Encryption Techniques in the Cloud

Khalid Alshafee ORCID 0000-0003-4478-8568

Abstract— Cryptography is critical and necessarily for the integrity as well as the security of data which is to be stored in the cloud. Here are numerous cryptographic methods applied for this purpose on some cloud which mainly protects the data as well as the applications on the cloud atmosphere. Specific security technique doesn't primarily use single encryption scheme rather it makes use of different encryption schemes for the encryption of the data and convert the data to unreadable format and later on decrypted using some unique key. Numerous encryption techniques by now are available for the protection of the data in the various application. The cryptographic schemes are considered necessary for the data confidentiality that is saved over the cloud. Cloud computing shares resources such as software, services, platform, and infrastructure for the clients. So using the cryptographic techniques within the cloud will ensure the data security and integrity which is mostly required in cloud atmosphere. In this research, different encryption techniques used in the cloud environment are analyzed to find which is most suitable in what capacity.

Index Terms— Cryptography, Cloud Computing, Cloud Computing Security, Cloud Computing Encryption, Virtualization Security, Virtualization Encryption, Virtual Desktop Security.

1 Introduction

Data privacy is crucial on shared resources or over internet and encryption generally plays a significant role in protecting data. The security issues are numerous in cloud computing and on the web in general, and various cryptography algorithms have been designed to protect the data not only at cloud level but also at the applications level on desktops. Cryptography mainly refers to a different science in which ciphers are designed particularly stream ciphers and block ciphers as well as the hash functions. Encryption is a technique in which the ordinary text is converted to some secret text for the protection and integrity of the text. Mainly two categories of the encryption algorithm are there: 1) symmetric algorithms including Triple DES, AES, DES and 2) symmetric algorithms also known as public key encryption algorithms including ECC, Diffie-Hellman and RSA and others. The main difference among the both is the way; keys are used. In the symmetric encryption, the sender of data and the receiver of data/information share a key, and it is usually a secret key. This secret key is later on used for the encryption as well as decryption of the messages. While on the other hand, in the asymmetric encryption, there are usually two keys: one for the encryption and is publically available while the other is for the decryption and is secret.

Cloud computing, in general, is a very leading technology and numerous businesses and corporates now are migrating towards it. The major bottleneck in the broad acceptance of the cloud technology is the lack of the proper security. The security in the cloud computing is vulnerable to numerous issues like legal compliance, process and physical security aspects, privacy and confidentiality, data integrity, access control and identity management, software platform and finally the virtualization infrastructure within the cloud. Cloud computing enables the individuals and organizations to work and make their work accessible from anywhere in the world, and the services and resources offered by the cloud are also on demand. Cloud computing also ensures the on-demand and appropriate access to the network resources like the services, applications as well as infrastructure (Grance, 2011).

Using the encryption techniques for the security in the cloud computing is important. In this research, the analysis of different encryption techniques which are in use in cloud computing security will be performed. Numerous security issues within the cloud computing will also be discussed here. Various encryption techniques by now are implemented to ensure the privacy and security in cloud atmosphere. Though only three techniques will be analyzed in this research.

2. Privacy Issues in Cloud Computing

2.1 The challenges of privacy

The challenges of privacy within the public cloud include privacy breaches, data loss, data retention, dynamic provisioning, trans-border flow of data, data proliferation, secondary use of data which may be unauthorized, and no user control (Benameur, 2010). Due to the geographically distributed cloud services and the service providers, so the customers' data is typically stored on the remote servers and hence the possibility of data theft is high in such distributed structure (Monjur Ahmed, 2014). Numerous challenges also include the insider's attack in which the people from within the domain of the cloud service providers are involved in breaching the security of the client's data (Behl, 2011). Distributed Denial of Services (DDoS) is another form of a security breach in which the networks and the servers generally are brought down to non-functioning state due to an unnecessary amount of traffic and as a result, the user gets denied of the requested services (L. Ertaul, 2010). Cloud is an atmosphere where there is always need to transfer a lot of data between the customer and the service provider requiring data to get firmly authenticate and authorize (R. Balasubramanian, 2012). While the challenges related to security include audit and multi-tenancy, no proper standardization, backup and availability, and control at the data lifecycle. Trust challenges are also there which means that weak trust relationship is present among the customer and cloud service provider (Mhammed Chraibi, 2013). The multi-tenancy architecture of cloud has also raised security issues

due to the resource sharing and pooling (B. Grobauer, 2011) (Ransome, 2009). Since the architecture of cloud is divided into three layers: SAAS, PAAS, IAAS so the SAAS is entirely totally dependent on the service provider so here the security issues may rise as the biggest problem (Viega, 2009). So mostly user is reliant on the SAAS provider for the security of his/her data (J. Ju, 2010). Virtualization feature of the cloud may also help in providing security to the multi-tenant structure of cloud (Singh, 2014). Cloud has also brought about the API level security threats as well (Petcu, 2013). Cloud being an atmosphere most heavily relying on virtualization, so the security risks of the virtual machines also need to be addressed in order to provide the tight security within the cloud (Arshad, 2013). Security issues within the cloud can also be classified within the levels as available in the cloud. Different types of the security solutions are provided depending on the kind of the security challenge. The security within the cloud is mainly grouped in a model which is comprised of seven different categories (Nelson Gonzalez, 2011). Those categories are data security, network security, virtualization, interface security, governance, legal and compliance issues. Mainly 14 security domains for the cloud computing are defined by Cloud Security Alliance (CSA) (CSA, 2011) and accordingly top 10 threats have also been identified by CSA as mentioned in the table below:

Domain No.	Security Domains	Guidance on
D1	Architectural Framework of Cloud Computing	Cloud conceptual framework
D2	Enterprise and Governance Risk Management	Implementation and identification of the appropriate organizational control, processes, and structures
D3	Legal Issues: Electronic and contracts discovery	Legal issues may be raised through moving of the data to cloud as well as issues in the services management within the cloud
D4	Audit and Compliance Management	Understanding of existing audit and compliance practices, processes and standards
D5	Data security and information management	Lifecycle of the data security for defining and evaluating the strategies of the data security in cloud
D6	Portability and Interoperability	Designing for interoperability and portability
D7	Disaster recovery, business continuity, and traditional security	Sharing the understanding of the traditional security within the cloud services
D8	Operations of data center	Remodeling and construction of the data centers within the cloud
D9	Incident response	Effective and efficient handling of the security incidents involving the cloud resources
D10	Application security	Following the practices, while migrating or developing of the applications to cloud
D11	Key and encryption management	Binding of the cryptographic operations as well as the key management to the corporate identity system
D12	Access, Entitlement, and Identity Management	Designing of common services in order to work independently to more ensure the removal of application without compromising the current information security procedures and policies
D13	Virtualization	Issues related to virtualization
D14	Security as Service	Providing security to the cloud and complete security systems within the cloud using cloud based applications and services

Table 1: Security Domains in Cloud Computing

Table 2 shows numerous security threats in the 14 different security domains within cloud

Threats	D1	D2	D3	D4	D5	D6	D7	D8	D9
Breach of data					√				
Loss of data					√				
Hijacking of account		√			√		√		√
Insecure APIs					V	√			√
Denial of Services (DoS)								√	√
Intruders		√			√				
Cloud services' abuse		√							√
Improper diligence		√	√					√	√
Shared re-	√				√				

source/technology issue														

Table 2: Mapping of Security Threat to Cloud Security Domains

2.2 Encryption Techniques Applied within Cloud Computing

Numerous encryption methods have been implemented in the cloud computing, and some of them are discussed here. Cryptography is the most common method by which the users can get authenticated as well as the communication system may also get authenticated (Yashpalsinh Jadeja, 2012).

2.2.1 Identity-Based Encryption

This technique mainly helps in certificate management and management of public key for the public key infrastructure (PKI) (Jin Li, 2015). Outsourcing computation here is put to the identity-based encryption while the same scheme for the server has also been proposed. The operation of the key generation is assigned to the Key Update Cloud Service Provider and then the left out operations are very simple (Jin Li, 2015). This scheme uses the public key cryptography where the server of some third party mainly uses the simple identifier like the e-mail addresses for the generation of the public key which can then be helpful in the decryption as well as encryption of the electronic messages. Such type of encryption technique by large reduce the complexity of whole encryption method and ease is provided for in fact the administrators and the users. Here for the searching, the symmetric encryption algorithm by large is used for the encryption of the plain text. The Identity-based signature scheme actually would be deterministic only if the signature on the message through the same user remains same always.

2.2.2 Attribute-Based Encryption (ABE)

This type of encryption, in general, has numerous forms. The most common one among them is cipher text attribute based and key attribute based encryption. Some researchers have also suggested a new attribute based encryption method with the hierarchical name attribute based encryption (Kaur, 2012). This latest one is compared by the researcher with the two previous types of attribute-based encryption techniques which were only ciphertext and key policy. User's private key mainly ensures access policy for the algorithm. The main difference between the latest and old attributed based encryptions techniques is that the old ones are mainly dependent on the access policy. In the key policy attribute based encryption, cipher text gets attached to some attributes set and then gives the owner of the data the policy and key pair. The whole message then gets decrypted only if the attribute within cipher text mainly complies with the policy of key access. The Ciphertext gets attached to the access policy besides getting decrypted with the attributes satisfaction. All the mentioned techniques were numerically tests by using the NIST Statistical Test, and the result was that the multi-authority hierarchical attribute based encryption mainly ensures more data security (R.Ramachandran, 2014).

The modified version of the CP-ABE is the CP-ASBE (Cipher Text Policy Attribute Set Based Encryption) mechanism (Wan Z, 2012). This scheme adds the hierarchical structure which then provides more flexibility and scalability. This would then enable the party who manages the master keys in the distribution as well as domain authorities who are responsible for the encryption and decryption of the owner's data. Data also gets stored on storage which is also provided by the cloud services provider. This scheme has similar security rate as was found in CP-ABE (Bobba R, 2009).

2.2.3 Fully Homomorphic Encryption

This technique ensures the security of the data used in the communication or the storage or also which are used with the tools similar with the conventional cryptography. This also adds some extra attributes of the computing on the encrypted data and the searching of the encrypted data and much more. Big disadvantage connected with the traditional encrypted techniques is that if the data is to be manipulated, so it required getting coded first. The fully homomorphic encryption performs the computation with the encrypted data which is then sent. For this, some particular scheme was prepared where the calculations were performed very much securely in the cloud without the server having any knowledge of the contents of data sent or without having any knowledge what functions were performed. For designing of this fully homomorphic encryption, a similar design was used as employed in the symmetric homomorphic encryption in order to ensure the data security and privacy which helps in calculations to get performed on the encrypted data having no need to use client's any secret key (Gountia, 2013). Here the encryption is symmetric also which thus reduces the rate of MIPS accordingly.

Some other researchers also used the fully homomorphic encryption technique with symmetric key encryption technique in which they incorporated the fully homomorphic scheme with the symmetric keys and was used on an application (Sharma, 2013). It has been observed from the literature that numerous of the schemes proposed on fully homomorphic encryption mainly involves single party while the schemes proposed and implemented ensured multiparty computation.

In literature, it was also found that a study was conducted on seven different encryption algorithms such as Diffie-Hellman, RSA, Blowfish, RC4, 3DES, DES and AES in the XEC cloud atmosphere. The main analysis parameters used were the input data size, the data itself, and the size of key to be used on different cryptographic algorithms that were analyzed. The main objective of this analysis was to check the data security level in those algorithms as well as the performance of those algorithms was also analyzed. So the end result of the analysis was that the symmetric encryption methods were much faster and efficient than the asymmetric encryption methods (Omer K.Jasim, 2013) (Krunal Suthar, 2012) (Bhansali, 2013). It was also found that there exists an inversely proportional relation among the size of the input file and running time. The more

the input file size increases, the algorithm's running gets decreased except for RSA encryption algorithm as in this case the running time changes slightly with the increase in the size of the input file.

Some other researchers performed a comparative analysis of the encryption techniques namely Blowfish, Twofish, RC6, Rc4, 3DES, DES, AES, and MARS. The comparative testing of these algorithms was performed on a desktop computer and the Amazon EC2 Micro instance Cloud atmosphere (Sherif Eletriby, 2012). For the purpose of analysis, the NIST statistical analysis technique was conducted as well as the Pseudo Random Number Generator (PRNG) also was applied for testing of randomness. All the algorithms mentioned above were implemented using Java Cryptography Extensions (JCE). Results of the simulations showed the effectiveness of the algorithms. In the Amazon Ec2 cloud, the DES, AES, RC6 and Blowfish showed better results than any other encryption techniques used for the analysis while among even them, the AES stood out to be the best while DES and Blowfish were concluded best on the basis of time. On the desktop testing, the RC4, DES, Blowfish, AES and RC6 showed better results than any other encryption technique used in the analysis while the RC6 was concluded best for the desktop testing and the Blowfish turned out to be better on the basis of time.

The working system design for the data security within the cloud atmosphere using the Des algorithm was also proposed by some researchers (Sunita Sharma, 2013). Their design was made up of those components which may provide better security for the users as well as at the admin level. The components used were an adversary, data security, unauthorized data corruption and modification, cloud server authentication, cloud data storage, system, and client. That particular system had the very dynamic support of data including both the block delete, update, as well as append operations. The dependability of data was ensured by using the erasure correction code within the file distribution. The localization of the data errors was mainly achieved using homomorphic tokens having more scattered verification of the removal of the coded data. The DES encryption algorithm is having a correction of the removed data technique mainly was used in order to give the data integrity and security.

Another technique was also proposed, and it was the efficient hybrid cryptography system known as the Hybrid Vigenere Caesar Cipher Encryption (HVCCE) (Holmes, 2013). The main aim of this proposed system was to prevent cloud infrastructure at main three places, at the server, network and client location. His proposed system was designed in a method that the time which was taken for the decryption of the ciphertext by hackers was much higher as expected than the single system.

3. Analysis

After studying these techniques and finding their success evidence from the literature, we can have the analysis as follows:

The Identity-Based Encryption is the form of the public key encryption/cryptography where the server of some third party mainly uses the simple identifier like e-mail addresses for the generation of the public key which and this can then be applied in the decryption and encryption of the electronic messages. In such type of encryption indeed, the complexity gets reduced from the whole encryption process at the end of the both administrators and the users. While in Liner Search Algorithm, the symmetric encryption scheme/algorithm is mainly used for the encryption of plain text. The identity-based signature scheme mainly is deterministic only if the signature on some message by the same user remains same always. Homomorphic encryption mainly is the encryption technique in which both the ciphertext and the plaintext are equally treated using the same algebraic function. The public key encryption is having keyword search (PEKS) scheme mainly contains the four polynomial time algorithms. While in Attribute-Based Encryption, the policies and attributes of the message, as well as the user, then decides on which user should be given the authority to decrypt the cipher text. The main authority creates the secret keys to be used by the users based on the policies/attributes for every user.

4. Conclusion

The data has been increasing in quantity in recent years, and the rate of this expansion is very much explosive. So it is a huge concern to keep the confidentiality of the data high, and this demand is also increasing with the expansion of the data. Cloud computing is still young, and it is getting fame for providing on-demand services and resources at low prices over the internet. Cloud computing has distributed computing structure. So it also eliminates the need for maintaining of the costly computing services and facilities by the institutes and companies. It is still a concern that cloud computing is getting fame slowly, and one of the main reasons for this is the security. Due to having no proper rules and regulation and the laws for the governing of the responsibility for the data flow on the cloud. For the purpose of security, normally cryptographic methods are used for the protection of the data on the cloud. The same techniques can also be used for the data sharing and availability over the cloud. Asymmetric and symmetric encryption alone is not enough to fulfill the security needs over the cloud atmosphere. There should be a combination of more than one cryptographic techniques in order to provide tight security of data over the cloud. The very common and generic encryption techniques and their analysis have been performed in this research. The more capabilities are being given to the cloud; the more security is becoming the major concern and challenge in the wider adoption of the cloud. But still there is a question: can the users fully trust the cloud atmosphere? If their data are totally safe over the cloud? Such questions are still hovering in the minds of the users as well as the cloud computing services providers and by now still no valid or acceptable solution has been found. The cloud is equally getting attractive for the cyber crooks. Cloud by now faces numerous external and internal security threats such as malicious insiders, administrator errors, malware, software bugs, and media failures etc. the cloud services providers hold personal data of the users as well as their identity information like financial transactions, tax documents, social security numbers, medical

records, address books, calendars, and photographs, etc. If such data is properly analyzed, they can provide a lot of information about the user and his/her life. So it is important to safeguard the personal identity of the users. Financial institutions and banks process very sensitive data so if they start using the cloud for their operations, so they would require a highly secure atmosphere in order to perform these operations. Normally in cloud architecture, the third party services are acquired for the storing and security of the data so again there is a question: are the third parties that reliable and trustworthy? It is a concern and challenge as well to hand over sensitive and personal data to the third party. Trusting some third party means to take the risk that the third party will behave and act the similar way as it is expected of them and this trust may not always is fulfilled as expected. The data exposure threat is not only limited to a single individual rather it is distributed at complete cloud level. Loss of data is another very common issues on the cloud. The crucial information may get disappear without leaving any trace, and this is a huge concern for not only the users of the cloud but also the cloud administrators. Some malicious hacker may delete the data from some target cloud, or the data may also get lost due to careless handling by the cloud service provider. Another threat which is created by the cloud is its scalable nature. The cloud services providers mainly share the applications, platforms, and infrastructure in order to provide services to the clients as per their needs and demands. It is indeed a concern that there is no proper isolation among the rights of the providers. Two different service providers may be using the same type of hardware without having any knowledge of it. So if some crucial component in the cloud architecture gets compromised, so the entire cloud atmosphere gets exposed to the potential breach and compromise to the malicious users. Numerous examples are there such as Google was at time forced to make an apology when the Google mail service got collapsed in the Europe and the other example is the Salesforce.com even still handling the phishing attack which was made on it in 2007 and in this scam a staff member was found culprit in revealing the passwords of the clients. Still, big companies such as Amazon and Google are struggling to provide a mechanism to block the cyber-attacks but still this is a dream which is yet to be materialized. So if such big companies can face the security threats and breaches, so this creates more concern for an ordinary cloud user, and the trust level of the cloud goes further low. It is also important to identify the responsibilities of people who should handle the data security over the cloud. Still, it is not clear whose responsibility is it to provide the security of data over the cloud. Either it is the sole responsibility of the cloud service provider, the business entities or other stakeholders to be made responsible for the data security. So legal decision are yet to be made at the cloud level to mark the people responsible for the security breaches and the providing of the security of the data stored in the cloud. Developing secure cloud storage space over the public cloud is still a challenge though security measures are to some extent taken at the private cloud level but on the public clouds, the tight measures are yet to be taken. The private cloud infrastructure is owned and managed by clients or customers, and such clouds are normally located on the premise which means the data remains in control of the customer/client. The data remains in control, and the breaches can hardly be seen only if the third parties are not trusted completely. On the other hand, the infrastructure of the public cloud is managed and owned by the service provider and normally this type of cloud is located off the premise which means the cloud is in the control of the service provider. So the customer data is by large out of the control of his own hands and relied on the trust of the service provider, and the providers can grant access to the public cloud to even the untrusted third parties. Though public cloud provides many benefits than private clouds but it also introduces more security threats as well as privacy risks than the private cloud. So this is the major reason the cloud computing is gaining fame very slowly, and people still don't trust the cloud infrastructure completely as they trust their own data centers at their own premises. This fear of users needs to be eliminated by introducing proper security and privacy mechanism within the cloud so that user data remain safe, and the level of confidentiality of the users' data stays high. Cryptography is considered the best mechanism to provide this security and numerous encryption techniques have also been devised to provide the said purpose. In this research, some of those techniques have been analyzed, and it is found that every encryption technique is good at some specific domain. No single technique is capable of providing answers to all types of security threats as mentioned in Table 2. So normally a mix of encryption techniques are employed to gain the required benefits but 100% success is yet to be seen through more rigorous research in this domain.

REFERENCES

[1] Arshad, J. T. P. a. X. J., 2013. A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, Volume 29, pp. 416-428.

[2] B. Grobauer, W. T. a. E. S., 2011. Understanding Cloud Computing vulnerabilities. IEEE Security Privacy, 9(2), pp. 50-57.

[3] Behl, A., 2011. Emerging security challenges in cloud computing: An insight into cloud security challenges and their mitigation. Mumbai, IEEE.

[4] Benameur, S. P. a. A., 2010. Privacy, Security and Trust Issues Arising from Cloud Computing. s.l., IEEE.

[5] Bhansali, A. S. a. M., 2013. Enhancing Cloud Computing Security using AES Algorithm. International Journal of Computer Applications, pp. 19-23.

[6] Bobba R, ,. K. H. a. P. M., 2009. Attribute-sets: A practically motivated enhancement to attribute-based encryption. Computer Security–ESORICS, pp. 587-604.

[7] CSA, 2011. Security guidance for critical areas of focus in cloud computing, s.l.: Cloud Security Alliance, Tech, Rep..

[8] Gountia, B. K. M. a. D., 2013. Fully homomorphic encryption equating to cloud security: An approach. IOSR Journal of Computer Engineering (IOSR-JCE), pp. 46-50.

[9] Grance, W. J. a. T., 2011. Guidelines on Security and Privacy in Public Cloud Computing, s.l.: National Institute of Standards and Technology.

[10] Holmes, N. S. a. J., 2013. Designing of Cryptography Based Security System for Cloud Computing,". s.l., s.n., pp. 52-57.

[11] J. Ju, Y. W. J. F. J. W. a. Z. L., 2010. Research on Key Technology in SaaS. Washington DC, IEEE.

[12] Jin Li, J. L. X. C. a. C. J., 2015. Identity-based Encryption with Outsourced Revocation in Cloud Computing. IEEE TRANSACTIONS ON COMPUTERS, pp. 425-437.

[13] Kaur, S., 2012. Cryptography and Encryption In Cloud Computing. s.l., s.n., pp. 242-249.

[14] Krunal Suthar, P. K. H. G. a. H. P., 2012. Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment. International Journal of Computer Applications, pp. 16-19.

[15] L. Ertaul, S. S. a. S. G., 2010. Security challenges in Cloud Computing. Las Vegas, IEEE.

[16] Mhammed Chraibi, H. H. a. A. M., 2013. Classification of Security Issues and Solutions in Cloud Environments. s.l., s.n.

[17] Monjur Ahmed, M. A. H., 2014. CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD. International Journal of Network Security & Its Applications, 6(1), pp. 25-36.

[18] Nelson Gonzalez, C. M. F. R. T. C. M. S. M. N. a. M. P., 2011. A quantitative analysis of current security concerns and solutions for cloud computing. s.l., IEEE.

[19] Omer K.Jasim, S. A. E.-S. E.-H. a. A.-B. M. S., 2013. A Comparative Study between Modern Encryption Algorithms Based on Cloud Computing Environment. s.l., s.n., pp. 531 - 535.

[20] Petcu, D. M. G. P. S. a. C. C., 2013. Portable Cloud applications—From theory to practice. Future Generation Computer Systems, Volume 29, pp. 1417-1430.

[21] R. Balasubramanian, D., 2012. Security Problems and Possible Security Approaches In Cloud Computing. International Journal of Scientific & Engineering Research, 3(6), pp. 1-4.

[22] R.Ramachandran, R. M. a., 2014. Comparative study of attribute based encryption techniques in cloud computing. s.l., s.n., pp. 116-120.

[23] Ransome, J. R. a. J., 2009. Security in the Cloud. s.l., CRC Press.

[24] Sharma, C. G. a. I., 2013. Fully Homomorphic Encryption Scheme with Symmetric Keys. s.l., s.n.

[25] Sherif El-etriby, E. M. M. a. H. S. A.-k., 2012. Randomness testing of modern encryption techniques in cloud environment. Informatics and Systems, pp. CC1-CC6.

[26] Singh, P. K. a. R., 2014. CRYPTO MULTI TENANT: AN ENVIRONMENT OF SECURE COMPUTING USING CLOUD SQL. International Journal of Distributed and Parallel Systems, 5(1), pp. 77-85.

[27] Sunita Sharma, A. C. a. A. K., 2013. ENHANCING DATA SECURITY IN CLOUD STORAGE. International Journal of Advanced Research in Computer and Communication Engineering, pp. 2132-2134.

[28] Viega, J., 2009. Cloud Computing and the common Man. IEEE Computer Society, 42(8), pp. 106-108.

[29] Wan Z, L. a. J. D. R., 2012. HASBE: A Hierarchical Attribute Based Solution for Flexible and Scalable Access Control in Cloud Computing. Information Forensics and Security, pp. 743-754.

[30] Yashpalsinh Jadeja, K. M., 2012. Cloud Computing-Concepts, Architecture and challenges. s.l., ICCEET.