INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

A COMPREHENSIVE APPROACH TO SECURE PERSONAL HEALTH RECORD SHARING IN CLOUD ENVIRONMENTS

Man, hon Liu

Department of Computing, The Hong Kong Polytechnic University, Hong Kong

Abstract: The rapid advancement of cloud computing technology has revolutionized the healthcare industry, offering unprecedented opportunities for the storage, sharing, and management of personal health records (PHRs). However, the transition to cloud-based systems also introduces significant security and privacy challenges, particularly concerning the sensitive nature of health data. This paper presents a comprehensive approach to secure sharing of PHRs in cloud environments, addressing the multifaceted issues of data confidentiality, integrity, and access control.

Our framework integrates advanced cryptographic techniques, robust access control mechanisms, and efficient data management strategies to ensure the secure handling of PHRs. The primary components of the framework include a hybrid encryption scheme, role-based access control (RBAC), and secure data storage protocols. The hybrid encryption scheme leverages the strengths of both symmetric and asymmetric encryption to protect data at rest and in transit, ensuring that only authorized users can access and modify the records. The RBAC model enforces stringent access policies based on user roles and responsibilities, preventing unauthorized access and ensuring that users can only perform actions pertinent to their roles.

To enhance data integrity and auditability, our framework incorporates blockchain technology to create an immutable ledger of all access and modification activities. This ensures transparency and accountability, allowing patients and healthcare providers to trace any changes made to the records. Additionally, we implement secure key management practices to safeguard encryption keys, including periodic key rotation and secure key distribution methods.

Our approach also addresses the usability and scalability aspects of secure PHR sharing. We propose a user-friendly interface that simplifies the management of access permissions, enabling patients to easily share their records with healthcare providers, family members, or researchers without compromising security. The framework is designed to be scalable, accommodating the growing volume of health data and the increasing number of users in a cloud environment.

To evaluate the effectiveness of our proposed framework, we conducted extensive simulations and performance analyses. The results demonstrate that our approach provides a high level of security

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

without significantly impacting system performance. The hybrid encryption scheme ensures robust protection against unauthorized access, while the RBAC model effectively manages access rights and minimizes the risk of data breaches. The integration of blockchain technology enhances data integrity and accountability, providing a transparent and tamper-proof record of all activities.

In conclusion, this paper presents a comprehensive and effective framework for secure sharing of personal health records in cloud environments. By combining advanced cryptographic techniques, robust access control mechanisms, and innovative data management strategies, our approach addresses the critical security and privacy challenges associated with cloud-based PHR systems.

This framework not only ensures the confidentiality, integrity, and availability of health data but also enhances patient trust and promotes the widespread adoption of cloud technology in the healthcare sector. Future work will focus on further optimizing the framework's performance and exploring additional features such as machine learning-based anomaly detection to enhance security measures.

Our comprehensive approach demonstrates the potential of integrating cutting-edge technologies to create a secure, efficient, and user-friendly environment for managing personal health records in the cloud. By addressing the inherent security challenges and providing a robust solution, this framework paves the way for a more secure and efficient healthcare system, ultimately improving patient outcomes and fostering innovation in the healthcare industry.

Keywords: Secure sharing, personal health records, cloud systems, data privacy, healthcare data, encryption, access control, cloud security, data integrity, patient confidentiality, cloud computing, healthcare IT, secure data storage, data sharing protocols, healthcare information security.

INTRODUCTION

The advent of cloud computing has revolutionized the way data is stored, accessed, and managed, offering unparalleled convenience and efficiency. In the healthcare sector, this technological advancement has opened new avenues for the management and sharing of Personal Health Records (PHRs). PHRs are critical documents that contain comprehensive health information about individuals, ranging from medical history, diagnoses, medications, immunization dates, allergies, and test results to demographic information. The shift towards digitizing these records and storing them in the cloud promises significant benefits, including improved accessibility, enhanced patient care, and streamlined administrative processes. However, this transition also introduces substantial challenges, particularly in the realm of data security and privacy.

One of the primary concerns with cloud-based PHR systems is ensuring the confidentiality, integrity, and availability of sensitive health information. Given the sensitive nature of PHRs, any breach can have severe consequences, including identity theft, financial loss, and erosion of trust in the healthcare system. Thus, developing a robust framework for securely sharing PHRs in the cloud is paramount. This framework must

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

address various threats, including unauthorized access, data breaches, and malicious attacks, while also complying with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA).

Moreover, the unique characteristics of cloud computing, such as multi-tenancy, elasticity, and resource sharing, add layers of complexity to the security paradigm. Multi-tenancy, where multiple users share the same physical infrastructure, raises concerns about data isolation and cross-tenant attacks. Elasticity, which allows resources to scale up or down dynamically, necessitates continuous monitoring and adaptation of security measures. Resource sharing, a core feature of cloud computing, demands stringent controls to prevent data leakage and ensure proper access control.

These factors necessitate a comprehensive and dynamic approach to securing PHRs in the cloud.

To address these challenges, a comprehensive approach must incorporate several key elements: strong encryption mechanisms, robust access control policies, secure data sharing protocols, and continuous monitoring and auditing. Encryption ensures that data remains unreadable to unauthorized users, both during transmission and while at rest. Access control policies, including role-based and attribute-based access control, ensure that only authorized individuals can access specific parts of the PHR. Secure data sharing protocols, such as secure multi-party computation and homomorphic encryption, enable data to be shared and processed without exposing it to unauthorized parties. Continuous monitoring and auditing help detect and respond to security incidents in real-time, ensuring that any breaches are swiftly addressed.

Another critical aspect of a secure PHR sharing framework is user-centric design. Patients must have control over their health data, including the ability to grant and revoke access permissions. This empowerment not only enhances data security but also fosters trust and engagement in the digital health ecosystem. User-friendly interfaces and clear communication about privacy policies and data usage are essential to ensure that patients can make informed decisions about their health information.

Furthermore, collaboration between stakeholders, including healthcare providers, cloud service providers, policymakers, and patients, is crucial to developing and implementing effective security measures. Healthcare providers must ensure that their data practices comply with regulatory requirements and best practices. Cloud service providers must offer secure infrastructure and services that support the specific needs of PHR systems. Policymakers must establish clear guidelines and regulations to protect patient data while promoting innovation and efficiency in healthcare. Patients, as the ultimate owners of their health data, must be educated and engaged in the security processes.

METHOD

To establish a comprehensive framework for the secure sharing of personal health records (PHRs) in cloud environments, we employed a multi-faceted methodology encompassing system architecture design,

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

encryption techniques, access control mechanisms, and user authentication protocols. This section details the methodologies used in each of these critical areas to ensure data security, privacy, and accessibility.

System Architecture Design

The foundation of our framework is a robust system architecture designed to handle PHRs securely in a cloud environment. We utilized a hybrid cloud model that combines the benefits of both private and public clouds. Sensitive PHR data is stored on a private cloud to ensure maximum security and compliance with healthcare regulations such as HIPAA, while less sensitive data and applications run on a public cloud to leverage scalability and cost-efficiency. This hybrid model ensures that critical health information remains protected while still benefiting from the cloud's flexibility.

Encryption Techniques

Encryption is a cornerstone of our security strategy. We implemented advanced encryption standards (AES-256) to encrypt PHR data both at rest and in transit. For data at rest, we utilized server-side encryption with customer-managed keys to provide an additional layer of control and security. For data in transit, we employed transport layer security (TLS) to protect data during transmission between users and the cloud servers. This dual approach ensures that PHR data is protected from unauthorized access and potential breaches at all stages.

Access Control Mechanisms

Access control is crucial to prevent unauthorized users from accessing sensitive health data. We adopted a role-based access control (RBAC) system, which assigns permissions to users based on their roles within the healthcare system. Healthcare providers, patients, and administrative staff each have different access levels, ensuring that users can only access the information necessary for their role. Additionally, we incorporated attribute-based access control (ABAC) for more granular control, considering user attributes such as job function, location, and time of access. This dual- layer access control mechanism enhances security and operational efficiency.

User Authentication Protocols

To further secure PHR access, we implemented strong user authentication protocols. Multi-factor authentication (MFA) was mandated for all users, requiring at least two forms of verification—such as a password and a mobile authentication app. This reduces the risk of unauthorized access even if one authentication factor is compromised. Additionally, we integrated biometric authentication methods, including fingerprint and facial recognition, to provide a seamless and highly secure login experience. These protocols ensure that only authorized users can access PHRs, significantly reducing the potential for data breaches.

Data Integrity and Auditing

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

Ensuring the integrity of PHR data is vital for maintaining trust and reliability. We employed cryptographic hash functions to create unique digital fingerprints for PHR data, allowing us to detect any unauthorized modifications. Regular integrity checks are performed, and any discrepancies trigger alerts for immediate investigation. Furthermore, we implemented comprehensive auditing mechanisms to log all access and modification activities. These logs are stored securely and analyzed regularly to identify and respond to suspicious activities, ensuring continuous monitoring and protection of PHR data.

Compliance and Regulatory Adherence

Compliance with healthcare regulations is a critical aspect of our methodology. Our framework is designed to comply with key regulations such as HIPAA in the United States and GDPR in Europe. We conducted thorough risk assessments and implemented necessary safeguards to meet these regulatory requirements. Regular compliance audits are performed to ensure ongoing adherence, and any identified gaps are addressed promptly. This proactive approach to compliance helps protect patient privacy and avoid legal and financial penalties.

User Education and Training

Recognizing that security is not solely a technological challenge, we implemented a comprehensive user education and training program. Healthcare providers and administrative staff receive regular training on best practices for data security, including recognizing phishing attempts and using secure communication channels. Patients are also educated on how to protect their personal information and understand their rights regarding PHR access and sharing. This focus on user education helps create a culture of security awareness and reduces the risk of human error compromising PHR data.

Continuous Improvement and Future Research

Security is an evolving field, and our methodology includes a commitment to continuous improvement. We regularly review and update our security protocols in response to emerging threats and technological advancements. Additionally, we engage in ongoing research to explore new security technologies and methodologies that could enhance our framework. This commitment to continuous improvement ensures that our PHR sharing framework remains robust and resilient in the face of evolving challenges.

RESULT

Our research focused on developing a comprehensive framework for secure sharing of personal health records (PHRs) in cloud environments, addressing key challenges such as data privacy, access control, and system efficiency. The results of our study demonstrate the viability and effectiveness of the proposed framework through a series of experimental evaluations and security analyses.

Firstly, the framework employs a robust encryption scheme to ensure data confidentiality. By utilizing attribute-based encryption (ABE), we achieved fine-grained access control, allowing patients to specify

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

who can access their PHRs based on user attributes. The implementation of ABE not only protects sensitive health information from unauthorized access but also provides flexibility in managing access rights. Our experiments show that the encryption and decryption processes in ABE are computationally efficient, making it feasible for real-time applications in cloud environments.

Secondly, the framework integrates a secure key management system that simplifies the distribution and revocation of keys. This system leverages a hybrid approach combining symmetric and asymmetric encryption, ensuring that keys are securely shared and managed without compromising system performance. Our results indicate that this key management system significantly reduces the risk of key leakage and unauthorized access, enhancing the overall security of PHR sharing.

Another critical component of our framework is the incorporation of blockchain technology to ensure data integrity and transparency. By recording all access and modification activities on a tamper-proof blockchain ledger, we provide an immutable audit trail that can be used to verify the authenticity and integrity of PHRs. Our performance evaluation of the blockchain component reveals that it introduces minimal overhead, making it a practical addition to the cloud-based PHR sharing system. The blockchain ledger also enhances trust among stakeholders by providing a transparent and verifiable record of all transactions.

Furthermore, our framework includes a privacy-preserving access control mechanism that leverages secure multi-party computation (SMPC). This mechanism allows multiple parties to collaboratively process PHRs without revealing their individual inputs, thereby preserving patient privacy. Our experimental results demonstrate that SMPC-based access control is effective in protecting sensitive information while enabling collaborative data analysis. The computational overhead introduced by SMPC is manageable, ensuring that the system remains responsive and efficient.

To evaluate the practical applicability of our framework, we conducted a case study involving a healthcare provider and several patients. The case study demonstrated that our framework could be seamlessly integrated into existing healthcare systems, providing secure and efficient PHR sharing. Patients reported high satisfaction with the ease of managing their access rights, while healthcare providers appreciated the enhanced security and transparency. The case study also highlighted the scalability of our framework, as it successfully handled a large number of access requests and data transactions without significant performance degradation.

In terms of system performance, our framework showed promising results in various metrics, including encryption/decryption time, key distribution latency, blockchain transaction throughput, and overall system response time. The encryption and decryption times were within acceptable limits, ensuring that the framework could handle real-time data access scenarios. Key distribution latency was minimal, thanks to the efficient key management system. The blockchain component maintained a high transaction

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

throughput, supporting the scalability of the system. Overall, the framework demonstrated a low system response time, indicating its suitability for practical deployment in cloud-based PHR sharing applications.

Lastly, the security analysis of our framework confirms its resilience against various threats, including unauthorized access, data breaches, and insider attacks. The combination of ABE, secure key management, blockchain, and SMPC provides multiple layers of security, making it difficult for attackers to compromise the system. Additionally, the framework's design ensures that any attempt to tamper with PHRs or access them without proper authorization is quickly detected and mitigated.

DISCUSSION

The advent of cloud computing has revolutionized the way personal health records (PHRs) are managed, shared, and stored. With the promise of high availability, scalability, and cost efficiency, cloud environments provide an ideal platform for the storage and sharing of PHRs. However, the sensitivity and confidentiality of health information necessitate robust security measures to protect against unauthorized access, data breaches, and privacy violations. This discussion explores the key components and challenges of a comprehensive approach to secure personal health record sharing in cloud environments, emphasizing the integration of advanced encryption techniques, access control mechanisms, and data integrity measures.

Encryption Techniques

Encryption is a cornerstone of secure data sharing in the cloud. It ensures that PHRs are unreadable to unauthorized users, both during transmission and while stored in the cloud. Traditional encryption methods like symmetric and asymmetric encryption are widely used, but their application in PHRs must consider the specific requirements of health data. Symmetric encryption, while efficient, necessitates secure key management, as the same key is used for both encryption and decryption. In contrast, asymmetric encryption, which uses a pair of public and private keys, offers enhanced security but at the cost of computational overhead.

Advanced encryption techniques such as homomorphic encryption and attribute-based encryption (ABE) are particularly promising for PHRs. Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, preserving privacy while enabling data processing. ABE, on the other hand, enables fine-grained access control by associating encrypted data with access policies and attributes. This means that only users whose attributes match the specified policy can decrypt the data. These techniques provide a balance between security and usability, essential for the effective sharing of PHRs in cloud environments.

Access Control Mechanisms

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

Access control is crucial for ensuring that only authorized individuals can access sensitive health information. Role-based access control (RBAC) is a widely adopted method, where access rights are assigned based on the roles of users within an organization. However, the dynamic nature of PHR sharing requires more flexible and context-aware access control mechanisms. Attribute-based access control (ABAC) is an effective solution, as it grants access based on attributes such as the user's identity, the resource being accessed, and the context of the request.

Moreover, patient-centric access control models empower patients to manage their own health records by specifying who can access their data and under what conditions. These models typically involve user-friendly interfaces that allow patients to set permissions easily. Combining patient- centric models with ABAC can create a robust and flexible access control system, enhancing both security and user autonomy.

Data Integrity Measures

Ensuring the integrity of PHRs is vital to maintaining trust in cloud-based health systems. Data integrity involves protecting data from unauthorized alterations, ensuring that health records remain accurate and reliable. Techniques such as digital signatures and hash functions are commonly used to verify data integrity. Digital signatures, which use cryptographic algorithms to generate a unique signature for data, can be verified by anyone with the corresponding public key, confirming that the data has not been tampered with.

Additionally, blockchain technology presents a novel approach to data integrity in cloud environments. By recording transactions in a decentralized and immutable ledger, blockchain can ensure that any changes to PHRs are transparent and traceable. Each block in the chain contains a cryptographic hash of the previous block, creating a secure link that is resistant to tampering.

Implementing blockchain for PHRs can enhance security by providing a trustworthy and auditable record of data access and modifications.

Privacy-Preserving Techniques

Beyond encryption and access control, privacy-preserving techniques such as differential privacy and federated learning are gaining traction in the realm of PHR sharing. Differential privacy aims to provide insights from data while minimizing the risk of identifying individual records. It introduces a controlled amount of noise to the data, balancing the trade-off between data utility and privacy.

Federated learning, on the other hand, enables collaborative data analysis without sharing raw data. By training machine learning models locally on patient data and only sharing model updates with a central server, federated learning preserves data privacy while leveraging the benefits of collective

intelligence. These techniques are particularly useful in healthcare, where data privacy is paramount.

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

Challenges and Future Directions

Despite the advancements in secure PHR sharing, several challenges remain. One of the primary challenges is ensuring interoperability between different health systems and cloud providers.

Standardizing data formats and protocols is essential for seamless data exchange and integration. Furthermore, the scalability of security solutions must be addressed, as the volume of health data continues to grow exponentially.

User education and awareness are also critical components of a comprehensive security strategy. Patients and healthcare providers must understand the importance of security measures and how to implement them effectively. Regular training and awareness programs can help mitigate the risks associated with human error and social engineering attacks.

CONCLUSION

In this study, we have presented a comprehensive framework for securely sharing personal health records (PHRs) within cloud environments. The growing adoption of cloud computing in the healthcare sector necessitates robust security measures to protect sensitive patient information from unauthorized access and breaches. Our framework addresses critical security challenges by incorporating encryption, access control mechanisms, and secure data sharing protocols, thereby ensuring the confidentiality, integrity, and availability of PHRs.

Firstly, the encryption of PHRs plays a pivotal role in safeguarding data both in transit and at rest. By employing advanced encryption techniques, such as attribute-based encryption (ABE) and homomorphic encryption, our framework ensures that only authorized individuals can access and manipulate the data. ABE enables fine-grained access control by associating attributes with users and policies, allowing for flexible yet secure sharing of information based on predefined criteria. Homomorphic encryption further enhances security by enabling computations on encrypted data without exposing the underlying information, thus maintaining confidentiality during data processing.

Secondly, access control mechanisms are integral to our framework, providing a structured approach to managing user permissions and roles. Role-based access control (RBAC) and attribute- based access control (ABAC) are utilized to define and enforce access policies, ensuring that only authorized users can access specific PHRs. RBAC assigns permissions based on user roles, simplifying the management of large user groups, while ABAC allows for more dynamic and context-aware access decisions by evaluating attributes such as user identity, location, and time of access. The combination of these access control models enhances security and usability, accommodating the diverse needs of healthcare providers and patients.

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

Secure data sharing protocols are another cornerstone of our framework, facilitating the safe exchange of PHRs between stakeholders. These protocols leverage secure multi-party computation (SMPC) and blockchain technology to establish trust and transparency in data sharing processes.

SMPC enables multiple parties to collaboratively compute a function over their inputs while keeping those inputs private, thus ensuring the confidentiality of shared data. Blockchain technology, with its decentralized and immutable ledger, provides a tamper-proof record of data transactions, enhancing accountability and traceability in the sharing of PHRs. The integration of these technologies within our framework ensures secure and verifiable data sharing, fostering trust among healthcare stakeholders.

Moreover, our framework emphasizes the importance of compliance with regulatory standards and best practices in healthcare data management. Adhering to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) is crucial for ensuring the lawful and ethical handling of PHRs. Our framework incorporates these regulatory requirements into its design, providing guidance on data protection measures, user consent, and breach notification procedures. By aligning with these standards, our framework not only enhances security but also promotes patient trust and confidence in cloud-based health record systems.

In addition to technical measures, our framework acknowledges the significance of user education and awareness in maintaining PHR security. Healthcare providers and patients must be well- informed about potential security risks and the best practices for safeguarding their data. Training programs and awareness campaigns can empower users to recognize and mitigate threats such as phishing attacks, social engineering, and weak password practices. By fostering a culture of security awareness, our framework aims to reduce the likelihood of human errors that could compromise PHR security.

Furthermore, the scalability and adaptability of our framework make it suitable for diverse healthcare environments, ranging from small clinics to large hospitals and healthcare networks. Its modular design allows for the seamless integration of new security technologies and protocols as they emerge, ensuring that the framework remains resilient against evolving threats. This flexibility is essential for addressing the dynamic nature of cybersecurity challenges in the healthcare sector.

REFERENCES

1. Akinyele, J., Lehmann, C., Green, M., Pagano, M., Peterson, Z., & Rubin, A. (2010). Self- Protecting Electronic Medical Records Using Attribute-Based Encryption. Cryptology ePrint archive, report 2010/565.
2. Ateniese, G., Fu, K., Green, M., & Hohenberger, S. (2005). Improved proxy re-encryption schemes with applications to secure distributed storage. In NDSS. The Internet Society.
3. Attrapadung, N., & Yamada, S. (2015). Duality in ABE: converting attribute-based encryption for dual predicate and dual policy via computational encodings. In CT-RSA 2015 (Vol. 9048, pp. 87–105). Springer.

Volume09 Issue08, Aug-2024, pg. 10-20

Published Date: - 03-08-2024

E-ISSN: 2536-7919
P-ISSN: 2536-7900
SJIF 2019: 4.58 2020: 5.046 2021: 5.328

4. Beimel, A. (1996). Secure Schemes for Secret Sharing and Key Distribution (PhD thesis). Israel Institute of Technology, Israel.
5. Blaze, M., Bleumer, G., & Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. In EUROCRYPT (Vol. 1403, pp. 127–144). Springer.
6. Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil pairing. In
7. ASIACRYPT (Vol. 2248, pp. 514–532). Springer.
8. Canetti, R., & Hohenberger, S. (2007). Chosen-ciphertext secure proxy re-encryption. In
9. CCS'07 (pp. 185–194). ACM.
10. Chase, M. (2007). Multi-authority attribute based encryption. In S.P. Vadhan (Ed.), TCC 2007 (Vol. 4392, pp. 515–534). Springer.
11. Chase, M., & Chow, S.S.M. (2009). Improving privacy and security in multi-authority attribute-based encryption. In CCS 2009 (pp. 121–130). ACM.
12. Deng, H., Wu, Q., Qin, B., Susilo, W., Liu, J.K., & Shi, W. (2015). Asymmetric cross- cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data. In ASIACCS (pp. 393–404). ACM.
13. Deng, H., Wu, Q., Qin, B., Susilo, W., Liu, J.K., & Shi, W. (2015). Asymmetric cross- cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data. In F. Bao, S. Miller, J. Zhou, G. Ahn (Eds.), Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS'15 (pp. 393–404). ACM.
14. Garg, S., Gentry, C., Halevi, S., Sahai, A., & Waters, B. (2013). Attribute-based encryption for circuits from multilinear maps. In CRYPTO 2013 (Vol. 8043, pp. 479–499). Springer.
15. Han, J., Susilo, W., Mu, Y., & Yan, J. (2012). Privacy-preserving decentralized key-policy attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 23(11), 2150–2162.
16. Hohenberger, S., & Waters, B. (2014). Online/offline attribute-based encryption. In Public- Key Cryptography (Vol. 8383, pp. 293–310). Springer.