A survey on attribute based encryption techniques in data security using cloud environment

Article *in* Journal of Advanced Research in Dynamical and Control Systems · January 2018

CITATIONS
2

READS
660

2 authors, including:

C. Bagyalakshmi
Hindustan institute of technology and science
7 PUBLICATIONS **26** CITATIONS

SEE PROFILE

A survey on attribute based encryption techniques in data security using cloud environment

C. Bagyalakshmi[1*], E.S. Samundeeswari[2]

[1]*Research Scholar, Department of Computer Science, Vellalar College for Women.*
[2]*Associate Professor, Department of Computer Science, Vellalar College for Women.*
**Corresponding author E-mail:bagyachithra@gmail.com*

Abstract

Cloud computing is a transformative computing paradigm that involves delivering applications and services over the internet. It is a pay-per-use model to the users and user can either transfer the file or share the data through internet. It also provides software and hardware installation by it, hence user can access or store the data without any installation requirements. But the most challenging phenomena in cloud environment is data security as users need proper security aspects to handle access or storage of data. There exists many cryptography techniques for data security. Cryptography techniques uses private and public keys that are used for exchanging information between client and server over the internet. The key based cryptographic techniques are classified into Symmetric key encryption and Asymmetric key encryption. Asymmetric key encryption are classified into Identity Based Encryption (IBE) and Attribute based Encryption (ABE).This paper focuses on one of the asymmetric key encryption technique ABE and about it types.

Keywords: *Encryption, decryption, ABE, CP-ABE, KP-ABE.*

1. Introduction

Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. Cloud computing technology is based on pay-as-you-go pricing model over internet.

1.1 Deployment modes of cloud

Four cloud deployment models (Figure 1) available are private cloud, public cloud, hybrid cloud and community cloud.

Private cloud

Private cloud infrastructure is operated for exclusive use of a single organization. They are suitable for applications where security is very important and organizations that want to have very tight control over the data.

Public cloud

Public cloud services are available to the general public or a large group of companies. The cloud resources are shared among different users[1].There are certain limitations in public cloud towards security and construction. Public cloud is not suitable for the organizations using sensitive data. The cloud services are provided by a third-party cloud provider like Amazon Web Service (AWS),Microsoft Azure, Google Cloud Platform, Adobe, VMware, IBM Cloud, Rackspace, Red Hat, Salesforce, Oracle Cloud, SAP, Verizon Cloud, Navisite, Dropbox and Egnyte.

Hybrid cloud

Hybrid cloud combines the services of multiple clouds. Hybrid clouds are suited for organizations that want to take advantage of secured application and data hosting on a private cloud, and at the same time benefit from cost savings by hosting shared applications and data in public clouds.

Community cloud

The cloud services are shared by several organizations that have the same policy and compliance considerations. Community cloud suited for organizations that want access to the same application and data, and want the cloud costs to be shared with larger group.

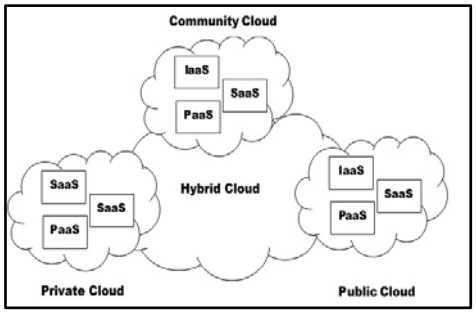

Figure 1: Cloud Deployment Models

Received: 5 Feb 2018/Accepted: 15 Mar 2018

1.2. Cloud service models

Cloud computing service models (Figure 2) are offered to users in different forms based on the type of services provided.

Software as a service (SaaS)

SaaS provides the users a complete software application or the user interface to the sufficient application itself [3].Applications are provided to the user through a thin client interface (e.g browser)SaaS applications are platform independent and can be accessed from various client devices such as workstations, laptop, tablets and smartphone, running different operating systems.

Platform as a service (PaaS)

PaaS provides the users the capability to develop and deploy application in the cloud using the development tools, Application Programming Interfaces (APIs), software libraries and services. The users, themselves, are responsible for developing, deploying, configuring and managing applications on the cloud infrastructure.

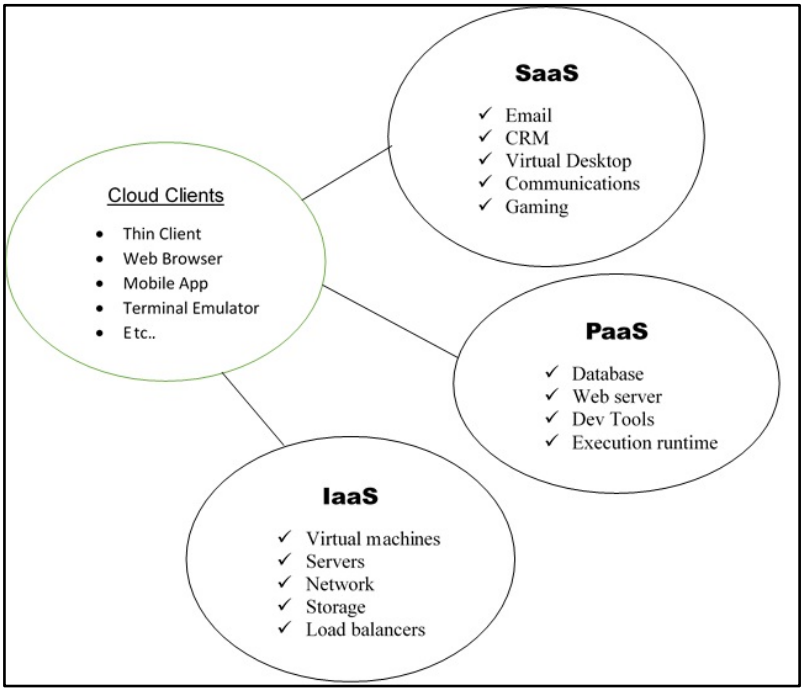

Figure 2: Cloud services Models

Infrastructure as a service (IaaS)

IaaS provides the users the capability to provision computing and storage resources. The cloud service provider manages the underlying infrastructure. Virtual resources provisioned by the users are billed on a pay-per-use paradigm.

1.3 Data security in cloud

More and more organizations are moving their applications and associated data to cloud to reduce costs, operational and maintenance overheads. Securing data in the cloud is critical for cloud applications as the data flows from applications to storage and vice versa. Cloud applications deals with both data at rest and data in motion [10]. Data at rest is the data that is stored in database in the form of tables/records. Data at rest is secured by encryption techniques. Data in motion is the data flowing between a client and a server over an insecure network andit is important to ensure data confidentiality and integrity.

Encryption is the process of converting data from its original form (plaintext) to a scrambled form (ciphertext). Decryption converts data from ciphertext to plaintext [4]. Encryption can be of two types: Symmetric Encryption and Asymmetric Encryption (public key algorithms). Symmetric encryption uses the same key for both encryption and decryption. The secret key is shared between the sender and receiver. Popular symmetric encryption algorithms include: AES (Advance Encryption Standard), Twofish, Blowfish, DES (Data Encryption Standard), 3DES (Triple DES) and RC5 (Rivest Cipher). Asymmetric encryption uses two keys, one for encryption (public key) and another for decryption (private key). The two keys are linked to each other. Popular asymmetric encryption algorithms include: RSA (Rivest, Shamir and Adleman), DSA (Digital Signature Standard) and Diffie-Hellman.

Public key cryptography is a traditional method of encryption and now it is upgraded to next level of security concerns so public key cryptography is called as Functional Encryption (FE) method [5]. In FE method, a secret key allows one to learn a function of what the ciphertext is encrypting. FE is classified into two types: Identity Based Encryption (IBE) and Attribute Based Encryption (ABE).

Identity Based Encryption (IBE) is a public key encryption technique based on the unique information and identity of the user [6].In this technique users were identified by their username, email, mobile no, etc., IBE allows any party to generate a public key from a known identity value based on ASCII string.

Received: 5 Feb 2018/Accepted: 15 Mar 2018

1.4 Attribute based encryption (ABE)

Attribute Based Encryption (ABE) is the recent method for public-key encryption in which the user's secret key and ciphertext are governed by the attributes. Public-key cryptography is based on ABE from IBE, so ABE allows the public key as an arbitrary string. ABE defines the identity as not atomic but as a set of attributes, these attributes are represented as regular ASCII strings [7]. ABE gives advance trusted sharing and access of data confidentially and allows a policy or attributes without prior knowledge of the recipient. ABE attributes are accessed by the tree-based access structure format, it is based on AND and OR operations. In the tree-based access structure, encrypter specifies the attributes to decrypt the data. ABE should satisfy the given set of attributes to decrypt the data. Hence ABE reduces the number of key used and thus makes encryption and decryption process faster.

2. Types of attribute based encryption

Various security aspects of cloud environment are confidentiality, access availability and integrity. Security is very important because cyber theft spreads through internet, hence it is important to protect our system using cryptographic method. Attribute-based encryption (ABE) is reasonably a new method, it is based on the concept of public-key cryptography where the private key is used to decrypt data [8]. ABE is classified into two schemes Ciphertext-Policy (CP-ABE) and Key-policy (KP-ABE). ABE depends on certain user attributes such as position, place of residence, type of account etc.

2.1 Ciphertext-policy ABE (CP-ABE)

The client privatekeys are based on set of attributes and ciphertext for specified common attributes within the system (Figure 3). A specific key can decrypt the actual ciphertext only if there is a counterpart between the attributes of cipher text and user's key [9].

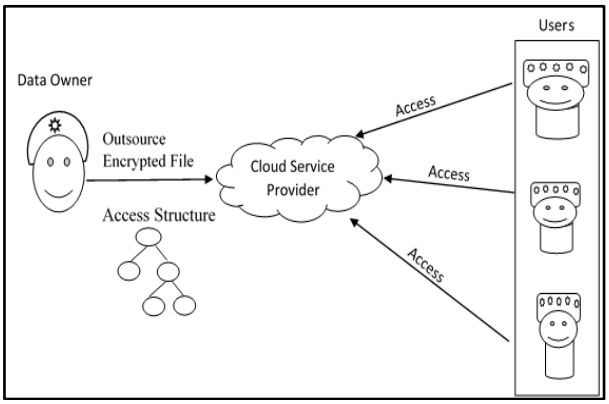

Figure 3: CP-ABE Scheme

The decryption parameters are private key PK, ciphertext CT, access policy A, secret key SK and private key for a set of attributes S. The fundamental schemes (Figure 4) of CP-ABE are Setup, Encrypt, Keygen and Decrypt.

CP-ABE schemes are described below,

1. **Setup:** An input security parameter k to generate a public key PK and master's secret key MK.
2. **Encrypt:** Encrypts a file according to a policy, which is an expression in terms of attributes. The input parameters like public key PK, message M, and an access structure T provide an output as a ciphertext CT.
3. **Key-Gen:** Set of attributes are associated with user and the master secret key MK as an input and secret key SK as anoutput that enables the user to decrypt a message in the way of encrypted under an access tree structure T.
4. **Decrypt:** Input ciphertext CT and a secret key SK for an attributes set. It returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

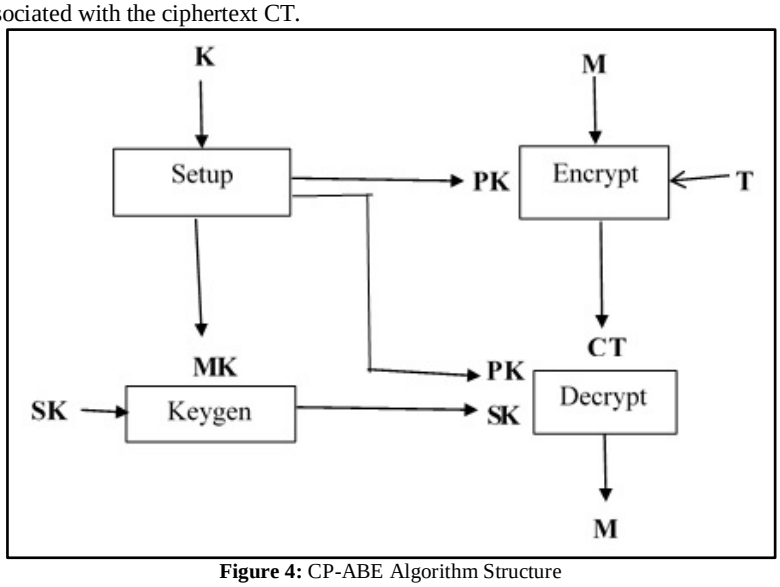

Figure 4: CP-ABE Algorithm Structure

Received: 5 Feb 2018/Accepted: 15 Mar 2018

Limitations of CP-ABE

CP-ABE has a restriction in terms of specifying policies, user management attributes and denials of most CP-ABE schemes. The schemes are still not satisfying the enterprise requirements of access control which require considerable flexibility and efficiency. In decryption keys only support user attributes, those keys are organized logically as a single set. The users can only use all possible combinations of attributes in a single set of keys issued to fulfill their policies.

2.2 Key-policy ABE (KP-ABE)

The Key Policy Attribute Based Encryption (KP-ABE) is an important class of ABE (Figure 5). The ciphertext has labeled with set of attributes, private keys are associated with access structures that controls ciphertext so user which can able to decrypt. The encrypted data was described by a set of attributes to get access with private key of user [5]. If a set of data matches through attributes in the structure of access to the users private key, so that the data can be decrypted. The encryption schemes(Figure 6)are different from the original version of the ABE generating the private key. User's private key was created by allowing the structure for required access.

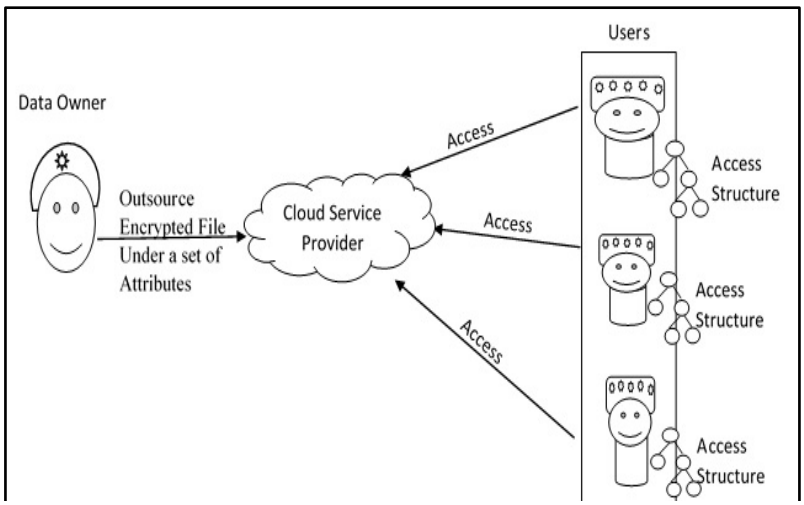

Figure 5: KP-ABE Scheme

KP-ABE schemes are explained below,

1. **Setup:** An input security parameter k to generate the public key PK and master secret key MK.
2. **Encryption:** An input parameter message M and public key PK to generate the ciphertext CT as output.
3. **Key Generation:** An access structure T, master secret key MK as an input and secret key SK as output. Key generation scheme permits the user to decrypt a message encrypted under a set of attributes if and only if equals T.
4. **Decryption:** The input users of secret key SK for Access structure T and the ciphertext CT, which was encrypted under the attribute set where it produces the message M as output. Output is produced if and only if the attribute set satisfies the user's access structure T.

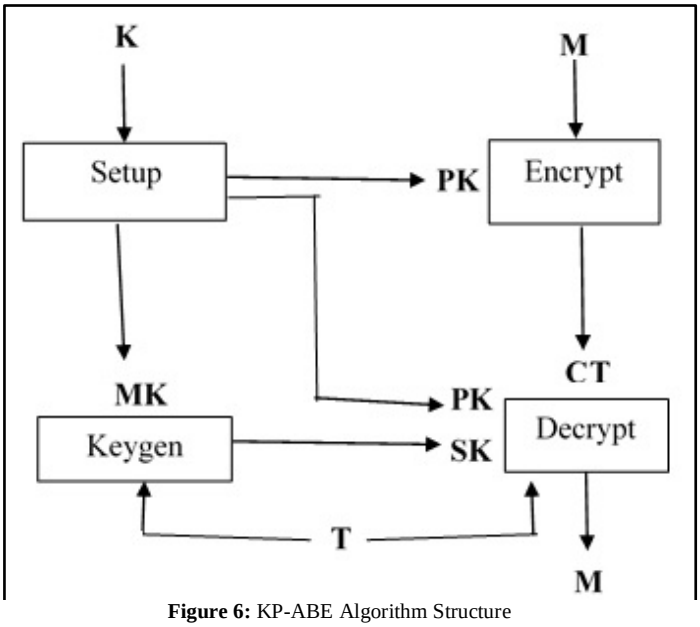

Figure 6: KP-ABE Algorithm Structure

Limitations of KP-ABE

The Encrypter cannot resolve who can decrypt the encrypted data. Encrypter can choose only descriptive attributes for the data, hence no choice but to trust the key issuer. KP-ABE not naturally suitable for certain applications. This scheme supports user secret key accountability and it provides fine grained access but has no longer with flexibility and scalability.

Received: 5 Feb 2018/Accepted: 15 Mar 2018

3. Literature survey on cloud data security

The following (Table 1) shows the review on cloud data security based on different literature.

Table 1: Review on Cloud Data Security

Title	Techniques Used	Summary
CP-ABE Based Encryption for Secured Cloud Storage Access, (2012), B. Raja Sekhar, et.al.,[6]	CP-ABE	CP-ABE enables the data owners to define their own access policies over the user attributes and enforce those policies on data to be distributed. CP-ABE based secured cloud storage model uses the methods like key generation centre, data storing centre, data owner and user. Encryption and Decryption is based on the policy specified over the attributes.
Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview (2013), Anup R. Nimje, et.al.,[1]	KP-ABE	The secret key and ciphertext are connected with a set of attributes. ABE can be further modified into KP-ABE that offers fine grained access control. KP-ABE attribute policies are associated with keys and data is associated with the attributes. In which data can be decrypted by the policy satisfied by the attributes. Ciphertext is related with an access tree structure in which each user secret key is rooted with a set of attributes.
A Key-Policy Attribute-Based Broadcast Encryption (2013), Jin Sun, et.al., [3]	Key Policy Attribute Based Broadcast Encryption (KP-ABBE)	KP-ABBE has been applied extensively in the area of access control. It is based on the broadcast encryption scheme with wide real world applications. The size of attribute set used for encryption has a large attribute universe. Attribute set supports the selective security group with static, generically secure assumptions in Composite order. Attribute set of bilinear groups does not depend on the number of queries made by the attacker. KP-ABBE supports LSSS (Linear secret- sharing schemes) matrices as access structure with secret keys, also provides delegation capabilities to users additionally.
Comparison of Security Algorithms in Cloud Computing (2015), Dinesh Devkota et.al.,[2]	MIST	This paper deals with MIST algorithm based cloud security for aerospace applications. MIST is a newly developed technique for security in cloud-based server. In this algorithm relevance of cloud systems in gathering sensitive information for aerospace platform. MIST technique prevents common attacks through password recovery, retrieval, authentication and hardening systems. In case of security breaches, it would be advantageous to include the capabilities of the MIST algorithm.
P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for Clouds (2016), Lifeng Li,et.al., [4]	P-CP-ABE (Parallelize Ciphertext Policy ABE) Method, AES, Multithreading	Significant components such as key generation and encryption/decryption process are parallelized by multithreading technique. The original Cipher Block Chaining (CBC)operation mode of AES is replaced by Counter (CTR) mode. New AES encryption mode of operation is adopted for further performance gain.
A Secured Storage using AES Algorithm and Role Based Access in Cloud (2017), M. Saraswathi, et.al.,[7]	Role Based Access Control	Role based access control provides two-factor protection mechanism to enhance the confidentiality of outsourced data. If a user wants to recover the outsourced data, user is required to hold sufficient attribute secret keys with respect to the access policy and authorization key. It provides the user-level revocation for data owner in attribute-based data access control systems.
A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing (2017),SphurtiAtram, et.al., [9]	File Hierarchy ABE Scheme	The layered access structures are integrated into a single access structure. The hierarchical files are encrypted with integrated access structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage time and cost of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption.
An Improved Integrated Hash and Attributed based Encryption Model on High Dimensional Data in Cloud Environment (2017), Satheesh K S V A Kavuriet.al., [8]	ABE Multi-File Data Partition Algorithm. Parallel multi-doc based Hash Algorithm (PMHA).	A novel multi-user based privacy protection mechanism need to design and improve the privacy protection on high dimensional data. Integrity algorithm with attribute based encryption model is implemented to ensure confidentiality for high dimensional data security on cloud storage. The main objective of the model is to store, transmit and retrieve the high dimensional cloud data with low computational time and high security. Experimental results of the proposed model has high data scalability, less computational time and low memory usage compared to traditional cloud based privacy protection models.
Secure Framework for Data Security in Cloud Computing (2018), Nishit Mishra et.al., [5]	AES	Storing information in the cloud could be more agile and difficult to break in. The proposed model will help in securing cloud databases and servers by encrypting the information and credentials. The combination of symmetric algorithm and XOR operation with message digest makes the encryption stronger. There is a central key distribution center (CKDC) which stores all the unique keys generated. Proposed method uses very complex calculations which are difficult for an attacker to solve in a given time, hence the attack can be stopped and prevented.

4. Conclusion

Security is a more important issue in cloud environment so the user data must be secured, in order to recover the data various security algorithms are required. More number of users can access resources from cloud environment, hacker may also attack the data along with the user. In order to avoid hacking, data can be protected in secured mode from the internet. Data security can be enhanced by using

Received: 5 Feb 2018/Accepted: 15 Mar 2018

symmetric and asymmetric algorithms in networks. Asymmetric algorithm integrated with ABE may be used for improving the cloud data security. This paper reviewed about cloud data security based on different types of ABE.

References

[1] Anup RN, Gaikwad VT & Datir HN, "Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview", *International Journal of Computer Trends and Technology*, Vol.4, No. 3, (2013), pp. 419-423.

[2] Devkota D, Prashant G, John B & Ihssan A, "Comparison of security algorithms in cloud computing", *IEEE Conference on Aerospace*, (2015), pp.1-7.

[3] Jin S, Yupu H & Leyou Z, "A Key-Policy Attribute-Based Broadcast Encryption", *International Arab Journal of Information Technology*, Vol.10, No.5, (2013), pp.444-453.

[4] Li L, Xiaowan C, Hai J, Zhongwen L & Kuan CL, "P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds", *17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*,(2016), pp.575-580.

[5] Nishit M, Tarun KS, Varun S & Vrince V, "Secure Framework for Data Security in Cloud Computing", *Advances in Intelligent Systems and Computing (Springer)*, (2018), pp.61-71.

[6] Raja Sekhar B, Sunil Kumar B, Swathi Reddy L & PoornaChandar V, "CP-ABE Based Encryption for Secured Cloud Storage Access", *International Journal of Scientific & Engineering Research*, Vol.3, No.9, (2012), pp. 1-5.

[7] Saraswathi M & Bhuvaneswari T, "A Secured Storage using AES Algorithm and Role Based Access in Cloud", *IJSRSET*, Vol.3, No.5, (2017), pp.511-515.

[8] Satheesh KS Kavuri VA, Gangadhara RK & Basaveswararao B, "An Improved Integrated Hash and Attributed based Encryption Model on High Dimensional Data in Cloud Environment", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.7, No.2, (2017), pp.950-960.

[9] SphurtiAtram NRB, "A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing", *International Journal of Computer Science and Mobile Computing*, Vol.6, No.5, (2017), pp. 260-266.

[10] Bahga A & Vijay M, *Cloud Computing: A Hands-On Approach*. Create Space Independent Publishing Platform, (2013).

Received: 5 Feb 2018/Accepted: 15 Mar 2018