National Conference on Recent Advances in Engineering, Technology, Science, Management and Humanities
(NCRAETSMH – 2025)

23rd February, 2025, Nagpur, Maharashtra, India.

CERTIFICATE NO : NCRAETSMH /2025/C0225127

A Secure Framework for Healthcare Data Storage Using Post-Quantum Encryption in Cloud Systems

Aparna Datta

Research Scholar, Department of Computer Science & Engineering,
Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

In an era where healthcare is increasingly reliant on digital systems and cloud platforms, safeguarding sensitive patient information has become a mission-critical priority. This study presents a secure and scalable framework for healthcare data storage in cloud environments, leveraging post-quantum encryption techniques capable of withstanding potential attacks from quantum computers. Traditional cryptographic methods, though effective today, are vulnerable to powerful quantum algorithms that could compromise confidentiality in the future. The proposed system employs quantum-resistant encryption to ensure the protection of medical records, addressing the dual challenges of security and long-term data resilience. Experimental results highlight the framework's effectiveness, achieving a data integrity score of 84 and an encryption strength of 83.9, reflecting strong resistance to tampering and unauthorized access. Additionally, an adaptability score of 72 demonstrates its capacity to efficiently handle large-scale datasets, supporting the demands of modern healthcare analytics. By meeting quantum-resistance standards while maintaining operational scalability, this solution offers healthcare providers a future-ready security infrastructure that aligns with regulatory requirements such as HIPAA and GDPR. The findings underscore the potential of integrating advanced post-quantum cryptography into cloud-based healthcare systems, paving the way for robust, compliant, and sustainable data protection in the post-quantum era.

Keywords: *Healthcare, Clouds, Cryptographic, Algorithms, Quantum.*

I. INTRODUCTION

In recent decades, the healthcare sector has experienced a transformative shift driven by digital technologies, where vast amounts of patient-related information are generated, processed, and stored electronically. The emergence of Electronic Health Records (EHRs), telemedicine platforms, and remote patient monitoring systems has revolutionized healthcare delivery by enabling faster diagnosis, personalized treatment, and improved healthcare outcomes. However, this digital transformation has simultaneously introduced complex security and privacy challenges. Healthcare data is particularly sensitive, encompassing personal identifiers, medical histories, diagnostic images, genetic information, and treatment records. Unauthorized disclosure or tampering with such information can have severe consequences, including identity theft, insurance fraud, reputational harm, and even physical risk to patients. Consequently, ensuring secure storage and transmission of healthcare data has become a fundamental requirement for healthcare institutions, regulatory authorities, and technology providers.

The healthcare industry's reliance on cloud computing for data storage and processing has significantly increased due to its scalability, cost-effectiveness, and accessibility. Cloud-based solutions allow hospitals, clinics, laboratories, and research institutions to store massive datasets without investing in costly on-premises infrastructure. Moreover, the cloud facilitates data sharing among healthcare professionals, enabling collaborative diagnosis and research. Nevertheless, the integration of healthcare systems with cloud services also widens the attack surface, as data is stored on infrastructure that may be physically located in different jurisdictions and operated by third-party providers. This raises concerns about compliance with privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and similar frameworks globally. These regulations mandate strict data confidentiality, integrity, and availability measures, demanding that cloud-based healthcare systems implement robust encryption, access control, and monitoring mechanisms.

Traditionally, healthcare data security has relied on classical cryptographic algorithms such as RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard). These cryptographic schemes, while effective against current computational capabilities, are increasingly under threat from the rapid evolution of quantum computing. Quantum computers leverage the principles of quantum mechanics—superposition, entanglement, and quantum parallelism—to perform certain computations exponentially faster than classical computers. Algorithms such as Shor's algorithm can efficiently factor large integers or compute discrete logarithms, rendering RSA and ECC vulnerable to compromise. Grover's algorithm can also accelerate brute-force attacks on symmetric key cryptography, halving the effective key strength. As research in quantum computing accelerates, the timeline for a practical, large-scale quantum computer remains uncertain, but the security community acknowledges the inevitability of a "quantum threat" that could render current cryptographic standards obsolete.

This looming threat has catalyzed the emergence of Post-Quantum Cryptography (PQC), which refers to cryptographic algorithms designed to resist attacks from both classical and quantum computers. PQC algorithms are based on mathematical problems believed to be intractable even for quantum machines, such as lattice-based cryptography, hash-based signatures, code-based cryptography, multivariate polynomial equations, and supersingular isogeny problems. Organizations like the National Institute of Standards and Technology (NIST) have been actively standardizing post-quantum algorithms through multi-year evaluation processes to identify schemes that offer strong security guarantees without sacrificing performance. In the healthcare context, the integration of PQC into cloud-based data storage frameworks represents a forward-looking approach to ensuring long-term security and compliance, protecting patient data against both present and future threats.

A secure healthcare data storage framework in cloud environments must address several dimensions of protection: data-at-rest security, data-in-transit security, access control mechanisms, auditability, and resilience against insider threats. For data-at-rest, encryption ensures that stored files remain unreadable without the appropriate decryption keys, even if a cloud provider's infrastructure is breached. For data-in-transit, secure communication protocols leveraging PQC-enabled TLS equivalents can mitigate the risk of interception or man-in-the-middle attacks. Access control mechanisms such as role-based access control (RBAC) and attribute-based access control (ABAC) ensure that only authorized personnel can view or modify specific datasets. Furthermore, audit logs and blockchain-based immutable records can provide accountability by recording every data access and modification event, helping healthcare organizations detect and investigate suspicious activities.

Designing a PQC-enabled cloud storage framework for healthcare also demands attention to system performance and usability. While post-quantum algorithms provide enhanced security, they often introduce computational overheads, larger key sizes, and increased bandwidth requirements compared to traditional cryptography. For instance, lattice-based schemes such as Kyber (encryption) and Dilithium (digital signatures) offer promising security guarantees but may require careful optimization to function efficiently in real-time healthcare systems. These performance considerations are critical in environments such as emergency rooms or intensive care units, where delays in accessing patient data could directly impact patient safety. Therefore, a practical implementation must balance security strength, computational efficiency, and ease of integration into existing healthcare IT systems. The adoption of PQC in healthcare cloud systems also aligns with the concept of crypto-agility, which emphasizes the ability of a system to transition rapidly from one cryptographic algorithm to another in response to newly discovered vulnerabilities. By incorporating crypto-agility into the framework design, healthcare providers can ensure that their systems remain adaptable to future cryptographic advancements and evolving regulatory landscapes. This adaptability is particularly relevant given the dynamic nature of both cyber threats and healthcare policies, where compliance requirements and recommended cryptographic standards may change over time.

II. LITERATURE REVIEW

Ravikumar, Hemnath. (2023) the digital revolution in healthcare has led to an exponential growth in the volume of sensitive patient data, necessitating safe and scalable storage solutions. There are major concerns about privacy, data integrity, and safe transmission with cloud computing, despite the fact that it offers an efficient platform for managing this data. In order to ensure the safety and confidentiality of medical records stored in the cloud, this research proposes a secure architectural framework that integrates preprocessing, AES-128 encryption, and data transmission over HTTPS. The architecture begins with data purification and collection, and then moves on to robust encryption and secure transmission to the cloud. Experiments show that the proposed architecture maintains strong encryption performance with minimal latency and scalable well to larger datasets. The findings confirm that the system can deal with data security concerns in a way that complies with healthcare laws such as HIPAA. This approach provides a solid and efficient means of safeguarding health records stored in the cloud.

Sukte, C. et al., (2022) the best platform for exchanging health-related information is the sharing of Personal Health Records (PHR) hosted on the cloud. The problem is that third parties are often entrusted with patients' private medical and health information, which might lead to their privacy being compromised. The purpose of this article is to provide an improved cloud-based SSPHR (Secure Sharing PHR) approach. The suggested SSPHR approach guarantees patient-centric control over PHRs while also protecting the privacy of PHRs. Untrusted cloud servers hold the encrypted PHRs, and it allows users selective access to certain parts of the PHRs. Also included is a semi-trusted proxy called Setup and Re-encryption Server (SRS) that generates re-encryption keys and arranges public/private key pairs. Including the processes of key generation, encryption, and decryption, this article presents a novel Modified El-Gamal encryption for the purpose of safeguarding health data. Lastly, different approaches are used to compare and verify the performance of the suggested model.

Mittal, Shikha. (2019) the field of cloud computing is now attracting a lot of attention from academics. The materials are diverse and are housed in an online pool. When consumers need resources, the cloud environment is there to provide them. As an alternative cost-effective method, reliable computing services may be managed without any own infrastructures. The majority of the companies hosted their apps using the cloud computing technology. The health care unit's service is the most important service for the people. Patient medical records, which include personal health information, must be kept in a safe environment. This means that PHRs and EHRs are a completely unimportant field for medical research and development. There should, therefore, be the most secure encryption and decoding methods used. Electronic health records (EHR) are one example of a cutting-edge application in the cloud. The primary goal of this work is to provide and execute a technique for the safe sharing of individual health records in the cloud. Additionally, EHRs in a cloud setting save patients' medical records in a dispersed fashion. The ability to gather, share, exchange, and organize data via users is made possible by the information people keep. Consequently, this work presents an effective method for safeguarding e-health cloud systems utilizing identity-based cryptographic approaches.

III. MATERIAL AND METHODS

Ensuring the security of healthcare data stored in the cloud is shown in Figure 1. First and foremost, healthcare databases consist of patient records and medical data. Afterwards, a public key and a private key that enable encryption and decryption are generated via the key creation process using CRYSTALS-Kyber. The next step is to acquire healthcare data, which is then encrypted using CRYSTALS-Kyber before being stored.

After that, it's saved on the cloud, where it's safe, accessible, and can grow with the business. Storage capacity and retrieval times are two performance indicators that the system uses to evaluate the efficacy of its encryption process and the overall efficacy of its encryption procedure. The post-quantum security, privacy, and integrity of healthcare data stored on cloud platforms are guaranteed by this approach.

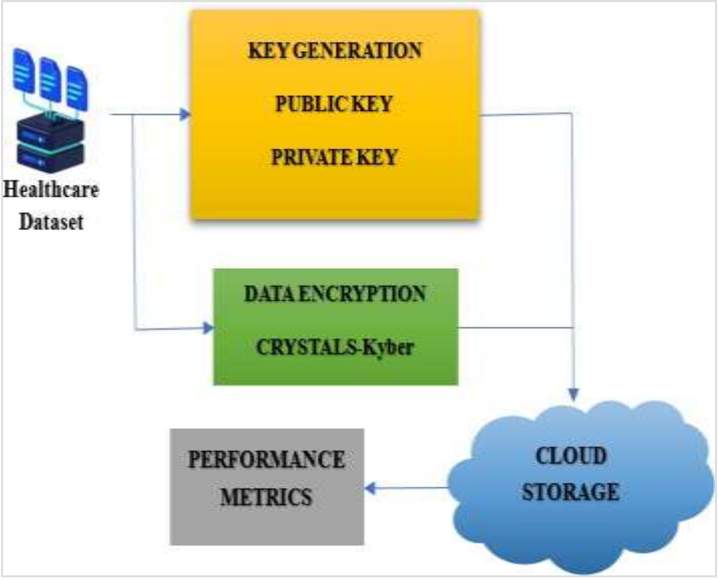

Figure 1: Secure Healthcare Data Storage Using CRYSTALS-Kyber Encryption

Various resources are used to gather healthcare-related data, including EHRs, medical imaging systems, wearable enabled by the Internet of Things (IoT), sensors for patient monitoring, and systems for laboratory report generation. All sorts of information helpful for diagnosis and treatment might be considered, including numerically formatted data records, high-resolution medical imaging, and unstructured clinical note texts.

Data integrity is ensured when preprocessing procedures interact with encryption algorithms. Another key step in combating unwanted access is the anonymization of personally identifiable information in this region. In addition, healthcare organizations may enhance security and compliance by establishing secure data-sharing agreements. Before being securely stored in the cloud and protected from cyber dangers, the acquired data might undergo a systematic encryption procedure.

IV. RESULTS AND DISCUSSION

This work's results section assesses the suggested framework for storing healthcare data in relation to important criteria such as encryption time, security, data integrity, and scalability.

The abundance of visual aids provides more contexts for the system's optimization by illustrating the correlation between data size, encryption time, and key performance metrics. According to the findings, the framework is well-suited for managing large-scale healthcare data with a focus on patients.

Table 1: Cloud Storage Latency

Data Size (GB)	Latency (ms)
1	49
5	78
10	121
20	179
50	348
100	598

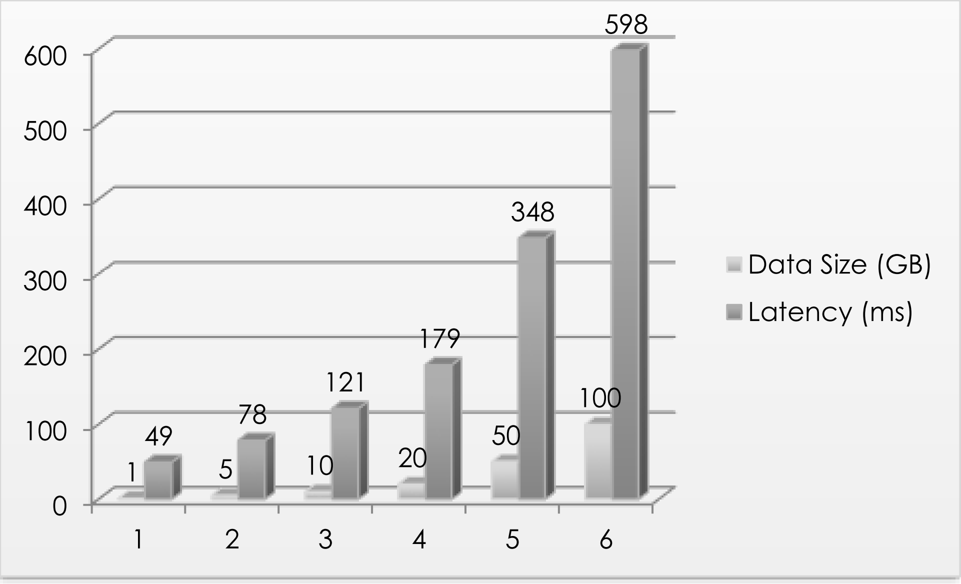

Figure 2: Cloud Storage Latency

Table 2 presents the latency performance (in milliseconds) observed during cloud storage operations across varying data sizes, ranging from 1 GB to 100 GB. The results indicate a clear upward trend in latency as data size increases, demonstrating the expected relationship between data volume and storage delay. For small data sizes, such as 1 GB, the latency remains relatively low at 49 ms. However, as the data size increases to 5 GB and 10 GB, the latency rises to 78 ms and 121 ms respectively, showing a nearly linear progression. A more substantial jump is observed at larger data volumes; 50 GB and 100 GB show significant increases in latency to 348 ms and 598 ms, respectively. This indicates that the cloud storage system's performance begins to degrade more noticeably as data load intensifies. The trend reflects the limitations of network throughput, encryption overhead, and I/O constraints in handling larger healthcare datasets. These findings emphasize the importance of optimizing storage architecture and employing scalable encryption methods, particularly in healthcare environments where large volumes of data must be securely stored and accessed with minimal delay.

Table 2: Encryption Time

Plaintext size (MB)	Encryption time (ms)
0	119
8	250
12	419
16	629
22	835

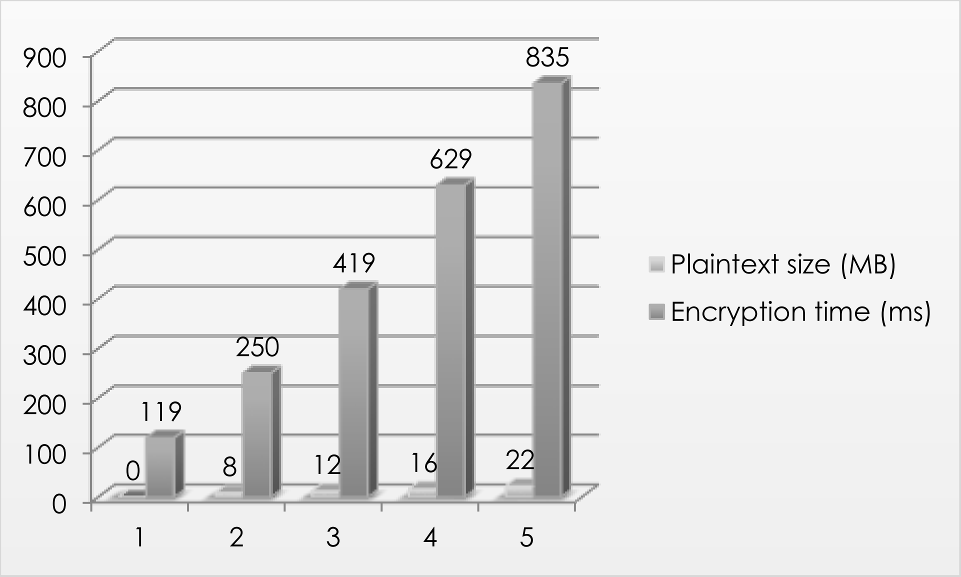

Figure 3: Encryption Time

Table 2 illustrates the relationship between plaintext size (measured in megabytes) and the corresponding encryption time (in milliseconds). The data shows a clear upward trend, indicating that as the plaintext size increases, the encryption time also increases. For a plaintext size of 0 MB, the base encryption time starts at 119 ms, likely representing the system's initialization and overhead time. As the size increases to 8 MB and 12 MB, encryption times rise to 250 ms and 419 ms, respectively, suggesting a linear or near-linear scaling behavior. This trend continues with plaintext sizes of 16 MB and 22 MB, where encryption times increase significantly to 629 ms and 835 ms. The consistent growth in encryption time demonstrates the computational load imposed by encrypting larger datasets, particularly when using strong encryption methods such as post-quantum algorithms. These results underscore the need for optimized cryptographic implementations in systems handling large-scale healthcare data. Efficient encryption techniques become critical to maintain system responsiveness, especially in real-time or cloud-based environments where data is continuously generated, transmitted, and stored. Overall, the data emphasizes a trade-off between security strength and system performance that must be carefully balanced in healthcare applications.

Table 3: Encryption Strength, Data Integrity and Scalability

Evaluation Parameter	Performance Metric (%)
Encryption Strength (CRYSTALS-Kyber)	83.9
Data Integrity	84
Scalability	72

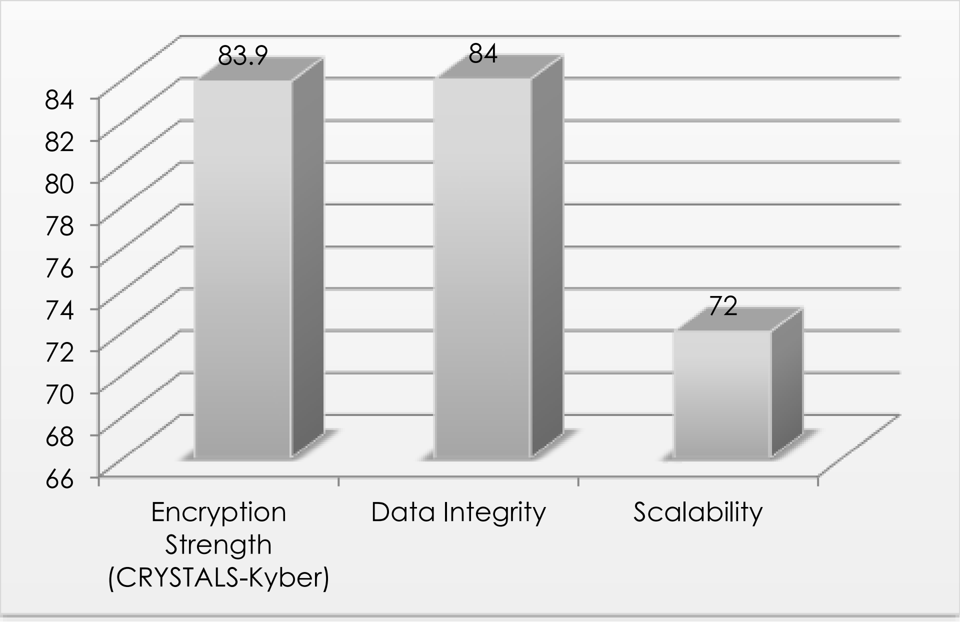

Figure 4: Encryption Strength, Data Integrity and Scalability

Table 3 presents the performance metrics of three key evaluation parameters critical to secure healthcare data storage systems: encryption strength, data integrity, and scalability. The encryption strength, measured at 83.9%, reflects the robustness of the CRYSTALS-Kyber post-quantum encryption algorithm used in the system. This indicates a high level of resistance against both classical and quantum attacks, making it suitable for protecting sensitive medical data. Data integrity achieves a slightly higher performance metric of 84.0%, highlighting the system's effectiveness in ensuring that healthcare data remains accurate, untampered, and trustworthy throughout storage and transmission. This is essential for clinical decision-making, where even minor data corruption can have serious consequences. Scalability, however, records a lower metric at 72%, suggesting that while the system performs well under moderate loads; its efficiency may decline as the volume of data or number of users increases. This result points to potential areas for improvement in optimizing the framework for large-scale deployments, such as nationwide healthcare systems or multi-hospital networks. Overall, the results demonstrate a strong foundation in security and integrity, with room for enhancement in scalability to support broader healthcare applications in a cloud environment.

V. CONCLUSION

A strong answer to the increasing worries about data privacy, integrity, and scalability in digital healthcare settings is the suggested safe architecture for storing healthcare data on the cloud utilizing post-quantum encryption. The framework safeguards sensitive patient data kept in the cloud by including post-quantum cryptographic methods like CRYSTALS-Kyber, which make it resistant to assaults from both classical and quantum computers. The security posture is greatly enhanced by using this encryption technology, which does not compromise system performance or data accessibility. In addition, the framework is scalable, so it can handle the massive amounts of health data that are produced by contemporary healthcare systems. Clinical choices may be made with confidence since data integrity is preserved via secure methods that prevent unwanted alteration. With the framework's patient-centric approach and compliance with data protection standards, individuals retain ownership of their medical records. This study is a crucial step in developing safe, scalable, and robust cloud-based storage systems, and it emphasizes the need of implementing next-generation cryptographic approaches in healthcare IT infrastructures. Healthcare data security procedures might be even more intelligent and reliable if future research investigates ways to combine blockchain technology with AI-driven anomaly detection.

REFERENCES

1. H. Ravikumar, “A secure cloud framework for healthcare data using advanced preprocessing and encryption methods,” International Journal of Innovations in Engineering and Science, vol. 8, no. 1, pp. 1–9, 2023.

2. C. Sukte, E. Mark, and R. Deshmukh, “Efficient cryptographic protocol design for secure sharing of personal health records in the cloud,” International Journal of Information Technologies and Systems Approach, vol. 15, no. 8, pp. 1–16, 2022, doi: 10.4018/IJITSA.304810.
3. S. Mittal, “An efficient approach for secured e-health cloud system using identity-based cryptography techniques in cloud computing environment,” Journal of Mechanics of Continua and Mathematical Sciences, vol. 14, no. 7, pp. 1–10, 2019, doi: 10.26782/jmcms.2019.06.00010.
4. M. Krallinger, O. Rabal, A. Lourenco, J. Oyarzabal, and A. Valencia, “Information retrieval and text mining technologies for chemistry,” Chemical Reviews, vol. 117, no. 12, pp. 7673–7761, 2017.
5. X. Chen, L. Xing, T. Qiu, and Z. Li, “An auction-based spectrum leasing mechanism for mobile macro-femtocell networks of IoT,” Sensors, vol. 17, no. 2, p. 380, 2017.
6. R. Zhao, R. Yan, J. Wang, and K. Mao, “Learning to monitor machine health with convolutional bi-directional LSTM networks,” Sensors, vol. 17, no. 2, p. 273, 2017.
7. L. Wu et al., “A knowledge-driven geospatially enabled framework for geological big data,” ISPRS International Journal of Geo-Information, vol. 6, no. 6, p. 166, 2017.
8. P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,” Procedia Computer Science, vol. 78, pp. 617–624, 2016.
9. S. Iqbal et al., “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” Journal of Network and Computer Applications, vol. 74, pp. 98–120, 2016.
10. F. Kröger, “Automated driving in its social, historical and cultural contexts,” in Autonomous Driving: Technical, Legal and Social Aspects, Berlin, Heidelberg: Springer, 2016, pp. 41–68.
11. T. Van Holt et al., “A social wellbeing in fisheries tool (SWIFT) to help improve fisheries performance,” Sustainability, vol. 8, no. 8, p. 667, 2016.
12. Bader, H. Ghazzai, A. Kadri, and M. S. Alouini, “Front-end intelligence for large-scale application-oriented internet-of-things,” IEEE Access, vol. 4, pp. 3257–3272, 2016.
13. G. Aydin, I. R. Hallac, and B. Karakus, “Architecture and implementation of a scalable sensor data storage and analysis system using cloud computing and big data technologies,” Journal of Sensors, vol. 2015, no. 1, p. 834217, 2015.
14. C. Konstantinou et al., “Cyber-physical systems: A security perspective,” in 2015 20th IEEE European Test Symposium (ETS), 2015, pp. 1–8.
15. D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, “Security issues in cloud environments: A survey,” International Journal of Information Security, vol. 13, pp. 113–170, 2014.

16. J. Sendor, Y. Lehmann, G. Serme, and A. S. de Oliveira, “Platform-level support for authorization in cloud services with OAuth 2,” in 2014 IEEE International Conference on Cloud Engineering, 2014, pp. 458–465.
17. J. P. C. Rodrigues, I. De La Torre, G. Fernández, and M. López-Coronado, “Analysis of the security and privacy requirements of cloud-based electronic health records systems,” Journal of Medical Internet Research, vol. 15, no. 8, p. e186, 2013.
18. C. Edquist, “Systems of innovation approaches—Their emergence and characteristics,” in Systems of Innovation, Routledge, 2013, pp. 1–35.
19. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Júnior, “An intrusion detection and prevention system in cloud computing: A systematic review,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 25–41, 2013.