International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 1, February 2022, pp. 853~858
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp853-858

Mutual query data sharing protocol for public key encryption through chosen-ciphertext attack in cloud environment

Tarasvi Lakum[1], Barige Thirumala Rao[2]
[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[2]Department of Computer Science and Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, India

Article Info

Article history:

Received Jan 31, 2021
Revised Jun 17, 2021
Accepted Jun 29, 2021

Keywords:

Cloud computing
Data sharing protocol
Identity-based cryptography
Privacy protecting cloud
chosen-ciphertext attack

ABSTRACT

In this paper, we are proposing a mutual query data sharing protocol (MQDS) to overcome the encryption or decryption time limitations of exiting protocols like Boneh, rivest shamir adleman (RSA), Multi-bit transposed ring learning parity with noise (TRLPN), ring learning parity with noise (Ring-LPN) cryptosystem, key-Ordered decisional learning parity with noise (kO-DLPN), and KD_CS protocol's. Titled scheme is to provide the security for the authenticated user data among the distributed physical users and devices. The proposed data sharing protocol is designed to resist the chosen-ciphertext attack (CCA) under the hardness solution for the query shared-strong diffie-hellman (SDH) problem. The evaluation of proposed work with the existing data sharing protocols in computational and communication overhead through their response time is evaluated.

Corresponding Author:

Tarasvi Lakum
Department of Computer and Science Engineering, Koneru Lakshmaiah Education Foundation
Vaddeswaram, India
Email: tarasiru1@gmail.com

1. INTRODUCTION

Cyber-physical cloud systems [1]-[5] are applicable in healthcare, in smart electricity grids, in advanced smart cities and so on. In these application [6]-[10], the resource constraint client devices are used to access the user data to analyze and store in the cloud from the cloud. The client device data stored in the client devices, have less computing capabilities and with inadequate security measures compare with the base stations. Among them is an example of cloud-assisted cyber-physical architecture, where the client device is a mobile device, which is connected to the mobile network through base stations like a base transceiver station. The user mobile device information including identity and location is shared with the central processors, in turn are connected to data servers for user data processing. As the home agent (HA) [11] and mobile subscriber data stored in the central processor data servers, mobile network operators perform the access request function to accept or decline for a particular service ie., in the form of Authentication of user, The requests made provides the data server services, the security challenges in the cyber-physical environments are: Mutual authentication, anonymous user, password protection, confidentiality and data integrity. The research is on privacy protection of multimedia file data in cloud through proxy re-encryption. Aiming to ensure the privacy and security for the shared cloud multimedia file data owner (CDO) and within the time to reduce the bandwidth of the multimedia files. The contributions are summarized: i) a chosen-ciphertext attack (CCA)-secure public key encryption (PEK) scheme in which the mutual cloud user pairing is removed for the improvement for the efficiency use; ii) to improve the security of cloud shared multimedia files in cloud service platforms, the research work in this paper, through a mutual sharing protocol, a new CCA secure PEK scheme is proposed to result a CDO secured one.

Section 2 introduces the related works of the proposed work. In section 3, the proposed work is illustrated, and in section 4, the security proof and efficiency comparison are provided. Sections 5 and 6 gives the conclusion and future scope of the proposed work.

2. RELATED WORKS

Security against CCA [12] gives the exact security representation for a cryptosystem. The literature works [13]-[17] have come up with the schemes to make a secure cryptosystem through the semantic security systems. In a weaker security system called lunch-time attack is proposed, the decryption of ciphertexts were considered before user receives the required ciphertext. They presented a conversion method for chosen-ciphertext attacks through non-interactive zero-knowledge proof systems, they lack to provide a ciphertext necessity during decryption. In the non-interactive zero-knowledge proofs is constructed, during the encryption of messages, a zero-knowledge proof of the plaintext is appended, leading to the adaptive chosen-ciphertext secure cryptosystems. A plaintext-awareness is proposed, by building a valid ciphertext, by providing the known corresponding plaintext.

Security for public-key encryption schemes is formally defined, through semantic security of a message encryption keeping the attacker from computing the message without the encryption key and message. They provided this by: two plaintexts; a ciphertext C that encrypts the plaintexts in a feasible way, and mounting a chosen-plaintext attack security system called 'CPA-security' but this semantic security could not provide decryption device security against an attacker. In the settings of decryption is made in-distinguish ability through the appropriate non-adaptive case. The semantic security models provide the extensions of the chosen-ciphertext attacks, with in-distinguish ability.

Semantic security of encryption schemes [18], [19], are extended to public-key cryptosystem (PKC) with a system of having and decryption servers to hold the private decryption scheme, called t-secure, which reconstructs the cleartext from the distinction between the ciphertexts of different messages. Security against CCA were defined, to provide additional security when using these CCA systems in general security applications. There are numerous applications [20]-[25] of the above said decryption service, to distribute security service [26], [27] in a key recovery mechanism, by allowing decryption of specified messages. Here, the process of decryption is done by authenticated user, but if a specified party is capable to decrypt the ciphertext, then the decryption services are to be organized. In this paper, the process of decryption based on mutual query data sharing protocol, the security provision is through the mutual authentication by an identity-based protocol, by demonstrating session key authentication and user key attack computations.

The cloud multimedia CDO, wants to share a message in the form of file F1, among the group of users. To perform this activity, the CDO is registered with the public-key generator through cloud enabled service and with appropriate CDO credentials. After the registration and login procedures, the following tasks are performed by CDO. The CDO containing public and private keys ie., key-pair with a cloud management software is enabled through the CDO credentials. In CDO cloud folder, the CDO files are stored in cloud folder as user. The stored files are encrypted and accessed by executing the cloud software. The key-pair is made available in public folder of CDO, which makes the CDO to have the copy of key-pair in public and private domain. The sharing of key-pair among the cloud owners through client software, among the two different authorized cloud owners, Alice and Bob, by using the key sharing Alice have an access to Bob key-pair and vice versa.

In the proposed mutual query PKE-based solution, the authentication is not transparent as key-pair. The file encryption and sharing are performed through a randomly generated number to perform symmetric encryption of the CDO credentials based. The CDO experience in using the encryption process is enhanced by multicast mechanism of the CDO key-pair, so that the user key-pair are provided with three registration authentication service.

3. PROPOSED RESEARCH WORK

In this section, the proposed scheme is presented in the form of protocol and authentication process with an implementation algorithm for data sharing. The proposed protocol contains three phases, namely: initiation, encryption and sharing and accessing and decryption. The processes in these phases are file initialization, process to create, file encryption, and file sharing in cloud, keyword based file accessing and symmetric key decryption: i) initiation: the CDO owner generates a multimedia file to share in the cloud, for that CDO owner need a public-key generator (PKG) to run setup file based algorithm with security parameters and authentication credentials *k*, in order to produce parameters and master private key (MSK), here CDO owner holds MSK in private and parameters as public; ii) encryption and sharing: now CDO owner (called as primary) wants to share to another CDO owner (called as secondary).

To perform this, the secondary CDO owner has to register in cloud server to PKG using any cloud service provider platform like mobile or PC. After, secondary CDO owner need to login to the cloud service where primary CDO owner multimedia message file is shared, with proper login procedures and credentials to the cloud center (CC). The primary CDO performs many tasks in order share the multimedia message file to secondary CDO owner, they are:

- For a set of groups U and set of individual users V in cloud CC, the multimedia message file M is created.
- For the number of U and V variables, the encryption process is initiated by Encrypt (U, V, M, parameters) keyword passing the cloud software platform.
- With the usage of keywords in cloud service provider, the primary CDO owner have a symmetric encryption key, which is a randomly generated number assigned to each CDO. Through this, the encrypted M is sent to public network along with the CDO identifier keywords.
- The randomly generated number of primary CDO owner is known to cloud server, causes the cloud server to check the M result which is in the decryption form. The decrypted M file is stored in the cloud server center, and can be decrypted by CC with keywords shared by primary CDO owner.
- Now, the primary CDO owner, multicasts the decrypted keywords through CC to the U and V through a client device such as mobile or PC.
- Through the credentials and authentication process, the secondary CDO owner gets in to the CC to access the cloud shared files.
- With the received keywords, the secondary CDO owner searches for the M file based on the query of the keywords. The M file based through keywords are analyzed multiple times, until the M file is found. As the M file is found, the secondary CDO owner data center (DC) is to be determined by the primary CDO owner CC, whether secondary CDO owner is authorized to receive the M file. As the CC founds the presence of access grant for secondary CDO owner, the symmetric encryption process if initiated with the use of randomly generated number along with the encryption ID of cloud service is shared with the DC over a public cloud network. After receiving the encryption ID, the DC at the secondary CDO owner performs the symmetric key decryption algorithm.
- After the decryption process through public key, the secondary CDO owner need to encrypt the message M file into ciphertext (CT). For this, secondary CDO owner asks private key to PKG of DC cloud service provider. Through the private key, the Extract() algorithm is performed.
- The key-pair is being used in the above steps, based on private and public keys, after Extract() algorithm, the Decrypt (MSK, ID, CT, params)=M algorithm is executed and received at the secondary CDO owner cloud software platform. The above steps completes the proposed protocol phases of message creation, file initialization, process to create, file encryption, file sharing in cloud, keyword based file accessing, decryption of message and symmetric key decryption.

3.1. Proposed MQ-PKE based authentication process

Here, the identification and registration of CDO is performed through PKE authentication process. In four phases, the PKE authentication process to check whether the cloud owner from CC and data center (DC) are identified is shown in Figure 1.

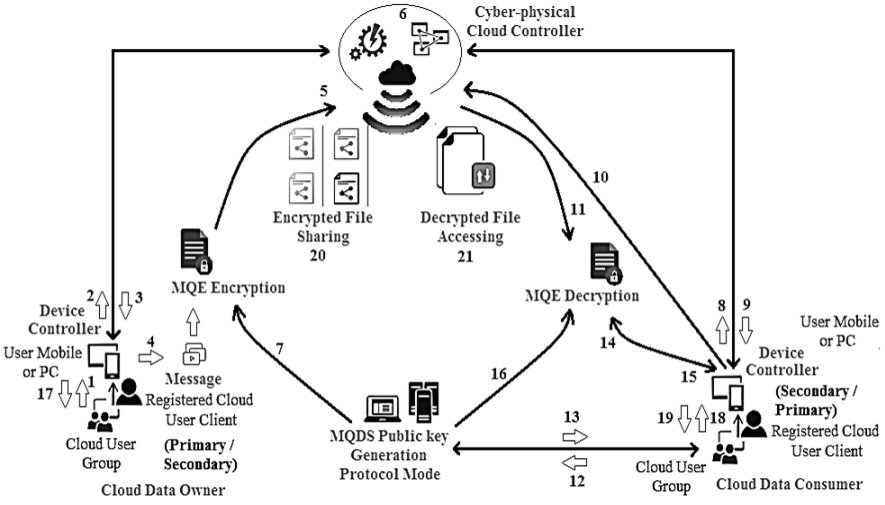

Figure 1. Proposed MQ-PKE based cloud network model for cloud security

4. RESULTS AND DISCUSSION

4.1. Simulation of the MQDS protocol through cyber-physical cloud environment

In the proposed work, the process of authentication technique is discussed to check the authorization of cloud user client for the CDO logging into the cloud server. In the demonstration of the proposed protocol, the security vulnerabilities such as password guessing attack, impersonation attack and session key discloser attack are well protected. The simulation of the proposed authentication protocol through cyber-physical cloud environment is made in this paper, to ensure the protection of data sharing security attacks against the key-pair CDO.

4.2. Computational analysis

The computational analysis is made with the proposed authentication technique and mutual query encryption (MQE) scheme for CDO multimedia message file for encryption and decryption. To reduce the computational complexity overhead, the CDO and cloud share the authentication by hash function level of security. The level of security is given in two ways: firstly, for a single cloud server (CS) and CDO, there are three computational exponentials for each CS. Secondly, for a separate cloud user group, CS need these three computational exponentials. Completely, there are six computational exponentials needed by CS to perform for each CDO, which is an exponential term based on the number of individual cloud user, who might be in the same cloud user group or in the different with different number of cloud user, making the CS to perform (3c+6g+2) exponential operations, where c is the number of individual cloud user in the group, g is the number of different cloud user group with the same or different cloud user in that group. Table shows the computational analysis of each stage of the proposed data sharing and encryption schemes.

4.3. Protocol implementation analysis

In the proposed data encryption scheme, CDO generates a ciphertext, with the variable size depending on the cloud users and groups. For c number of individual cloud user and g number of cloud user groups in each cloud group, with a total of 2c+2g*4u, where u is the number of cloud users in the cloud group, with the size of ciphertext is (c+g)|G1|+|G2|+|Zp*|.

4.4. Implementation

The execution process of the proposed protocol operations is made on a HP with Intel (R) Core (TM) i5-3230M CPU @ 2.60 GHz with 8 GB RAM running on Windows 8. The markings of mutual query data sharing (MQDS) with the execution time requirements for encryption and decryption by MQE scheme with 128-bit key is listed in Table 1. Similarly, the execution time of MQDS operation is computed through 10 successful runs among two CDO users, with a random input by MQDS software library.

Table 2 shows the benchmark times of MQDS protocol operations through the cloud group user by comparing with the exponential operations which were computed in the proposed work implementation, by pre-processing requirements. To have fastest key-pair process, Type-A security of cloud user group size of 512-bit with embedding degree of 2 is made for 1024 bit rivest–shamir–adleman (RSA) security level. The Type-A is a super-singular curve of y2+x3+x of Solinas prime ordered group, where G1=G2. For the sake of comparison, |G1|=|G2|=|Zp*|, G=G1, GT=G2. And there are 10 cloud users from different data customers, belonging to same groups are allowed and accessed to perform the common information sharing. Table 3 shows the execution times by different algorithms in MQDS protocol. Table 4 shows the execution time required for the MQDS protocol algorithms in different schemes of comparative protocols for 10 data customers.

Table 1. Practical benchmark of AES symmetric key encryption

Algorithm	Keysize	Encryption	Decryption
Proposed MQDS PKE	128-bit	105.635 x 128 bits/s	129.532 bits/s

Table 2. Benchmark execution time ms of different cryptographic operations

Curve (Type)	Bilinear Pairing (Tp) of key-pair		Exponentiation (TE)		Modular inversion (TINV)	Map-To-Point Hash (TMTP)
	Normal	PreComp	In G	In GT		
Type-A	2.621	1.345	0.564	0.091	0.012	0.412

Table 3. Minimum cost (ms) required by data owner and consumer during encryption and decryption

Protocol	Setup	Extract	Data Owner	Data Consumer
Proposed MQDS PKE	1.396	0.614	4.014	1.105

Table 5 shows the efficiency comparison for CCA-secure encryption schemes. The proposed MQDS PKE is compared with kurosawa-desmedt variant of cramer-shoup encryption (KD-CS), here exp stands for exponentiation; "f-exp" refers to exponentiation relative to a fixed base and one multi-exponentiation is counted as 1.5 exponentiations. Ciphertext overhead (in bits) is the difference between the lengths of the ciphertext and the message. L_{BG} is the bit-length of an element in a group, L_{DDH} is the bit-length of an element in a group suitable for the KD-CS scheme and L_{MQDS} is the bit-length of an element in a group suitable for the proposed MQDS PKE scheme. Table 6 gives the encryption/decryption times for comparison. The proposed MQDS PKE is compared with the performance of the RSA, multi-bit transposed ring learning parity with noise (TRLPN) and ring-learning parity with noise (RLPN) cryptosystems, and key-Ordered-decisional learning parity with noise (kO-DLPN) for various security levels. As a benchmark, the proposed scheme is performed with the number of operations on w plaintext bits in parallel where w, the word size, is in our case 128.

Table 4. Time (ms) required by surveyed algorithms

Scheme	Computational Cost			
	Setup	Extract	To Upload	To Download
Cheng *et al.*	0.311	0.645	10.88	1.422
Han *et al.*	1.866	6.995	20.64	2.798
Yang *et al.*	1.245	0.311	1.244	7.773
Zhou-Huang	3.108	6.842	15.296	4.972
Karati	1.458	0.640	4.340	1.156
Proposed MQDS PKE	1.394	0.612	4.012	1.098

Table 5. Efficiency comparison for CCA-secure encryption schemes

Scheme	Encryption	Decryption	Key Generation	Ciphertext Overhead
Boneh	3.5 f-exps	1.5 exp+1 pairing	4 f-exps	2. L_{BG}+704
KD_CS	3.5 f-exps	1.5 exps	3 f-exps	2. L_{DDH}+128
Proposed MQDS PKE	3.5 f-exps	1.5 exps+2 pairing	5 f-exps	2. L_{MQDS} +1024

Table 6. Encryption/decryption times for comparison

	Time Per Encryption (ms)			Time Per Decryption (ms)		
Security Level (bits)	80	112	128	80	112	128
RSA	0.010	0.030	0.060	0.140	0.940	2.890
Multi-bit TRLPN	1.400	3.100	4.400	0.052	0.098	0.128
Ring-LPN Cryptosystem	13.20	29.90	42.20	3.10	6.90	9.70
kO-DLPN	20.12	62.11	99.85	0.061	0.089	0.119
Proposed MQDS PKE	12.80	20.40	31.20	0.021	0.044	0.087

5. CONCLUSION

In this paper, a new MQDS protocol is proposed and designed for cyber-physical cloud security and privacy systems based on the CDO pairing through chosen-ciphertext attack in the cloud environment for public key encryption scheme. In this MQDS, firstly a new CDO is registered to the cloud server and cloud service software. Secondly, the CDO sends the encrypted multimedia message in the form of file, to the registered CDO user. If this registered CDO user is untrusted, the cloud controller commands this information to client devices as the registered CDO user becomes trusted. The design and implementation of MQDS is demonstrated with security and correctness of the MQDS protocol, and the performance is evaluated.

6. FUTURE SCOPE

In future research, through this proposed work, to prevent unauthorized cloud data usage, an access control system through a secret key search system with key-pair generation and decrypting of malicious user information through the public key encryption scheme is intended to design and implement.

REFERENCES

[1] A. Karati, R. Amin, S. H. Islam, and K. -K. R. Choo, "Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment," in *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 318-330, Jan.-Mar. 2021, doi: 10.1109/TCC.2018.2834405.

[2] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," *2012 8th international conference on network and service management (CNSM) and 2012 workshop on systems virtualization management (SVM)*, 2012, pp. 37-45.
[3] J. Yang, H. Wang, J. Wang, C. Tan, and D. Yu, "Provable data possession of resource-constrained mobile devices in cloud computing," *Journal of Networks*, vol. 6, no. 7, pp. 1033-1040, 2011, doi: 10.4304/jnw.6.7.1033-1040.
[4] J. Han, W. Susilo, and Y. Mu, "Identity-based data storage in cloud computing," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 673-681, 2013, doi: 10.1016/j.future.2012.07.010.
[5] H. Cheng, C. Rong, Z. Tan, and Q. Zeng, "Identity based encryption and biometric authentication scheme for secure data access in cloud computing," *Chinese Journal of Electronics*, vol. 21, no. 2, pp. 254-259, 2012.
[6] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," *SIAM Journal on Computing (SICOMP)*, vol. 36, no. 5, pp. 915-942, 2006, doi: 10.1007/978-3-540-24676-3_13.
[7] K. Kurosawa and Y. Desmedt, "A new paradigm of hybrid encryption scheme," in *Advances in Cryptology-Crypto 2004*, vol. 3152, pp. 426-442, 2004, doi: 10.1007/978-3-540-28628-8_26.
[8] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in *Cryptology Conference*, vol. 1462, pp. 13-25, 1998, doi: 10.1007/BFb0055717.
[9] K. Emura, G. Hanaoka, K. Nuida, G. Ohtake, T. Matsuda, and S. Yamada, "Chosen ciphertext secure keyed-homomorphic public-key cryptosystems," *Designs, Codes and Cryptography*, vol. 86, no. 8, pp. 1623-1683, 2018, doi: 10.1007/s10623-017-0417-6.
[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978, doi: 10.1145/359340.359342.
[11] S. Heyse, E. Kiltz, V. Lyubashevsky, C. Paar, and K. Pietrzak, "Lapin: an efficient authentication protocol based on ring-LPN," *International Workshop on Fast Encryption*, vol. 7549, pp. 346-365, 2012.
[12] T. Lakum and B. T. Rao, "A key-ordered decisional learning parity with noise (DLPN) scheme for public key encryption scheme in cloud computing," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 11, pp. 157-161, 2019, doi: 10.14569/IJACSA.2019.0101121.
[13] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: a case study of anonymous authentication," *Pervasive and Mobile Computing*, vol. 41, pp. 259-269, 2017, doi: 10.1016/j.pmcj.2017.03.009.
[14] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681-2691, 2015, doi: 10.1109/TIFS.2015.2473820.
[15] S. H. Islam and G. P. Biswas, "Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys," *Wireless Personal Communications*, vol. 82, no. 4, pp. 2727-2750, 2015, doi: 10.1007/s11277-015-2375-5.
[16] S. Chakraborty, S. Raghuraman, and C. P. Rangan, "A pairing free, one round identity based authenticated key exchange protocol secure against memory-scrapers," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 7, no. 1, pp. 1-22, 2016.
[17] L. Ni, G. Chen, J. Li, and Y. Hao, "Strongly secure identity based authenticated key agreement protocols without bilinear pairings," *Information Sciences*, vol. 367-368, pp. 176-193, 2016.
[18] L. Dang *et al*., "Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 4, 2018, doi: 10.1177%2F1550147718772545.
[19] S. Bala, G. Sharma, and A. K. Verma, "PF-ID-2PAKA: pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks," *Wireless Personal Communications*, vol. 87, no. 3, pp. 995-1012, 2016, doi: 10.1007/s11277-015-2626-5.
[20] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1621-1631, 2018.
[21] S. H. Islam and G. P. Biswas, "A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication," *Journal of King Saud University-Computer and Information Sciences*, vol. 29, no. 1, pp. 63-73, 2017, doi: 10.1016/j.jksuci.2015.01.004.
[22] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," in *IEEE Systems Journal*, vol. 12, no. 2, pp. 1621-1631, Jun. 2018, doi: 10.1109/JSYST.2016.2633809.
[23] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice based anonymous authentication protocol for mobile devices," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2775-2785, 2018, doi: 10.1109/JSYST.2018.2851295.
[24] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, no. 1, pp. 42-52, 2018, doi: 10.1016/j.jnca.2018.05.005.
[25] H. Yu, and B. Yang, "Low-computation certificateless hybrid signcryption scheme," *Frontiers of Information Technology and Electronic Engineering*, vol. 18, no. 7, pp. 928-940, 2017, doi: 10.1631/FITEE.1601054.
[26] Q. Huang, Y. Yang, and J. Fu, "PRECISE: identity-based private data sharing with conditional proxy re-encryption in online social networks," *Future Generation Computer Systems*, vol. 86, pp. 1523-1533, 2018, doi: 10.1016/j.future.2017.05.026.
[27] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1265-1277, Jun. 2016, doi: 10.1109/TIFS.2016.2523941.