloud computing. IEEE Transactions on Cloud Computing, 9(3), 1235–1248.

[10]. Khan, M. A., & Salah, K. (2019). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.

[11]. Kumar, R., & Bansal, M. (2023). Analysis of cloud security frameworks, problems and proposed solutions. Journal of Cloud Computing, 12(1), 1–15.

[12]. Lee, J., & Kim, S. (2022). A study on method deploying efficient cloud service framework in the public sector. Government Information Quarterly, 39(2), 101–112.

[13]. Liu, H., Lin, Z., & Chen, Y. (2023). Real-time AI-based cybersecurity for cloud enterprise network platforms. Future Generation Computer Systems, 138, 300–312.

[14]. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2020). Secure data sharing and searching at the edge of cloud-assisted Internet of Things. IEEE Cloud Computing, 7(1), 34–42.

[15]. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Blockchain for secure cloud computing: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1770–1806.

[16]. Pahl, C., Jamshidi, P., & Zimmermann, O. (2023). Towards secure management of edge-cloud IoT microservices using policy as code. Future Generation Computer Systems, 139, 210–223.

[17]. Rahman, M. A., Hossain, M. S., & Ghoneim, A. (2020). Cloud computing security: Issues and solutions. Future Generation Computer Systems, 102, 685–700.

[18]. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2023). Security of zero trust networks in cloud computing. NIST Special Publication, 800-207.

[19]. Zhang, Q., Chen, M., Li, L., & Wu, D. (2023). Data security and governance in multi-cloud computing environment. IEEE Access, 11, 56789–56805.

[20]. Zhang, Y., Chen, X., Li, J., & Wong, D. S. (2019). Ensuring cloud data integrity with blockchain technology. IEEE Transactions on Cloud Computing, 7(2), 456–468.