PROCEEDINGS OF SCIENCE

Towards Privacy and Accessibility Through Resource Integration

Kundjanasith Thonglek,[a,*] **Chonho Lee,**[a] **Hirotake Abe,**[a] **Arata Endo,**[a] **Kohei Taniguchi**[a] **and Susumu Date**[a]

[a] *Cybermedia Center, Osaka University, Japan*

E-mail: thonglek.kundjanasith@ais.cmc.osaka-u.ac.jp

Due to the rapid development of edge devices and existing infrastructure in the post-5G era, a significant flood of large and diverse data is streaming into cloud infrastructure via services on edge devices. Consequently, many cloud infrastructure providers must develop methods for efficient resource allocation and scheduling to support service deployment with high availability and reliability. However, existing infrastructure providers often overlook efficient resource provisioning to preserve data privacy from edge device services. Typically, every service employs high-security mechanisms to preserve data privacy, but this comes at the cost of high resource usage. On the other hand, employing low-security mechanisms may pose a high risk of violating data privacy. Therefore, we propose the creation of an infrastructure focused on ensuring high availability and reliability of service deployment, coupled with effective security mechanisms tailored to each individual data-driven service, all while minimizing financial costs for service developers. We propose a resource integration to categorize the transferred data from edge devices to the cloud for each service into four protection levels based on privacy requirement. We analyze patterns of data transmission based on possible privacy-violation severities and transmission frequency to prevent over or under allocation of resources, ensuring high availability, reliability, and security.

International Symposium on Grids & Clouds 2024, ISGC2024
24th - 29th March, 2024
Academia Sinica, Taipei, Taiwan

*Speaker

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).

1. Introduction

Privacy is the most important concern in the contemporary digital landscape, where the proliferation of data-driven services has become ubiquitous. The impending shift to post-5G technology emphasizes the urgent need for robust infrastructures. These infrastructures should not only ensure service reliability and availability but also integrate security mechanisms to protect sensitive information. In our interconnected world, privacy goes beyond safeguarding personal details; it encompasses preserving autonomy, trust, and the fundamental right to control one's digital footprint. The rise of data-driven services intensifies the need for a proactive approach to privacy, especially with the imminent post-5G era bringing new connectivity possibilities. In navigating the digitized world, privacy emerges as a guiding principle, shaping the ethical dimensions of technological advancement. It is a commitment to upholding personal space in the digital landscape, where privacy forms the foundation for reliability, availability, and security.

Despite the extraordinary expansion of data-driven services, the current state of infrastructures finds itself entangled in the challenge of effectively balancing the triad of service reliability, availability, and comprehensive security measures. This multifaceted challenge becomes notably pronounced when delving into the meticulous oversight required for efficient resource provisioning, specifically geared towards the preservation of data privacy. The intricacies of this challenge are further heightened in the context of services emanating from edge devices, where the convergence of technological functionalities and the imperative to preserve sensitive information demands a nuanced and tailored approach. In essence, as data-driven services continue their meteoric rise, the existing infrastructural frameworks must grapple with the evolving landscape, navigating the delicate balance between ensuring uninterrupted service performance and fortifying defenses against potential security breaches, particularly concerning the concept of data privacy, especially in the landscape of services originating from edge devices.

Current practices predominantly involve the adoption of high-security mechanisms to protect data privacy, albeit at the cost of increased resource usage, exemplified by technologies like fully homomorphic encryption. On the other hand, the implementation of low-security mechanisms poses a substantial risk of compromising data privacy. As each data category requires a different protection level, the infrastructure provides different security mechanisms to efficiently preserve data privacy. In response to these dynamics, we advocate for the development of a dedicated infrastructure designed to ensure high availability and reliability in service deployment. This infrastructure will be complemented by effective security mechanisms tailored to the unique requirements of individual services, all while minimizing financial burdens on service developers.

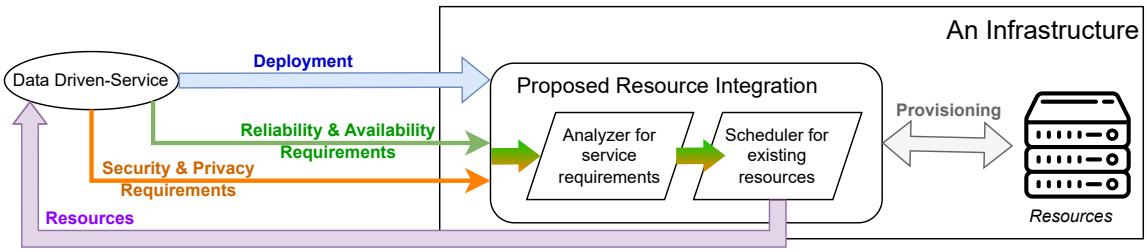

Figure 1: Overview of the proposed resource integration

In this paper, we propose a transformative approach through resource integration within infrastructure, aiming to extract and address the nuanced requirements of services, encompassing reliability, availability, security, and privacy considerations as shown in Fig. 1. The proposed resource integration comprises two primary modules. Resource integration is the process of combining and coordinating diverse computing resources such as edge devices, cloud servers, and on-premises systems—into a unified and cohesive system. Initially, the service requirements analyzer is employed to meticulously scrutinize the requisites of services, encompassing aspects of reliability, availability, security, and privacy in data transmission. Subsequently, based on the analysis, the resource integration proposes optimal approaches to uphold these requirements for each individual data-driven service, with a focus on minimizing financial costs for developers. In the second module, the existing resources are effectively allocated and scheduled for each data-driven service through the utilization of a dedicated scheduler.

The structure of this paper is as follows. Section 2 explains the existing techniques supporting the reliability and availability requirements of data-driven services. Section 3 describes the concept of classifying the data privacy levels based on the nature of the data. Section 4 provides insights into widely employed security mechanisms, accompanied by an analysis of the resource requirements for each method. In Section 5, we demonstrate the results of resource utilization analysis in supporting service requirements concerning reliability, availability, security, and privacy, while maintaining reasonable resource demands. Lastly, the paper concludes and outlines future work in Section 6.

2. Requirements for reliability and availability of services

Deploying data-driven services on infrastructure with integrated resources requires careful consideration of service reliability and availability, particularly when cloud servers and edge devices are involved. Reliability refers to the likelihood that a service will meet specified performance standards and produce accurate output within a given timeframe. Availability represents the percentage of time the service operates under normal conditions. When edge devices are part of the infrastructure, the challenge becomes even more significant due to their distributed nature and often limited computational resources. These devices, typically located close to the data source, are crucial for reducing latency and enabling real-time processing, but they also introduce potential points of failure that can impact overall service reliability and availability.

For example, consider the COVID-19 contact-tracing mobile application developed by Japan's Ministry of Health, Labour, and Welfare. With edge devices such as smartphones and wearables collecting and processing data locally, service reliability hinges on the ability of these devices to promptly send notifications to the designated target group within a specific timeframe, even when operating under varying conditions like intermittent connectivity or limited battery life. Similarly, service availability requires that both the application and the edge devices are operational 24/7. This ensures that the system can continuously receive data and promptly dispatch notifications, even if some devices temporarily go offline. The distributed nature of edge devices makes it essential to design the system with redundancy and fault tolerance, ensuring that service reliability and availability are maintained even in the face of device failures or network disruptions.

The importance of service reliability and availability in modern systems cannot be overstated. Numerous researchers have explored this crucial topic, developing diverse methodologies and frameworks to ensure consistent and dependable service delivery. In addressing reliability aspects, Avizienis et al. have designed fault-tolerant mechanisms, including redundancy measures such as data replication and server clustering, widely employed to mitigate the impact of failures and uphold service uptime [1]. Kolaczek et al. have advocated for predictive maintenance strategies, employing statistical analysis and anomaly detection to anticipate potential issues and enable proactive intervention, thereby preventing outages [2]. Shaoying et al. have proposed rigorous mathematical models and automated tools to verify the correctness and reliability of service implementations [3]. Thus, the proposed resource integration includes fault-tolerant design, predictive maintenance, and formal verification for supporting service reliability.

On the front of availability, Gray et al. have introduced an architecture for high-availability services using distributed systems with geographically dispersed components and automatic failover mechanisms, enhancing service availability even during localized disruptions [4]. Zheng et al. have explored dynamic resource allocation based on demand and service requirements to optimize utilization and prevent overload-induced outages [5]. Additionally, Gray et al. have delved into formal contracts between service providers and consumers, defining guaranteed levels of uptime and performance to incentivize providers in prioritizing service availability [6]. Hence, the proposed resource integration includes architecture design, resource allocation optimization, and serving service level agreements efficiently for supporting service availability. This comprehensive body of research reflects the ongoing dedication to advancing the understanding and implementation of reliable and available services, providing invaluable insights for the continual improvement of modern information systems.

While traditional approaches to service reliability and availability have proven effective, the rise of data-driven services presents unique challenges. Analyzing vast amounts of operational data to predict and prevent service disruptions or optimize resource allocation becomes increasingly complex. Enter machine learning (ML), a powerful tool capable of extracting insights from data and driving intelligent decisions. ML algorithms can be trained on historical service metrics, resource utilization patterns, and user behavior for:

1. Predicting Potential Failures: Campos et al. have devised accurate online failure predictors (OFP) tailored for modern complex systems. Their findings indicate that machine learning (ML)-based predictors can withstand variations without generating false alerts, maintaining predictive accuracy. This underscores the practical utility of OFP and suggests a need for further exploration in this area [7].

2. Optimizing Resource Allocation and Scheduling: Bu et al. approached the user scheduling problem in a massive multi-user multiple-input multiple-output system by modeling it as a Markov Decision Process. They characterized complex problems involving sequential decisions. Simulation results highlight the observable performance gains achieved through their proposed reinforcement learning-based scheduling and resource allocation scheme, outperforming other scheduling algorithms [8].

3. Exploring Self-Healing Mechanisms: Johnpill et al. conducted a comprehensive study on

existing vulnerabilities, threats, and challenges within cyber-physical systems. They critically analyzed current theories and methods utilizing machine learning for self-healing purposes, providing insights into the evolving landscape of self-healing mechanisms [9].

Incorporating machine learning into resource integration enhances service reliability and availability through proactive failure prediction and optimized resource allocation, effectively minimizing downtime and ensuring consistent service delivery. This integration contributes to operational efficiency by leveraging machine learning-driven resource management, which reduces costs by allocating resources based on real-time needs, thereby preventing unnecessary expenditures. Furthermore, the utilization of machine learning models fosters scalability and adaptability, as these models can continuously learn and adjust to evolving service requirements and user behavior, ensuring sustained service stability over the long term.

3. Data privacy classification

After understanding the challenges and existing approaches for integrating resources to achieve high reliability and availability in data-driven service deployment, the next crucial consideration is efficiently provisioning resources to secure data transmission across both edge and cloud environments. This is particularly important because these environments often involve the processing and transmission of sensitive data. Privacy becomes a critical concern, as data-driven services frequently handle various types of data, each with different levels of sensitivity.

For instance, edge devices might collect personal health information or location data, which must be carefully protected to prevent unauthorized access or breaches. When data is transmitted from these edge devices to the cloud for further processing, ensuring its security during transit is paramount. To address these concerns, it is essential to classify the privacy level associated with each data category within data-driven services. This classification helps in determining the appropriate security measures, such as encryption protocols and access controls, necessary to safeguard data at each stage of its lifecycle from collection on edge devices, through transmission, to storage and processing in the cloud. By prioritizing privacy, we can protect sensitive information, maintain user trust, and comply with regulatory requirements, all while enabling the efficient and secure operation of data-driven services.

Classifying the privacy level of each data category presents significant challenges within the field of information security, further compounded by its inherently subjective nature. The dynamism of data, constantly introducing new types and formats, makes it difficult to establish a static and all-encompassing classification framework. Moreover, the subjective interpretation of data sensitivity introduces variability among stakeholders, leading to potential inconsistencies in the classification process. Striking a balance between detailed categorization and operational practicality is an additional hurdle, as overly intricate schemes may hinder efficient implementation. The ever-changing regulatory landscape adds complexity, requiring continual adjustments to classification criteria to ensure compliance. In addition, the subjectivity of individual perspectives on data sensitivity poses a nuanced challenge, emphasizing the need for clear communication and collaboration among stakeholders to establish a unified understanding of privacy levels.

The privacy levels in our framework—high, moderate, low, and minimal—are designed to address varying degrees of data sensitivity and protection needs, drawing from established principles in standards like ISO/IEC 27001 and GDPR. Although ISO/IEC 27001 does not specify privacy levels, it emphasizes the importance of implementing security controls based on data sensitivity, aligning with our approach. GDPR, on the other hand, includes special protection for certain sensitive data categories, complementing our broader classification system. Our proposed privacy levels provide a flexible and adaptable framework tailored to resource integration needs, while also being compatible with evolving privacy standards and regulations. ISO/IEC 27001 is widely recognized and adopted globally, providing a framework that helps organizations address the challenges of securing sensitive information in an increasingly complex and interconnected digital environment [10]. Leveraging the principles of ISO/IEC 27001, we have structured data privacy into four distinct levels.

1. High privacy level
    (a) Government-issued identification numbers
    (b) Financial account information
    (c) Personal medical and health-related data
    (d) Biometric authentication data
    (e) Usernames or email addresses combined with passwords
    (f) Genetic data
2. Moderate privacy level
    (a) Security camera recordings
    (b) Body-worn video system recordings
    (c) Cameras recording cash handling
    (d) Building entry records
3. Low privacy level
    (a) Licensed software and software license keys
    (b) Library paid subscription electronic resources
4. Minimal privacy level
    (a) Published research
    (b) Press releases
    (c) Public event calendars

Assigning data to these categories enables the implementation of specific security mechanisms based on the level of protection required. This approach ensures that more sensitive data receives higher levels of security, while less sensitive information may be safeguarded with less resource-intensive measures. For a privacy policy to be developed, the data must be protected in data life cycle when it is created, stored, used, shared, archived, and destroyed [11].

4. Security mechanism identification

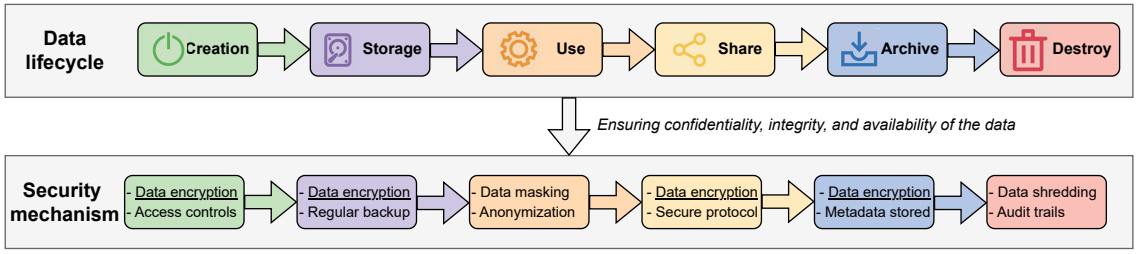

Figure 2: Security mechanisms for each phase within the data life cycle management

After the data privacy levels have been classified, the next critical step involves the introduction of security mechanisms tailored to each classification. This is particularly important in the context of edge and cloud computing, where data is frequently transmitted and processed across distributed environments. These environments are inherently vulnerable to security breaches during both communication and computation. Therefore, robust security measures are essential to protect sensitive information and maintain the integrity of data-driven services. Security protocols are strategically applied based on the classified privacy levels, with more rigorous measures for highly sensitive data and more resource-efficient solutions for less sensitive information. This approach ensures a comprehensive security framework that addresses the unique challenges and vulnerabilities of edge and cloud computing, fostering a secure and resilient environment for data-driven service deployment.

In Figure 2, the common security measures associated with each phase of the data lifecycle are detailed. During the creation phase, encryption techniques are employed to safeguard sensitive data from unauthorized access, and access controls are implemented to restrict data input to authorized personnel only. In the storage phase, data encryption at rest is applied to protect stored data from unauthorized access, while access controls regulate retrieval and modification. Regular backups are conducted to prevent data loss and facilitate recovery in case of a security incident. The use phase involves data masking or anonymization to minimize exposure of critical details. Secure file transfer protocols and encryption for communication are utilized during the sharing phase. In the archiving phase, data encryption is maintained for confidentiality, and metadata management ensures accurate retrieval and usage information. The destruction phase employs data shredding for physical media containing sensitive information and maintains audit trails to record and verify the destruction process for compliance and accountability.

Data encryption stands as an important mechanism within the security mechanism throughout the data lifecycle. It plays a pivotal role in preserving sensitive information from unauthorized access and potential security breaches. Encryption involves transforming data into a secure, unreadable format that can only be deciphered by individuals possessing the appropriate decryption key. The emphasis on the variation of data encryption for each data privacy level stems from the recognition that not all data possesses the same level of sensitivity. Tailoring encryption methods to specific privacy levels allows organizations to apply varying degrees of protection based on the inherent sensitivity of the data. This nuanced approach ensures that the security measures align with the

distinct requirements and potential risks associated with each classification, ultimately contributing to a more robust and adaptive security posture.

We categorize data encryption into two main approaches: symmetric and asymmetric encryption. These categories are based on the fundamental principles of how encryption keys are utilized to secure information. In symmetric encryption, the same key is used for both the encryption and decryption processes, providing an efficient and fast method for securing data. On the other hand, asymmetric encryption employs a pair of keys: a public key for encryption and a private key for decryption. This dual-key system enhances security by allowing secure communication between parties without the need to share the private key.

In practical applications, a frequently employed strategy is the integration of both symmetric and asymmetric encryption strengths in hybrid encryption systems [1]. This approach capitalizes on the efficiency of symmetric encryption for data transmission and leverages the secure key exchange capabilities of asymmetric encryption. It is important to note that, for the purpose of this paper, the focus is exclusively on examining symmetric and asymmetric encryption approaches individually, without delving into hybrid strategies.

#	Mechanism	Key Length	Block Size
1	AES	128, 192, 256 bits	128 bits
2	DES	56 bits	64 bits
3	Blowfish	32-448 bits	64 bits
4	Twofish	128-256 bits	128 bits
5	RC4	Variable	Stream
6	Camellia	128, 192, 256 bits	128 bits
7	Serpent	128-256 bits	128 bits
8	ChaCha20	Variable	Stream

Table 1: The key length and block size for widely used symmetric encryption mechanisms [12]

For asymmetric encryption, we surveyed five widely used mechanisms including Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie-Hellman (DH), Quantum Key Distribution (QKD), and Homomorphic Encryption (HE). Table 2 compares asymmetric encryption mechanisms in the aspect of key exchange, digital signature, key length, and quantum resistance. Key exchange refers to the capability of an algorithm to securely share cryptographic keys between communicating parties. Digital signature capability involves the algorithm's ability to generate and verify digital signatures, providing a means for authentication and integrity verification. Quantum resistance denotes the algorithm's resilience against potential threats posed by quantum computers, ensuring continued security in a (post)-quantum computing era.

Each asymmetric encryption algorithm brings unique features to the cryptographic landscape. RSA, a stalwart in the field, offers versatile applications with support for both key exchange and digital signatures, encompassing key lengths ranging from 1024 to 4096 bits. Elliptic Curve Cryptography (ECC) stands out for its efficiency, particularly in resource-constrained environments, utilizing shorter key lengths (160-521 bits) and exhibiting inherent resistance to quantum attacks.

[1] https://cryptography.io

#	Mechanism	Key Exchange	Digital Signatures	Key Lengths	Quantum Resistance
1	RSA	Yes	Yes	1024-4096 bits	No
2	ECC	Yes	Yes	160-521 bits	Yes
3	DH	Yes	No	-	No
4	QKD	Yes	No	Quantum	Yes
5	HE	No	Yes	-	No

Table 2: Comparison of asymmetric encryption mechanisms

Diffie-Hellman, a cornerstone of key exchange, lacks support for digital signatures and does not specify key lengths as they depend on the chosen parameters during the exchange process. Quantum Key Distribution (QKD) introduces a paradigm shift, leveraging principles of quantum mechanics for theoretically quantum-resistant key exchange. Homomorphic Encryption, while not designed for key exchange, excels in privacy-preserving computations by allowing operations on encrypted data, with added support for digital signatures. The selection among these algorithms hinges on the specific security requirements and constraints of the given cryptographic scenario.

5. Analysis of privacy and security requirements

An analysis of Privacy and Security Requirements is a critical process aimed at ensuring that both privacy and security considerations are addressed comprehensively within a system. This analysis is closely related to security mechanism identification, where appropriate security controls and techniques are identified to protect the system's assets, and data privacy classification, which involves categorizing data based on its sensitivity and privacy needs. Together, these aspects enable the design of robust mechanisms to safeguard sensitive data, ensure compliance with regulations, and mitigate potential security threats.

For designing the proposed resource integration, we analyze the severity level of data privacy align on resource requirement for each security mechanism. we assess the data privacy's severity level aligned with the resource requirements for each security mechanism. This study classifies data privacy levels into categories of high, moderate, low, and minimal privacy. The emphasis is on examining 12 security mechanisms, comprising eight instances of symmetric encryption and four instances of asymmetric encryption. Our preliminary research reveals a direct correlation between the security level of a mechanism and its resource consumption. Specifically, asymmetric data encryption consumes more resources to secure data compared to symmetric data encryption.

Due to the lower security requirements for low and minimal data privacy, we suggest the utilization of symmetric data encryption for these specific privacy levels. Following this recommendation, we organize symmetric data encryption algorithms based on their security profiles and resource consumption, arranging them from the least resource-intensive to the most resource-intensive.

Starting with the deprecated Data Encryption Standard (DES), characterized by a small key size and susceptibility to brute-force attacks, we progress to the deprecated Rivest Cipher (RC4), known for vulnerabilities, including biases in its output. Moving forward, we consider Blowfish, still secure but largely replaced by more modern ciphers, and ChaCha20, deemed secure and commonly integrated into contemporary encryption protocols such as transport layer security.

Continuing this sequence, we explore Twofish, designed as an advanced successor to Blowfish and considered secure, followed by Camellia, acknowledged for its security and recognized as an alternative to the widely adopted Advanced Encryption Standard (AES). In the case of AES, it stands out as highly secure, widely embraced, and recommended for general use. We conclude with Serpent, recognized for its robust security design and resilience against known practical cryptanalysis methods. This systematic arrangement provides insights into the security and resource consumption aspects of each symmetric data encryption algorithm.

Utilizing asymmetric encryption is a recommended approach for securing data with high and moderate privacy levels. In line with this recommendation, we categorize asymmetric data encryption algorithms based on their security profiles and resource consumption, organizing them from the least resource-intensive to the most resource-intensive. Among these algorithms, Rivest Shamir-Adleman (RSA) has long served as a fundamental element in public-key cryptography. However, its security hinges on the complexity of factoring large numbers, necessitating longer key lengths as computational power advances. Despite this, RSA remains widely employed, albeit with increased key sizes to maintain security.

Diffie-Hellman, as a key exchange algorithm, ensures security, yet its efficacy is contingent on key size. Optimal security is achieved with larger key sizes, and Diffie-Hellman is extensively used in various encryption protocols. Elliptic Curve Cryptography (ECC) is acknowledged for its robust security, offering shorter key lengths compared to traditional methods like RSA. Currently deemed secure, ECC finds widespread application, particularly in resource-constrained environments. Quantum Key Distribution (QKD) stands out as the most secure among the listed encryption methods. Leveraging principles rooted in quantum mechanics, QKD establishes a theoretically secure key exchange that remains impervious to potential quantum computing attacks. This feature positions QKD as an advanced and highly secure choice for safeguarding sensitive data.

Furthermore, homomorphic encryption is a unique encryption approach that allows computations on encrypted data. While powerful, it is computationally intensive and may not be as widely adopted for general-purpose encryption due to performance considerations. Its security relies on mathematical properties. It is important to note that the security landscape evolves, and the effectiveness of encryption algorithms can change over time. Regularly updating encryption practices and adopting the latest standards is crucial to maintaining a high level of security. Additionally, the specific security requirements of a given application or system may influence the choice of encryption algorithms.

6. Conclusion

Towards privacy and accessibility through resource integration, we have introduced guidelines to categorize data into four privacy levels: high, moderate, low, and minimal. Subsequently, our focus has been on a comprehensive analysis of widely utilized security mechanisms, particularly data encryption, to ensure secure data transmission in data-driven services. In our current endeavors, we emphasize 12 extensively used data encryption methods by eight of which are symmetric encryption, and four are asymmetric encryption. Recognizing the lower security requirements for low and minimal data privacy levels, we advocate the use of symmetric encryption for these cases. In contrast, due to heightened security needs for medium and high data privacy levels,

we recommend employing asymmetric encryption. We have provided an ordered assessment of the security and complexity of each data encryption method, empowering users to select based on their financial constraints or existing resources. Our proposed resource integration is poised to encompass additional security mechanisms and delve into more intricate classifications of data privacy levels. Following this expansion, we envisage deploying the proposed resource integration on public infrastructure, safeguarding data privacy while upholding the reliability and availability of data-driven services.

Building upon our current conclusions, we plan to advance our resource integration framework by focusing on several key areas. We will enhance our data privacy classification system, introducing more detailed categorization criteria to better address a wider range of privacy needs. This refinement will ensure that our framework accurately reflects varying levels of data sensitivity and supports more tailored security measures. Additionally, our future work will include a thorough evaluation of advanced security mechanisms beyond the current encryption methods. We aim to integrate novel encryption technologies and other security protocols that offer improved protection, particularly suited for the unique requirements of edge devices and cloud environments. This effort will involve an in-depth analysis of the evolving privacy and security requirements specific to these distributed systems. We will develop strategies to address challenges related to data management, transmission, and processing across edge devices and cloud resources, ensuring robust protection and optimal performance. Our objective is to deploy the enhanced resource integration framework on public infrastructure, where it will be rigorously tested to confirm its effectiveness in balancing data privacy with the reliability and availability of data-driven services. This deployment will validate our approach in real-world scenarios, contributing to a more secure and resilient data management environment.

Acknowledgement

This paper is based on results obtained from "Research and Development Project of the Enhanced Infrastructures for Post-5G Information and Communication Systems" (JPNP20017), commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

References

[1] A. Avizienis and J. Kelly, "Fault tolerance by design diversity: Concepts and experiments," *Computer*, vol. 17, pp. 67–80, aug 1984.

[2] G. Kolaczek and A. Prusiewicz, "Anomaly detection system based on service oriented architecture," in *Intelligent Information and Database Systems* (J.-S. Pan, S.-M. Chen, and N. T. Nguyen, eds.), (Berlin, Heidelberg), pp. 376–385, Springer Berlin Heidelberg, 2012.

[3] S. Liu, J. A. McDermid, and Y. Chen, "A rigorous method for inspection of model-based formal specifications," *IEEE Transactions on Reliability*, vol. 59, no. 4, pp. 667–684, 2010.

[4] J. Gray and D. Siewiorek, "High-availability computer systems," *Computer*, vol. 24, no. 9, pp. 39–48, 1991.

[5] X. Zheng and Y. Cai, "Dynamic virtual machine placement for cloud computing environments," in *2014 43rd International Conference on Parallel Processing Workshops*, pp. 121–128, 2014.

[6] S. Garg and A. Misra, "Service level agreements for cloud infrastructures," in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 276–279, 2019.

[7] J. R. Campos, E. Costa, and M. Vieira, "On the applicability of machine learning-based online failure prediction for modern complex systems," in *2022 18th European Dependable Computing Conference (EDCC)*, pp. 49–56, 2022.

[8] G. Bu and J. Jiang, "Reinforcement learning-based user scheduling and resource allocation for massive mu-mimo system," in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 641–646, 2019.

[9] O. Johnphill, A. S. Sadiq, F. Al-Obeidat, H. Al-Khateeb, M. A. Taheir, O. Kaiwartya, and M. Ali, "Self-healing in cyber and physical systems using machine learning: A critical analysis of theories and tools," *Future Internet*, vol. 15, no. 7, 2023.

[10] H. Guo, M. Wei, P. Huang, and E. G. Chekole, "Enhance enterprise security through implementing ISO/IEC 27001 standard," in *2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 1–6, 2021.

[11] M. J. Corby, "The case for privacy," *Information Systems Security*, vol. 11, no. 2, pp. 9–14, 2002.

[12] F. Olajide, K. Assa-Agyei, and C. Edo, "An empirical evaluation of encryption and decryption times on block cipher techniques," in *2023 Congress in Computer Science, Computer Engineering, amp; Applied Computing (CSCE)*, (Los Alamitos, CA, USA), pp. 2385–2390, IEEE Computer Society, jul 2023.