Indian Journal of Science and Technology, Vol 8(36), DOI: 10.17485/ijst/2015/v8i36/87861, December 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Survey on Encryption Techniques used to Secure Cloud Storage System

R. Kirubakaramoorthi*, D. Arivazhagan and D. Helen

AMET University, Kanathur, Chennai - 603112, Tamil Nadu, India; Kiruba.daruth@gmail.com, it_manager@ametindia.com, helensaran15@gmail.com

Abstract

Cloud Computing is very flexible in nature that helps to quickly access the resources efficiently from the third party service provider to expand the business with low capitalization cost.A cloud storage system stores large number of data in its storage server. Since the data is stored for a long term over the internet it does not provide the data confidentiality and make the hackers to steal the data provided in the storage system and even when data forwarded to cloud environment, it lacks data integrity and makes the cloud user unsatisfied. In this paper, we study about different encryption technique to protect the cloud storage environment. This paper concisely covers some of the existing cryptographic approaches that can be used to improve the security in cloud environment

Keywords: Cryptographic Approaches, Cloud Storage System

1. Introduction

Cloud computing is the latest approach in the present generation to minimize the cost by providing a sharing environment for the cloud user, the cloud users can remotely store and retrieve their data into the cloud. By envisioning outsourcing of data, users can be released from the burden of data storage and maintenance. Preserving integrity of data is an issue that the physical possession of the possibly outsourced data is not known by the user makes the Cloud Computing very challenging and potentially tasking, particularly for users with certain constrained computing resources and capabilities.

Cloud computing, enables users to keep their information in the cloud so as to utilise scalable on-demand services. Mainly for small and medium-sized organisation with limited budgets, enabling to achieve high cost savings and enhancements of productivity by using cloud-based services for managing projects, to accomplish collabora-tions among each other's, Cloud Service Providers (CSPs), use to concentrate on sensitive data, raise potential secu-rity and privacy bottlenecks which are not available in the similar trusted domains of enterprise users. In-order to protect theuser sensitive data confidential from untrusted CSPs, a naive way is to use cryptographic methodologies, by disclosing decryption keys making available to accredit users. However, sensitive data is outsourced for sharing on cloud servers by organisation users; the encryption system applied will also provide increased performance, delegation, and scalability, besides supporting fine-grained access control. Thus, this is accomplished so as to best serve the needs for accessing data anytime irrespective of location, negotiating within the organisation.

Data storage and processing occurred within the secure resources of these end hosts, with the network simply provides the transfer. Therefore it is inevitable to discuss about data protection could largely involve privacy and security evaluations at all known end points of a data transaction, with necessary security measures applied to ensure production of data in movement. Cloud data storage (Storage as a Service) is an important service of cloud computing referred as Infrastructure as a Service (IaaS). Data storage offers so many benefits to users: 1. It provides unlimited data storage space for storing user's data. 2. Accessing the data from the cloud provider via internet anywhere in the world not on a single machine. 3. no necessity for buying any storage device for storing our data and to maintain data. Users participate in the

*Author for correspondence

CLOUD and they join or leave CLOUD at any point of time in cloud computing environment.

The major issue in adopting cloud is the security. The data stored in the cloud get increased every day and hence we need some mechanisms to ensure that our data is stored in secured manner without any unauthorized access. Security for the data stored in the cloud environment[1] is a wanted one. Providing integrity to the data that has been distributed over cloud is a challenging one. The primary solution to deal with this difficult situation is to use the cryptographic methods in cloud environment. In this paper, we describe various cryptographic techniques that can be used to protect the data used in the cloud and prevent information from being leak and to ensure that the privacy has been maintained. The cryptographic methods were used to ensure security for the data stored in the cloud.

This paper is organized as follows. Section 2 describes about Cryptographic Cloud Storage and its strengths, Section 3 addresses some Cryptographic Techniques that are used in cloud environment. Section 4 shows the description about the cloud service that uses the cryptographic techniques to ensure security and Section 5 gives the conclusion about this article.

2. Cryptographic Cloud Storage

The data may get disclosed or modified by any unauthorized access. It is essential that a special care must be taken to protect our sensitive data. A secure storage[2] must be achieved in cloud computing. So we adopt cryptographic techniques for the secure storage. The data is encrypted by the data owner before the data is uploaded to the cloud. The major feature of a cryptographic storage is that the security properties that are described below are accomplished

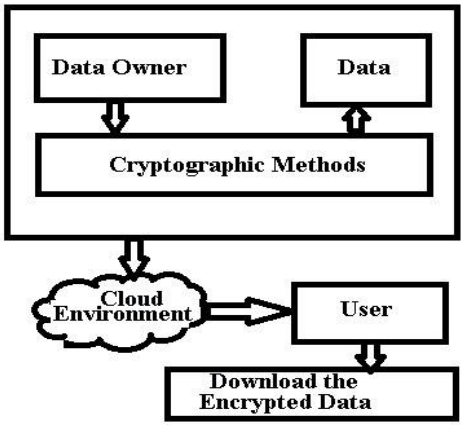

Figure 1. Cloud Strategy.

The above diagram represents cryptographic cloud storage. The owner of the data applies cryptographic methods to the sensitive data to protect the information from unauthorized access. The data owner uploads the encrypted data to the cloud environment. The authorized user can decrypt the data and download the required file.

The Strength of Cryptographic Cloud Storage are mostly depending on two factors they are Confidentiality and Integrity.

Confidentiality Cryptographic Cloud Storage[3,4] provides Confidentiality as the main characteristics. The information's were encrypted with the advanced cryptographic techniques and thus the secrecy is maintained.

Integrity: Cloud Storage provides Integrity to the data and thus it prevents any unauthorized people to modify the data.

3. Cryptographic Techniques

The main components of a cryptographic storage service which can be implemented by using a different techniques, out of which, some were designed specifically for cloud storage. In the beginning of the Cloud Computing, common encryption Technique like Public Key Encryption was applied. This traditional technique does not provide expected result as it support one to one encryption type communication. Public Key Encryption is not highly scalable. This gave rise to move forward to some advanced encryption methods. The advanced cryptographic methods includes the below encryption methods.

- Searchable Encryption
  - Symmetric searchable encryption
  - Asymmetric Searchable Encryption (ASE).
- Homomorphic Encryption
- Identity Based Encryption
- Attribute-based Encryption
  - KP-ABE
  - CP-ABE
  - MA-ABE
- Cloud DES Algorithm

3.1 Searchable Encryption

A searchable encryption scheme is applied at high level inoder to encrypt the content that is available in search index so that it can hidden from others except the party that provide the authorised tokens A collection of files which consists of full-text index otherwise keyword

index considered to generate a search index. The index is encrypted based on searchable encryption scheme in such a way (i) The pointers to the encrypted files can be retrieved based on the tokens given for the keyword. (ii) if the token is not provided then the contents are hidden for the index. However, with the complete understanding of secret key, the tokens are generated. The retrieval procedure does not reveal the content of the files or the keywords apart from the files that comprise the keyword in common. The previous statement is worth taking about since it is difficult to understand the searchable encryption that is applicable for security. After many searches the researchers identified the file containing the common keyword may have a probability to deliver the information to the third party. Based on the repeated search from the client search pattern, the server automatically guesses some assumption of required keywords that is being searched. While searching, some information is leaked and this information is similar to the appropriate file that is being returned to the customer by the server. This information that is leaked and based on leaked information the server retrieved the file is learned by the provider. (i.e. file may contain repeated keywords). We can also say the data leaked to the provider is based on the service is being used whereas it is not disclosed by the cryptographic primitives, (i.e., Exact keyword matches is used to fetch files). This leakage seems almost essential for both efficient and reliable service in cloud storage, At worst case, the data leaked from the public cloud storage service is having very less information. Depending on different scenarios, there exist various types of searchable encryption schemes that can be applied. For example, Symmetric Searchable Encryption (SSE) is implemented for data processing in small enterprise architectures, whereas Asymmetric Searchable Encryption (ASE) is implemented for large enterprise architecture. In the subsequent topics, we explain each type of encryption scheme in detail.

3.1.1 Symmetric Searchable Encryption

It is suitable for the environment where the client that searches the data and also he is responsible for generates it. A Single Writer/Single Reader (SWSR) is derived from cloud storage terminology. SSE schemes were presented in[4] and enhanced constructions and security terms were specified in[5-7]. SSE has two major advantages they are efficiency and security. It also has disadvantages such as functionality and tradeoff efficiency. SSE schemes are suitable for the entity who perform the encryption and also for the entity who searches with a keyword from the cloud storage system. Most SSE schemes are efficient because they use the concept of pseudo-random functions and also block ciphers for encryption purpose. In[7], Search technique can be efficient since SSE allows to pre-processed the data and efficiently represent in data structures. SSE provides security guarantees which are discussed as (i) the information about the data are hidden until the tokens are revealed. Since token is not revealed, the server learns only the length information. (ii) when the token is provided for a keyword, the server absorbs the document containing the keyword without knowing the keyword. When comparing with asymmetric and searchable encryption, it is found that security guarantees is much stronger without any limitations. Based on the various issues which is discussed above, every construction contains deterministic tokens. These deterministic tokens help the service provider to identify the repeated queries without knowing the query. Curtmola et al.[7] explained the duration of search time is optimal for the server but the index are inefficient during updates. On the other hand Goh[5] proposed the index can be updated efficiently in the server but the search time is not optimal. The above mentioned scheme don't not focus on the search based on conjunctions or disjunction of terms. SSE scheme alone handles the concept of conjunction[8] by pairing with the help of elliptic curves but it is inefficient when applying Asymmetric Searchable Encryption schemes (ASE). Another constraint of some searchable encryption is that they are only secure in a some situation where the queries are produced non-adaptively (ie, Without looking at the answer of the previous queries). In[7], some queries which need the answer for the previous query can also bereffered and this is known as adaptive setting in a secure environment.

3.1.2 Asymmetric Searchable Encryption (ASE)

This scheme is suitable for the environment where the client that searches the data is different from the one who generates it. This scenarios is referred as Many Writer/Single Reader (MWSR). The basic concept of ASE schemes were discussed in[9] and the enhanced definitions were explained in[10]. Numerous works have been performed to show how to achieve more difficult queries in public-key setting like conjunctive searches and range queries[11-13]. In[14-16] different issues that arise in various

application of ASE has been surveyed. In[17], the complete privacy of queries is guarantee in ASE. The main disadvantage of ASE is weaker security and it is not efficient while the major advantage is its functionality. Compared to SSE scheme, The ASE is suitable for enormous amount of setting due to the multiple writer and reader. ASE is inefficient because it make use of the concept of pairings on elliptic curves. This concept will make the operation slow when compared to hash functions or block ciphers. ASE allows to pre-processed the data and inefficiently represents in data structures. ASE provides security guarantees which are discussed as (i) the information about the data are hidden until the tokens are revealed. Since token is not revealed, the server learns only the length information. (ii) when the token is provided for a keyword, the server absorbs the document containing the keyword without knowing the keyword which is inefficient when compared to SSE setting. Byun et al.[18] depicts the server can introduced a dictionary attack for a token and identify the proper keyword the client is looking for. It can also identify the token and perform a suitable search to find out which documents comprise the (known) keyword.

3.2 Homomorphic Encryption

Ronald Rivest et al.[19] explain the Homomorphic encryption concepts. This scheme is applied in the cloud environment to protect the data. This Homomorphic encryption scheme allows executing computations on the encrypted data. It is only of the advanced cryptographic technique. In[20] the major drawback of homomorphic encryption is explained. It has a slow processing time during computation

3.3 Identity based Encryption

Identity Based Encryption cryptographic scheme has been developed by Shamir[21] in 1984. Major issue is the inability to build Identity Based Encryption system which is based on RSA. Later in 2001 an efficient Identity Based Encryption has been developed by Boneh and Franklin[19]. In Identity Based Encryption, an identity of the user plays a vital role. The sender who sends the message only needs to know the receiver's identity attribute in order to send the encrypted messages. Email Encryption is one of the major applications for Identity Based Encryption. However, key revocation is not achieved in Identity Based Encryption.

3.4 Attribute-based Encryption

Attribute-based Encryption is one of the cryptographic techniques used in Cloud Computing Environment. Attribute-based Encryption is first brought into use by Sahai and Waters[22] in the year 2005. The main focus of this Attribute-based Encryption scheme is to provide security to the data stored in the cloud. The four steps in Attribute Based Encryption are Setup, KeyGen, Encrypt, Decrypt. The KenGen() algorithm is used to the create private key of the user for secret sharing. The users who are authorized can decrypt the information using their private key. Attribute-based Encryption come up with access control. In Attribute Based Encryption, data owner uses a set of attributes to encrypt the data and only the authorized users who has the predicted or certain attributes can decrypt the data. This encryption scheme makes the cloud environment more secure. The various classes of Attribute-based Encryption are summarized.

3.4.1 Key-Policy Attribute-based Encryption

KP-ABE is introduced by VipulGoyal and Omkant Pandey[23] to achieve fine-grained access control[24] in one-to-many communications. In Key-Policy Attribute-based Encryption, the encrypted data is constructed with the set of attributes. The person is authorized to decrypt the Ciphertext if and only if the attributes that are built with the cipher text satisfy the access structure of their private or secret keys. The four steps in Key-Policy Attribute Based Encryption are Setup, KeyGen, Encrypt, Decrypt. The KeyGen and Decrypt algorithms get differed from the Attribute Based Encryption. In Key-Policy Attribute-based Encryption, private key of the user is cognated with the access structure. However unauthorized access may occur, the people may decrypt the information. This can be overcome in the Ciphertext Policy Attribute Based Encryption which construct the access policy in the encrypted data ie, ciphertext and employs a set of attributes to narrate the private key of the user. Also in some applications that uses this scheme, owner of the data must have a firm belief with the key issuer

3.4.2 Ciphertext Policy Attribute based Encryption

In 2007, Bethencourt et al.[25,26] proposed a cryptographic technique named cipher text policy attribute-based method. The access policy is built with the data that has been encrypted. In CP-ABE the cipher text is identified

with access structure and the private keys with the attributes. In Key-Policy Attribute Based Encryption, the major disadvantage is that the access policies were not created by the encryptor. This provided a route to the establishment of Ciphertext Policy Attribute Based Encryption which allows the access policies to be built with the encrypted data. The owner who encrypts the data, model the access policy. A proposal was made in[27] for the use of CP-AB technique. The data owner is in charge of defining the access policies. This prevents unauthorized access and promotes security. In CP-ABE, revocation is not achieved efficiently. Thus it is not so easy for the data owner to modify the access polices whenever needed.

3.4.3 *Multi_Authority Attribute based Encryption*

Multi-Authority Attribute Based Encryption is introduced by Chase[28,29]. The Multi-Authority Attribute Based Encryption (MA-ABE) is also a cryptographic technique which consists of many authorities to manage the attributes and the distribution of the secret keys. The user who wish to download the information will request the decryption keys from the attribute authority. The attribute key generation is one of the algorithm in MA-ABE. This algorithm is run by the authority and in turn the authority will distribute the keys to the users. An authorized user who has the appropriate decryption keys can view the information. The algorithms involved in this scheme include Set up, Attribute Key Generation, Central Key Generation, Encryption, Decryption. This cryptographic scheme handles more number of users. Data confidentiality can be achieved on using this type of technique in cloud environment. As it is suitable for multiple authorities scenario, this cryptographic technique is most suitable for the applications which contains various sectors. This cryptographic scheme improves security and reduces key management complexity which are the major advantages.

4. Cloud DES Algorithm

Neha Jain et al.[30] have introduced the concept of Data security using the DES algorithm in cloud computing. This approach is applicable for securing both the server and the clients. DES cipher block chaining is constructed for security architecture to eliminate the fraud that is taken place in stealing the data. The data forwarded to the receiver which is hacked is replaced with no danger. The system with encryption is adequately secure, but the kind of encryption increases is directly proportional to computing power. Symmetric key are used to encrypt the model to result in better secure communication system. The author insist that the cloud data security by analysing the encryption based on various factors such as the data security requirements, data security process, the data security risk, security functions of data deployment. The main view of their paper is the encryption of data security solutions, which is also important and it can be applied as reference when designing the entire security solution.

Monikandan et al.[20] have discussed an encryption algorithm to consider the security and privacy issue in cloud storage. It also protects the data present in secured cloud from unauthorized access. The data that is available in secure cloud can be attacked in two ways (i) insider attack (ii) Outsider attack. The insider attack is the admin of an organisation who has the privilege to access all user's data whereas the outsider attack belong to the third party trying to access the data of user's. The Author implemented a symmetric encryption algorithm to guard the data that is stored in cloud storage from the attackers. The technique is implemented by converting the plain text into cipher text by using ASCII code and key value between 1 to 256. By Combining substitution cipher and transposition cipher the classical encryption technique is enhanced. Symmetric encryption performs computational efficiency and high speed to handle large amount of data in cloud storage. Their proposed algorithm does not allow the administrators or attackers to access the data from the cloud storage since it the user data is encrypted.

The following table depicts comparative analysis of various cryptographic algorithms based on Access control, Scalability, Flexibility, Efficiency

Table 1. Cryptographic Algorithm Analysis

Schemes/ Parameters	Access Control	Scalability	Flexibility	Efficiency
IDE	Low	Avg	Low	Low
HE	Low	Avg	Low	Low
ABE	Avg	High	Avg	Avg
KP-ABE	Avg	Avg	High	Avg
CP-ABE	High	Avg	High	Avg
MA-ABE	Better	High	High	High

5. Proposed Work

In our proposed work, the data owner controls the problem of data forwarding between user and storage server. The system architecture consists of various key servers and disturbed storage servers. By storing the cryptographic keys in different key servers in order to perform cryptographic function to make the cloud storage data secure rather than keeping the cipher key in single server. Therefore security mechanisms will provide high security for the key server.

6. Conclusion

The data storage service is the main service provided by the cloud provider. The Cryptographic techniques have been used widely in cloud environment. Cryptography is an essential tool that helps to assure our data accuracy. Cryptographic methods has been effectively lead by the development of cloud computing and also due to vast increment in the range of users of the cloud. The cloud storage researchers also focus more on the cryptographic techniques. The data is provided with security by the usage of these above discussed cryptographic techniques. The security properties like confidentiality, integrity, reliability can be achieved.This paper describes various cryptographic techniques that can be used in cloud computing environment. Thus the data can be securely shared with the authorized users by adopting the cryptographic techniques.

7. Reference

1. Patil DH, Bhavsar RR, Thorve AS. Data security over cloud. IJCA Proceedings on Emerging Trends in Computer Science and Information Technology (ETCSIT2012) etcsit1001. 2012; ETCSIT (5):11–4
2. Bessani A, Correia M, Quaresma B, et al. DEPSKY: dependable and secure storage in a cloud-of-clouds. 6th Conference on Computer Systems (EuroSys'11). 2011. p. 31–46
3. Kamara S, Lauter K. Cryptographic cloud storage. 14th International Conference on Cryptography and Data Security, LNCS, IFCA/Springer-Verlag. 2010, 6054. p. 136–49.
4. Wagner D, Song D, Perrig A. Practical techniques for searching on encrypted data. IEEE Symposium on Research in Security and Privacy, IEEE Computer Society. 2000; 44–55.
5. Goh E-J. Technical Report 2003/216, IACR ePrint Cryptography Archive, 2003. Available from: http://eprint.iacr.org/2003/216.
6. Chang Y, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. In: Ioannidis J, Keromytis A, Yung M, editors. Applied Cryptography and Network Security (ACNS '05), Lecture Notes in Computer Science. Springer. 2005; 3531:442–55.
7. Curtmola R, Garay J, Kamara S, Ostrovsky R. Searchable symmetric encryption: Improved definitions and efficient constructions. In: Juels A, Wright R, De Capitani di Vimercati S, editors. ACM Conference on Computer and Communications Security (CCS '06), ACM. 2006. p. 79–88.
8. Golle P, Staddon J, Waters B. Secure conjunctive keyword search over encrypted data. In: Jakobsson M, Yung M, Zhou J, editors. Applied Cryptography and Network Security Conference (ACNS '04), Lecture Notes in Computer Science, Springer. 2004; 3089:31–45.
9. Boneh D, di Crescenzo G, Ostrovsky R, Persiano G. Public key encryption with keyword search. In: Cachin C, Camenisch J, editors. Advances in Cryptology – EUROCRYPT '04, Lecture Notes in Computer Science, Springer, 2004; 3027:506–22.
10. Abdalla M, Bellare M, Catalano D, Kiltz E, Kohno T, Lange T, Lee JM, Neven G, Paillier P, Shi H. Searchable encryption revisited: Consistency properties, relation toanonymous IBE, and extensions. In: Shoup V, editor. Advances in Cryptology, CRYPTO'05, Lecture Notes in Computer Science, Springer. 2005; 3621:205–22.
11. Park D, Kim K, Lee P. Public key encryption with conjunctive field keyword search. In: Lim CH, Yung M, editors. Workshop on Information Security Applications (WISA '04), Lecture Notes in Computer Science, Springer. 2004; 3325:73–86.
12. Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In Theory of Cryptography Conference (TCC '07), Lecture Notes in Computer Science, Springer. 2007; 4392:535–54.
13. Shi E, Bethencourt J, Chan T, Song D, Perrig A. Multidimensional range query over encrypted data. IEEE Symposium on Security and Privacy, IEEE Computer Society, Washington, DC, USA. 2007; 350–64.
14. Baek J, Safavi-Naini R, Susilo W. On the integration of public key data encryption and public key encryption with keyword search. International Conference on Information Security (ISC '06), Lecture Notes in Computer Science. Springer. 2006; 4176.
15. Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited. International conference on Computational Science and its Applications, Springer-Verlag. 2008; 1249–59.
16. Fuhr T, Paillier P. Decryptable searchable encryption. International Conference on Provable Security, Lecture Notes in Computer Science, Springer, 2007; 4784:228–36.
17. Boneh D, Kushilevitz E, Ostrovsky R, Skeith W. Public-key encryption that allowsPIR queries. In: Menezes A, editor.

Advances in Cryptology, CRYPTO '07, Lecture Notes in Computer Science, Springer. 2007; 4622:50–67.
18. Byun JW, Rhee HS, Park H-A, Lee DH. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In Secure Data Management. Lecture Notes in Computer Science, Springer. 2006; 4165:75–83.
19. Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing. Proceedings of Cryptography 2001, LNCS, Springer-Verlag. 2001; 2139:213–29.
20. Fontaine C, Galand F. A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security 2007. 2007 Jan; 1–15.
21. Shamir A. Identity-Based Cryptosystems and Signature Schemes. In Proceedings of Cryptography 1984, LNCS. Springer-Verlag. 1985; 196:47–53.
22. Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM. 2007; 203.
23. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data, CCS '06. 2006; 89–98.
24. Yu S, Wan C, Ren K, Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. Proceedings of IEEE Communications Society for publication. 2010; 534–42
25. Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption. Proceedings of IEEE Symposium Security and Privacy. 2007; 321–34.
26. Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Public Key Cryptography. 2011; 53–70.
27. RajaSekhar B, Kumar S, Swathi Reddy L, PoornaChandar V. CP-ABE Based Encryption for Secured Cloud Storage Acces. International Journal of Scientific and Engineering Research. 2012; 3(9).
28. Chase M. Multi-authority attribute based encryption. Proceedings of the Theory of Cryptography Conference. 2007; 515–34.
29. Chase M, Chow S. Improving privacy and security in multi-authority attribute-based encryption. Cloud Computing Security. 2009; 121–30.
30. Jain N, Kaur G. Implementing DES Algorithm in Cloud for Data Security, VSRD-IJCSIT. 2012; 2(4):316–21.
31. Arockiam L, Monikandan S. Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering. 2013 Aug; 2(8).