ISSN:2229-6093

IJCTA

Mehak Jain et al, International Journal of Computer Technology & Applications,Vol 7(6),759-767

Analysis of various Security Models in Cloud Computing

Mehak Jain
Undergraduate student,
BVCOE, New Delhi, India
mehak_jain13@yahoo.com

Rachna Jain
Assistant Professor, CSE department
BVCOE, New Delhi, India
rachna.jain@bharatividyapeeth.edu

Deepika Kumar
Assistant Professor, CSE department
BVCOE, New Delhi,
deepika.kumar@bharatividyapeeth.edu

Abstract

Cloud Computing is an upcoming computing technology wherein users can access various services such as IaaS, PaaS, SaaS in a pay as you go model. Over the years, the numbers of users using cloud services has exponentially increased owing to the benefits offered by it. These benefits include universal access, unlimited storage, scalability of resources, increased collaboration, cloud has slowly revolutionized the way commercial computing works. However, it has its fair share of drawbacks. The most concerning disadvantage pertaining to it is the security of data stored on the cloud. Users may store their sensitive data like credit card details, log information for a company, personal information (social security number), etc. on the cloud. However, this data can be accessed by a third party and used for actions with malicious intent. Various security issues like integrity of data, unauthorized access, privacy, etc. are the foremost concern of every cloud user. In this paper, we have analysed a large number of proposed and implemented cloud security techniques. These techniques range from two and three tier architecture models to various frameworks. This paper discusses the key features, advantages and disadvantages of these techniques. A comparative analysis of these techniques has been conducted, further highlighting their benefits and drawbacks.

Keywords - Cloud Computing, Security, Data Integrity, Encryption

1. Introduction

Cloud Computing basically refers to the applications that are provided as services as well as the system software and hardware in the data centres[1].According to NSIT, Cloud Computing is a model that enables convenient and on-demand network access to a shared pool of configurable computing resources. These resources can then be rapidly provisioned and released with minimal management effort[2].

Cloud Computing can be divided up into three service models, namely IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). Under IaaS model, infrastructure elements such as storage, operating system etc. are provided to the user. PaaS model provides tools, like libraries, database management system, etc., required by the end user to develop various applications. Under SaaS model, the end user is granted access to software application hosted by the CSP (cloud service provider) over the Internet.

There are four deployment models in cloud, namely private cloud, public cloud, community cloud and hybrid cloud. In public cloud the infrastructure can be used by anyone while in private cloud infrastructure can be used only by a single organization. Community cloud is an extension of private cloud where the cloud is owned, used and managed by more than one organization and hybrid cloud is a composition of two or more than two distinct cloud infrastructures which can be public, private and community.

The growing popularity of cloud computing can be accredited to the following advantages offered[3] -

1. On Demand Self-Service: The service provided is automatic and does not require human interaction.
2. Broad Network Access: Services are accessed over the network and hence can be used for any device and any location.
3. Resource Pooling: Using multi-tenant model, CSP's resources are pooled to serve multiple customers.
4. Rapid Elasticity: The resources can be rapidly scaled (inward or outward) depending on the demand.
5. Measured Service: The usage of various resources is monitored, checked and reported by the CSP.

This paper has been divided into 5 sections. Section I is the current section containing the introduction .Section II deals with security issues in cloud security. In section III, we have explored related work done in this field. Section IV provides a comparative analysis of all the security techniques discussed. Section V deals with conclusion of the paper.

2. Cloud Security Issues

Cloud has a fair share of advantages to its credit which have been discussed in the previous section. However, it has quite a few issues which have deterred various organizations from using cloud for storing its data. Some of these security issues have been discussed below.

- Data locality: In cloud computing, the users are unaware of where their data is being stored. This can lead to problems especially in case of sensitive data[3].
- Data Segregation: One of the main advantages of cloud computing is resource pooling. However, when data of many users reside at the same location, intrusion of a user's data by another becomes possible[3].
- Brute Force attack: Clouds that are secured using passwords only are vulnerable to Brute Force attack. In Brute Force Attack, the attacker tries different passwords till the right password is found.
- DOS and DDOS attacks: DOS (Denial of Service) and DDOS (Distributed Denial of Service) attacks overwhelm the server resources so that genuine users cannot access the cloud[4].
- Cloud Malware Injection Attack: In this attack, attacker injects a virtual machine or service implementation into the cloud system, tricking the cloud into redirecting user requests to the service or machine, thus gaining access to the user's data and activities[5].
- Man in the Middle Cryptographic Attacks: The attacker places himself in the communication path between two users thus being able to intercept and modify communications[5].
- Service Availability: Sometimes, due to excess traffic or some technical difficulties, the cloud services are inaccessible. This may hinder the proper working of an organization leading to various problems.
- Data loss: Data loss, due to hardware malfunction or natural disaster, without any kind of backup can become a major threat for an organization storing essential data on the cloud.

3. RELATED WORK

Various studies and researches are done in the field of cloud security. Some of these have been discussed in the following section.

Joshi M et al[6] proposed the architecture for a virtual private storage service which is based on cryptographic techniques on both consumer and enterprise level. Comprising of data processor, data verifier, token generator and a credential generator, the architecture ensures the confidentiality as well as the integrity of data while facilitating secure data sharing. However, the time required for encrypting and decrypting the data and generating various keys and credentials will reduce speed of transfer between client and server.

Ahmadi M.et al[7] proposed a user authentication model where two encryption procedures AES and RSA have been established in an Agent(an independent middleware between the end-user and

cloud servers) to perform various functions like user authentication, access control, etc. in cloud servers. AES is used as a symmetric cryptography algorithm in cloud servers and RSA is used as an asymmetric cryptography algorithm in Agent servers. The model can protect from attacks like Man in the Middle attack and Discrete Logarithm attack. The private key of the data is encrypted by the private key of the user and it is sent to the server. In the cloud server, the private key of the data is decrypted by the public key of the user, the AES main key is decrypted by the private key of data, and the data is decrypted by the AES main key.

Naik NV et al[8] proposed the introduction of third party auditor in between the client and the cloud server to help the client to frequently check the integrity of data stored in cloud. They proposed three different models. In the first model, the client uploaded the data blocks and calculated MAC of data to the server and stored the user's secret key to Third Party Auditor (TPA). The TPA then retrieved data blocks & the secret key was used to check integrity of the data in the cloud. The second model used Homomorphic linear authentication (HLA). HLA generated verification metadata from the user's data file that authenticated the correctness of a data block. In the third model, Challenge–handshake authentication protocol (CHAP) was used for authentication of data. Since the whole data infrastructure management in cloud is done by a TPA, it was necessary to hide the entire data from the TPA and only expose parts of it. Thus, HLA technique was used which permits the auditor to verify the genuineness of the data in the cloud without fetching the whole data.

Veeraragavan N et al[9] put forward a framework VEARAaaS consisting of three components, Authenticator, Encryptor and Key generator. Authenticator is used for verifying the user, the encryptor is used to encrypt the registration data of the user prior to storing the data and Key Generator is used to generate a key for encryption and authentication service. Additionally, Authenticator consists of two services UIDaaS and DIUaaS for all types of users and users requiring high end security respectively. Tackling the issue of cloud security, the framework has different Authentication as a Service (AaaS) to protect the data.

Kumar S et al[10] put forward a two tier authentication scheme using the user's personal device having a unique id. The first tier includes username and password authentication. In the second tier of authentication, One-Time Password (OTP) is sent from the server to the registered device. The user must enter the password in registered personal device's interface and send it back to the cloud server to gain entry to the cloud. Thus, the user is authenticated at the second tier using password and device's id. The advantage of this scheme is that the probability of success of hacking is significantly less than one-tier authentication. But, it mandates the use of additional hardware irrespective of whether the user possesses such a device or not. Furthermore, in case of theft of the concerned device the security of the user's cloud account gets compromised.

Sulochana V et al[11] proposed a puzzle based authentication scheme in which the user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and the user gets successfully authenticated. The main advantage of the scheme lies in the fact that the overall success rate of attackers is 0.095 since it is difficult to manipulate the time and sequence of image blocks to solve the puzzle. However, the time taken and the sequence followed by the user to solve the puzzle may vary from time to time. Thus, there may arise a scenario when a registered user is unable to login, thus creating complications.

Yan L, Rong C, Zhao G.[12] adopted a federated identity management along with hierarchical identity-based cryptography (HIBC) for both mutual authentication and key distribution. Federated identity management is a method for different establishments to share user and service identity. Using this, users and servers have their unique identity which are hierarchical in nature. Hence, user needs to authenticate only once to the system and this identity can be further used in different networks. In HIBC, a root PKG generates and distributes private keys for the domain-level PKGs. These domain-level PKGs further generate and distribute private keys to the users in their own domain. HIBC is better than Identity-based cryptography since it reduces the key-escrow problem faced by Identity-based cryptography. Further, HIBC is suitable for a large scale network

since it reduces workload of root PKG by distributing the work to domain level PKGs.

Goswani B et al[13] proposed a three-stage secured algorithm. The first stage includes shuffling of data using the linear congruential method followed by arranging the data in a matrix form. In the second stage, the matrix is transversed in different forms like helical, spiral, etc. Finally, the third stage deals with generating a system of non-homogeneous linear equations from which private keys are generated. The strength of the algorithm lies in the fact that it has constant complexity. Further, the security of the entire system is based on solving system of equations over the ring of integers which comes under the NP-Complete problems.

Squicciarini A, Sundareswaran S, Lin D.[14] designed a three-tier data protection architecture which has been used to accommodate different levels of privacy concerns by users. They developed a novel portable data binding technique to make sure that there is strong enforcement of users' privacy requirements. The architecture provides three degrees of privacy protection. Using the data policies provided by the user, a request analyser selects one of the three, strong, medium or low protection. It outputs JAR files which contain both data and policies. Portable data binding then enforces the strategies adopted by these three components. It defines Indexing Prevention Policy(IPP) which specifies access rights that a service provider will obtain to deal with the user's data. Nested JARs are utilised to bind the user's data with the corresponding IPP for the purpose of strong enforcement. The architecture ensures that there is full control from the user end and servers' authentication is achieved by leveraging the SAML infrastructure. Further, it introduces very less overhead.

Nagamani V et al[15] contemplated a design in which data is stored on the cloud in an encrypted format and a set of secret keys, implementing variable size cryptosystem, are used as a single aggregate key to decrypt the data. A key hierarchical structure is used for generation of key. The data is searched for a set of attributes, these attributes are arranged in a hierarchical structure which is further used to generate the aggregate key. Further, the data can be shared with other users by simply sharing the aggregate key. Thus, this design allows users to securely access and share data without relying on a third party software. However, since the design relies on a one tier security model, any person with access to the aggregate key acquires access to the data.

Tirodkar S et al[16] proposed a two phase, 3 dimensional architecture for ensuring security of data on cloud. The first phase deals with encryption and classification of data into three protection rings, with the innermost protection ring, protection ring 1, containing the most sensitive data. This classification is based on the following factors, Confidentiality, Integrity and Availability .The second phase deals with data retrieval. Depending on the layer accessed, a different mechanism is used to verify the user's identity. The outermost ring, protection ring 3 is authenticated using username and password, protection ring 2 uses graphical password authentication and protection ring 1 is authenticated using an OTP sent to the user's device. Finally, the retrieved data is decrypted using the decryption key. The architecture provides security from DDOS attacks and data leakage. However, the introduction of OTP and use of hardware devices for authentication introduces complications.

Ullah S et al[17] set forth a two module architecture consisting of client and server module. The main purpose of the client model, consisting of Multi-Purpose Access Module, Split/Merge Module and Encryption Module is to verify the user and encrypt or decrypt data for storing and retrieving the data respectively. Similarly, the server module is responsible for storing both the public data in encrypted form and private data consisting of user credentials and secret keys. As a result, the data has multiple levels of security due to the of split and merge technique followed the encryption process thus making it more secure. Further, it ensures that in case of any unauthorized access, the data remains safe since it is in encrypted format. But, the split/merge technique along with encryption of data adds extra overhead thus increasing the time required to store and retrieve the data.

Shyamala MG et al[18] put forward a two module, multi-level authentication architecture to ensure confidentiality and integrity of data. The two modules i.e. client and cloud module can further be divided into components. The client module consists of the Encryption Component, Encryption

ISSN:2229-6093

Database and Decryption Component. The Encryption Component encrypts the data using AES encryption, the Encryption Database acts as a secured storage and the Decryption Component retrieves the original data using inverse cipher text. On the other hand, the cloud module is responsible for authentication the user using a two session password sent to the email id of user and mobile number simultaneously. Additionally, it stores public data, in encrypted form, and private data consisting of user credentials and secret keys. The proposed architecture is very simple and highly secure.

Singh M et al[19] proposed a two tier authentication process where the first tier uses traditional encryption decryption mechanism and in the second tier the user is required to perform a certain sequence of predetermined activities on the fake screen. These steps may be Menu Activity i.e. a sequence of menu clicks on a fake screen provided by the Cloud, Mouse Activity like mouse clicking or mouse movements or Text Field Activity. The technique is a secure method of storing sensitive data since the probability of breaking second tier authentication is very less. Further, it provides better mechanism to handle pressurized circumstances by adding the concept of a fake screen. However, it requires the user to remember the required pattern along with the credentials thus increasing the complexity for the user.

Agme VS et al[20] proposed a secure cloud system where the permission for a given file or document is dependent not only on the identity of the person but the file as well. The data is encrypted and stored on the cloud by the owner. When a user requests access to a file, the owner gets notified. An authorized user is granted permission and data which can then be decrypted using the private key owned by the user. Hence, the system ensured that the data is secure against collusion attack and DDOS attack. Furthermore, the access permissions is decided by the owner, thus making it more secure. On the downside, whenever a user wishes to access the data, the owner needs to authorize the data, thus requiring constant work on the owner's side.

Rewagad P et al[21] provided a three way mechanism ensuring authentication, data security as well as verification. The mechanism uses digital signature and Diffie Hellman algorithm for key generation along with AES encryption algorithm for encryption and decryption of data. In the scenario that a key in transmission is hacked, it is of no use because of the usage of Diffie Hellman key exchange. The key is useless without user's private key, which is beyond the access of the hacker.

Sarkar MK et al[22] came up with an idea to ensure data security on the cloud by storing user's data in the form of images. The architecture, consisting of user, CSP-1, CSP-2 and CSP3, aims at securing data-at-rest using the underlying concept of Stenography. CSP-1 contains a database which maintains records of file names, number of characters present etc. consisting of the images containing the data. CSP-2 stores the algorithm for data hiding and retrieving and all the computations or actions carried out by the user takes place in CSP-3. Hence, any unauthorized user cannot access the data, thus ensuring the security of data and protection from various threats.

Casola V et al[23] put forward a framework that enables the adoption of a pre-service SLA model. The framework consists of building a list of security mechanisms which implement a set of security policies and offering them as-a-service. Thus, the SLA's are tailored to the needs of the customer and the service offered. The implementation consists of SLA Automator, Broker and a Configuration Manager. The Automator is responsible for negotiating with the CSC(Cloud Service Customer) on one end and controlling the Broker on the other end . The Broker acquired the resources from CSP(Cloud Service Provider) and Configuration Manager automates application of agreed security concerns . Additionally, the entire implementation is free from user-intervention, thus complying with the main cloud computing principles.

Warhade RG et al[24] proposed a Identity based multi-cloud storage scheme(IBMCSS) where the data is split , encrypted and stored on multiple clouds . In this scheme, the data is first split into chunks, then each chunk is encrypted using AES algorithm and finally the data is stored on multiple clouds. Hence, the data owner does not need to trust a single CSP with security of the entire data. Furthermore, the access permission to data is bound to file and the identity of authorised access device.

The major development phases as proposed in the scheme are Registration module, Login module, FTP settings module, File Upload and Download Module, File Encryption Module and File Splitting and Clubbing Module. The main advantages of the scheme lies in the fact that it can protect against data theft attacks and maintain confidentiality of data. However, when data gets split into large number of chunks, the splitting and merging time becomes large, thus affecting the uploading and downloading time.

Jung T[25] presented a semianonymous privilege control scheme named AnonyControl along with fully anonymous AnonyControl-F scheme to prevent data and identity leakage. The scheme AnonyControl decentralizes the central authority which will limit the identity leakage and generalizes the file access control to the privilege control. Both these techniques, AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption. The main difference between AnonyControl and AnonyControl-F is that there is partial disclosure of information in AnonyControl whereas there is none in AnonyControl-F. However, as long as the introduced OT does not leak information about the transferred attributes, AnonyControl-F leaks as much as information as Anony-Control does. In this scheme, encryption policy is described with a tree known as privilege tree. A data file has several operations executable on itself, and each of them is allowed only to authorize users with different level of qualifications. Thus, the scheme requires several trees in every data file to verify users' identity and to grant them a privilege accordingly. The main advantage of the schemes is that it can tolerate up to $N-2$ authority compromise. Also, the detailed security and performance analysis that has been conducted shows that AnonyControl and AnonyControl-F is both secure and efficient for cloud storage system. Incase of AnonyControl-F, there is extra communication overhead.

Dong X et al[26] presented a secure cloud sharing service allowing the users dynamic access to their data. It uses ciphertext policy attribute-based encryption(CP-ABE) combined with identity based encryption(IBE) to ensure privacy of data , collusion resistance and full privacy-preserving . Furthermore, it also supports efficient and secure dynamic operations. It uses four algorithms: System initialization, Encryption, Key generation, Decryption. At the initialization phase, the data owner uses the System initialization algorithm to generate the system parameters for all system entities. He then employs Encryption algorithm to encrypt files with "attributes" and uploads them to the cloud. Using the Key generation algorithm, the data owner generates secret keys for each user, further delivering them. When retrieving data, users use Decryption algorithm to decrypt ciphertext if their attribute set matches with the file attributes. The proposed policy is secure under the generic bilinear group model in the random oracle model. Performance analysis under computational complexity, communication cost, cost of revocation operation and ciphertext size revealed that the proposed scheme has low overhead and is highly efficient.

4. Comparative Analysis

The following tables, Table 1 and Table 2, shows a comparative analysis of all the techniques discussed so far. Table 1 shows comparison of various security techniques on basis of CIA, where C stands for Confidentiality, I stands for Integrity and A stands for Availability. Similarly, Table 2 shows comparison of various security techniques on basis of different attacks. As can be seen in the tables, nearly all the techniques ensure confidentiality of data stored through it. However, when we look at the protection offered against various attacks, there is a sudden decrease in the number of techniques that offer protection. Only the Identity based multi-cloud storage scheme(IBMCSS)[24] offers protection against data theft attack and the puzzle based authentication scheme[11] offers protection from online attack.

ISSN:2229-6093

Reference No.	Ensures Confidentiality of data	Ensures Integrity of data	Ensures Availability of data
[6]	✓	✓	
[7]	✓		
[8]	✓	✓	
[9]	✓		
[10]	✓		
[11]	✓		
[12]	✓		
[13]	✓		
[14]	✓		
[15]	✓		
[16]	✓	✓	✓
[17]	✓	✓	
[18]	✓	✓	
[19]	✓		
[20]	✓		
[21]	✓		
[22]	✓		✓
[23]			
[24]	✓		
[25]	✓		
[26]	✓		

Table 1

Comparison of various security techniques on basis of CIA

Reference No.	Protection from Man in the Middle attack	Protection from DOS attack	Protection from DDOS attack	Protection from tampering attack	Protection from online attack	Protection from insider attack	Protection from collusion attack	Protection from data theft attack
[6]								
[7]	✓							
[8]		✓		✓				
[9]								
[10]								
[11]					✓			
[12]								
[13]								
[14]								
[15]								
[16]			✓					
[17]								
[18]								
[19]						✓		
[20]			✓				✓	
[21]								
[22]								
[23]		✓						
[24]								✓
[25]							✓	
[26]							✓	

Table 2

Comparison of various security Techniques on basis of different attacks

5. CONCLUSION

This paper has reviewed techniques and architectures for cloud security. According to our study multi-tier authentication techniques are more secure than a single-tier authentication technique having lower success rate of hacking. Additionally, all the above techniques have their own pros and cons. Each technique is lacking in one or the other criteria. Hence, no technique is able to fulfil all the set criteria and further work can be done in this field to improve them. Future work can be done to develop an architecture which is capable of protecting against various types of attacks as well as ensuring data confidentiality, integrity and availability.

6. REFERENCES

[1]Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM. 2010 Apr 1;53(4):50-8.

[2]Mell P, Grance T. The NIST definition of cloud computing.

[3]Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications. 2011 Jan 31;34(1):1-1.

[4]Kilari N, Sridaran R. An Overview of DDoS Attacks in Cloud Environment. International Journal of Advanced Networking & Applications. 2015 May 2.

[5]Singh A, Shrivastava M. Overview of attacks on cloud computing. International Journal of Engineering and Innovative Technology (IJEIT). 2012 Apr;1(4).

[6]Joshi M, Moudgil YS. Secure cloud storage. International Journal of Computer Science & Communication Networks. 2011 Oct;1(2):171-5.

[7]Ahmadi M, Vali M, Moghaddam F, Hakemi A, Madadipouya K. A Reliable User Authentication and Data Protection Model in Cloud Computing Environments. arXiv preprint arXiv:1508.01703. 2015 Aug 7.

[8]Naik NV, Priyanka D. Affording Greater Privacy in Cloud Storage Auditing with Random Masking Technique. International Journal of Research. 2016 Jul 25;3(11):946-50.

[9]Veeraragavan N, Arockiam L. A Novel Framework for Authentication as a Service (AaaS) in Public Cloud Environment.

[10]Kumar S, Ganpati A. Multi-authentication for cloud security: A framework. International Journal of Computer Science & Engineering Technology. 2014 Apr;5(4):295-303.

[11]Sulochana V, Parimelazhagan R. A puzzle based authentication scheme for cloud computing. International Journal of Computer Trends and. 2013 Dec:210-3.

[12]Yan L, Rong C, Zhao G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. InIEEE International Conference on Cloud Computing 2009 Dec 1 (pp. 167-177). Springer Berlin Heidelberg.

[13]Goswani B, Singh DS. Enhancing security in cloud computing using public key cryptography with matrices. International Journal of Engineering Research and Applications. 2012 Jul;2(4):339-44.

[14]Squicciarini A, Sundareswaran S, Lin D. Preventing information leakage from indexing in the cloud. In2010 IEEE 3rd International Conference on Cloud Computing 2010 Jul 5 (pp. 188-195). IEEE.

[15]Nagamani V, Rao VV, Rao MV. Secure Scalable Data Sharing in Cloud Storage using Randomized Key Aggregate Crypto System. Global Journal For Research Analysis. 2016 Jul 9;4(7).

[16]Tirodkar S, Baldawala Y, Ulane S, Jori A. Improved 3-Dimensional Security in Cloud Computing. arXiv preprint arXiv:1404.1836. 2014 Apr 7.

[17]Ullah S, Xuefeng Z. TCLOUD: A Trusted Storage Architecture for Cloud Computing. International Journal of Advanced Science and Technology. 2014 Feb;63:65-72.

[18]Shyamala MG, Narmada B, Nivetha SM. A Trusted Storage and Data Retrieval in Cloud Computing. History. 2015;34(154):43-7.

[19]Singh M, Singh S. Design and implementation of multi-tier authentication scheme in cloud. International Journal of Computer Science Issues. 2012 Sep;9(5):181-7.

[20]Agme VS, Lomte AC. Cloud Data Storage Security Enhancement Using Identity Based Encryption. Identity. 2014 Apr;3(4).

[21]Rewagad P, Pawar Y. Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. InCommunication Systems and Network Technologies (CSNT), 2013 International Conference on 2013 Apr 6 (pp. 437-439). IEEE.

[22]Sarkar MK, Chatterjee T. Enhancing Data Storage Security in Cloud Computing Through Steganography. International Journal on Network Security. 2014 Jan 1;5(1):13.

[23]Casola V, De Benedictis A, Modic J, Rak M, Villano U. Per-service Security SLA: a New Model for Security Management in Clouds. InEnabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2016 IEEE 25th International Conference on 2016 Jun (pp. 83-88). IEEE.

[24]Warhade RG, Vankudothu B. Enhancing Cloud Security Using Multicloud Architecture and Device Based Identity. In2015 7th International Conference on Emerging Trends in Engineering & Technology (ICETET) 2015 Nov 18 (pp. 34-39). IEEE.

[25]Jung T, Li XY, Wan Z, Wan M. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. IEEE Transactions on Information Forensics and Security. 2015 Jan;10(1):190-9.

[26]Dong X, Yu J, Luo Y, Chen Y, Xue G, Li M. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. computers & security. 2014 May 31;42:151-64.