JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CLOUD CRYPTOGRAPHY TO ENSURE THE CLOUD COMPUTING SECURITY

Kumar Kishan Chandra, Research Scholar, YBN University
Guide :- Dr. Akhlesh Kumar Singh, Associate Professor, YBN University

Abstract: *The era of cloud computing is very useful in today's world because it uses the Internet and remote access to provide and store information and applications. Customers can use this type of programmer via cloud communication without the need to install anything. Additionally, customer transfer information can be accessed and updated from other computers on the internet. While the information and alerts are powerful and effective, the question remains of how to implement an environment that protects data and programs in the cloud from hackers and intruders. Cloud Computing Environment (CCE) provides a variety of deployment methods that represent the different types of clouds companies or organizations have. The cloud environment serves cloud users through various services such as IaaS, PaaS, SaaS. Cloud computing is essentially built on the concept of interconnecting all physical resources and presenting them as incomprehensible resources. A version used to create resources, control projects, and access Manifesto Expo staff items. It is a fashion organization focused on fashion export and fashion supply. IaaS, PaaS, and SaaS are examples of service fads. Public cloud, private cloud, hybrid cloud, and community cloud are all deployment models. Cloud computing has many good sites. Learn more about some security aspects of cryptography by showing some privacy issues in the ICE routine*.

Keywords: **Cloud Computing Environment, Cryptography,Security Quantum key distribution, Privacy Algorithms.**

I. INTRODUCTION

Cloud computing is an advanced network that provides a variety of services. Transforming the internet into design must be a challenging task. But there are security concerns. Software downloaded from the cloud carries significant risks. Cloud computing has all the weaknesses associated with using these networks. Various information privateers problems in cloud computing occur over the Internet. False significance of information utilized in corporations in cloud to 1/3 events is one of the essential problems which have been found [10]. Encryption needs to be nicely used and the crypto algorithms encompass AES, Rivest-Shamir-Adleman, Data Encryption Standard and three DES. In the presented paper, cryptographic algorithms are used so that you can boom safety concerns. Cloud Information integrity can help to assure security. Various encryption algorithms can be used to ensure cloud security. Symmetric encryption key algorithms and asymmetric encryption key algorithms are two types of algorithms. DES, AES, 3DES and Blowfish algorithms are examples of symmetric algorithms. Algorithms such as RSA and Diffie-Hellman key exchange are asymmetric. Symmetric and asymmetric key technologies are used to encrypt and decrypt data in the cloud. In general, cloud users benefit from resource allocation and scheduling services provided by cloud providers. Therefore, safety is important when using air. [3] [4]. 2. Details about the article [1] The authors discuss, to some extent, data protection issues during data transfer. What is most concerned

about this article is that the information is encrypted so that privacy and confidentiality can be ensured without any problems. The article [2] provides the command that is currently best used not to confirm and verify the integrity of data held on the remote using the properties of auditors or auditors, but instead to retrieve and retrieve information sent back as quickly as possible. The major gain of this scheme is using virtual signatures to guarantee the integrity of neighborhood records. However, the general system is elaborate and complex as the key and record are also encrypted and decrypted respectively. Allocating mathematical time addresses one of the most difficult problems in computing. While clients engage with remote computing centres, this record can maintain secrecy [18]. Its power derived from the use of quantum cryptography or Distributed Discrete (DID) techniques, which are considered the state-of-the-art in encryption and decryption systems [20], [21], as shown in Figure 1. Records are essentially based on fully structured states termed photons over quantum channels. These photons are subsequently transferred as "keys" for secure communication encryption and decryption [11]. The no-cloning theorem benefits from the use of such photons in record transmission.

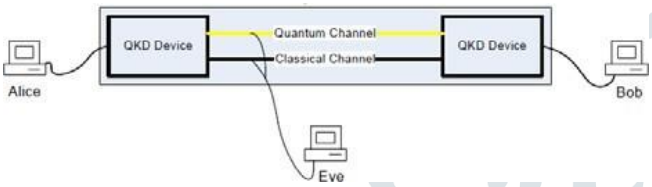

Fig. 1 Schematic of DKD

Researchers are working on the perfect combination of cloud computing and quantum computing to protect the security of data stored on remote computer systems or servers. They use data processing servers (e.g., quantum computers) to encrypt most data, thus successfully hiding input, processing, and data output from malicious attacks [22], [23], [24], [25]. Encryption and authentication in the cloud environment are the most important de facto security measures. Encryption has become one of the most important issues in keeping data safe in the cloud; Reputation as a method of data encryption is outdated. It also protects business data by performing encryption and tokenization on all non-public communications, and the cloud does not impact transactions, availability or operations. [28], [29] are two examples. Cipher Cloud has the ability to create unified data security across all clouds (Google, Amazon, Azure, etc .) that customers currently use to receive data. [14, 15, 16, 17, 18, 19]. Various AES-like memory encryption and tokenization options, as well as pattern- and attribute-preserving encryption methods, are CryptoCloud's strengths. When using Cipher cloud security gateway access software, users can see the actual data while the data stored in the cloud software is encrypted [30], [31]. Cipher Cloud eliminates the security, privacy, and compliance threats inherent in cloud computing by using encryption at the cloud security gate [12]. Cipher Cloud's security encryption protects all saved settings and features, so the cloud suite can continue to work but its main content remains locked on-premises [13]. The system is then reversed and employees instantly detect the data on the device and access the cloud suite, allowing customers to see the actual text of the data rather than an encrypted model in the cloud. II. Security and privacy algorithms in the cloud. Cryptography can help many companies realize privacy early using cloud computing. The most important aspect of privacy that encryption can provide for cloud computing is security and stability. Cryptography is a technique of storing data securely by converting unreadable data into unreadable data [7]. Cryptozoology is now considered a collection of three algorithms. Symmetric key algorithm, asymmetric key algorithm and hashing [6] are the algorithms discussed. Theoretical problems in cloud computing concern issues such as data security, data storage, community traffic, library materials, and host security. Secure HTTP, Encrypted VPN, TLS, Secure Shell, etc. to establish a secure and stable connection between the guest domain and the host domain or from the host side to the control structure. cryptographic technologies should be used. We will use encryption to protect you from attacks such as man-in-the-middle attacks, spoofing attacks, and comment hijacking. Customers can store data and run applications on computers or systems created by cloud computing. While cloud computing has many advantages, it also creates new security challenges because cloud workers are always on hand to manage data rather than relying on customers. We strive to create cryptographic foundations and protocols that can be used in cloud computing while maintaining the balance between security, performance and

practicality. Users dealing with the owners of data or links are no longer authorized and their identities must be protected by cloud statistics and calculations. Cryptography is widely used to solve the above problems as well as some theories in security, privacy and cloud computing. a) Symmetric key algorithm. Symmetric key algorithm uses different keys to perform encryption and

decryption operations. Symmetrical designs provide a useful tool for customers. Provides authentication and authorization of users. In symmetric key algorithm, best and best key is used for each. b) Advanced Encryption Standard (AES)Advanced Encryption Standard [3, 5] is a set of symmetric key encryption cryptography. The block length of each cipher is 128 bits, and the size is 128, 192 and 256 bits, respectively. AES ensures that procedures are followed.

Encryption at rest is used to encrypt the hash code. AES uses a block length of 128 bits. Below is a list of its rules: First Round Key Extension-Round keys are introduced. Subtle tour-A random phase shift in which each byte is replaced by a different byte according to the table. Lines modified-the level at which each country's lines are modified through a series of steps. These lines are combined. ROUND ADD KEY-Each byte of the country is combined with a round key and all encryption works using the key scheme obtained from the cryptographic key. Lower bytes, line changes, and update keys are all used at the end. In 1998, DES policies were compromised using $250,000 worth of equipment. As DES code evolved into mid-1970s technology, Triple DES became too slow and could not produce green, robust software code. Triple DES is slower because it has the same number of three sample DES rounds. a) Data Encryption Standard (DES) Data Encryption Standard (DES) is an important encryption variant and block cipher. It was discovered by the National Institute of Standards and Technology (NIST) in January 1977. For encryption, DES implicitly uses 64-bit plaintext and converts it to 64-bit ciphertext; For decryption, it converts 64-bit ciphertext to 64-bit plaintext for a total of 56 bits. Encryption and decryption are done secretly using a password. In encryption techniques, the first and last permutations of permutations (P boxes) and the Feistel Round of 16 are used. Each rounder uses a different type of 48-bit round key. b) Blowfish algorithm

Blowfish is also classified as a symmetric block cipher and can be used as a replacement for DES. It has flexible keys ranging from 32 to 448 characters, allowing it to be used in various places at home and abroad. Blowfish was created by Bruce Schneier in 1993 as a lightweight and fast alternative to traditional encryption methods. It has since been extensively tested and quickly gained competition as a strong encryption technique. Blowfish is patent-free and license-free, but should be comfortable enough to be used by anyone. Figure 3 Encrypted cloud storage architecture) Asymmetric key algorithm This is a new concept compared to symmetric encryption systems. Encryption and decryption are done using different keys. This is a feature that distinguishes the system from symmetric encryption schemes. Each recipient has a unique decryption key, often called a private key. The client wants to generate the public key, which is the encryption key. This type of encryption system usually relies on a third party declaring that the public key is the best key for a person or organization. d) RSA encryption systemThis encryption algorithm is one of the first and oldest encryption algorithms. Various cryptosystems. It is also the most widely used cryptographic system. This device was called the RSA encryption system because it was created by three students named Ron Rivest, Adi Shamir, and Edelman. This system is no longer used for personal identification numbers, but is now used for public key documents. This is a simple but often used rule of thumb. It usually has two keys: public key and private key. Public secrets are used to encrypt messages and make them known to everyone. The best way to decrypt a message encrypted with a public key is to use a private key. This is how the server uses public key authentication, using its own key to sign completely different messages (called virtual signatures). The customer must sign the form. It then verifies that the server has verified that the public key was used. e) Hash algorithm. MD5 - (Rule Digest Set 5)Cryptographic hash attribute ruleset that uses a 128-bit hash value and converts a variable length message into a 128-bit fixed output. The input message is first split into 512-bit chunks and then added so that the total time is divided by 512. The sender uses the public key to encrypt the communication. The receiver uses his own key to decrypt the communication. ii. Cloud Storage Kamara and Lauter et al. [32] proposed to provide a digital station that can meet many needs (confidentiality, integrity, authentication, etc.). Most requirements can be met by encrypting data stored in the cloud. But thanks to collaboration technology, this encryption has become stricter on all searches and changes to the data. Figure 3 shows the structure of an encryption station that can be used to address backup, storage, data integrity, static transactions, and e-discovery security. Designed" [9]. It has three main components: Data Processing (DP), which reads data before sending it to the cloud; Data Verifier (DV), which verifies the accuracy of the data; and Token Generator (TO), which allows naming the issuer to access information. Before sending statistics to the cloud, Alice uses a statistical process to encrypt and encode the data with metadata (tags, time, length, etc.) and then transfers them to the cloud. B. Custom designed models. These models include

cryptographic cloud version and cloud statistical encryption, both of which are primarily based on quantum cryptography. Therefore, to improve the service quality and reliability of Cloud Computing Encryption, the key technology and management are based on DID. Deploy decryption and policy mechanisms. (ii) Use of heavy computing devices that are not compatible with non-public computers. The concept version performs a lot of calculations before dynamically creating objects in the cloud; These calculations can be done in three simple steps as shown in Figure 1. 4: Enterprise, DID and Open Cloud segments. - EC (Business): EC (Business) SECURITY

CHALLENGES IN CLOUD

When it relates to privacy and security, the cloud poses significant risks. People should certify, just like merchants, that the cloud of harassment is free of issues such as knowledgeloss or data theft.

There is a possibility that a malicious user or hacker would enter the cloud under the guise of a normal user, affecting many of us who are infected or using the afflicted cloud. Cloud computing can be used in a variety of scenarios:

i. Data theft
ii. Data integrity
iii. Security issue
iv. Loss of sensitive data
v. Corrupt code
vi. Data abbreviation
vii. Data security at the business level
viii. Data security at the user level

Current generation cloud computing capabilities do not provide privacy from untrusted cloud operators and, therefore, there is no need to store sensitive information such as medical records, financial information or company-related information. We like to use different methods from theory to practice to solve this problem. The most common application of encoding is to ensure confidentiality by extracting all useful information from plaintext. Coding transforms useless information into unknown information. To solve this challenge, we developed cryptosystem algorithms that facilitate a variety of calculations on encrypted raw materials, from arithmetic calculations to designed custom calculations. Highly homomorphic encryption, searchable encryption, association encryption, and strategic encryption are all examples of homomorphic cryptography research. a. Storage proof. Buyers should check whether the cloud operator's credentials on stored data have been compromised. Buyers often avoid this by keeping a copy of the service file in their custody, even if the file does not need to be retained. Actually, the work is very good. b. Security storage system. We will strive to create cloud storage systems to protect customer data from cloud service providers in terms of confidentiality, security and integrity. These systems must be very efficient and use new cryptanalytic coding techniques such as homomorphic encryption, search encryption, identification codes and data storage to ensure confidentiality without being secure.

II. CONCLUSION

Cloud computing is a rapidly developing technology that has become a trend with many companies and large enterprises switching to the cloud. However, for safety reasons, the thermal insulation effect is the opposite. Cloud Security is the final building block to bridge the cloud adoption gap among large international companies, businesses and organizations. There are many security algorithms that can be used in the cloud. DES, Triple-DES, AES and Blowfish are examples of symmetric algorithms. Symmetric algorithms are used in DES and AES because they are secure. AES is more difficult to implement than DES. The algorithms used by RSA and Diffie-Hellman key exchange are very different. Encryption can be used in many ways for cloud security. Cryptography will be used for cloud data access control, cloud data trust, data analysis, cloud information authorization and authentication, and secure data storage. Also, generally, full-frame encryption and identity-based encryption are two important aspects of gifting.world that ensure cloud data security. In this area, there is stilla lot of research to be done.

REFERENCES

[1] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing,"2009,
[2] http://www.wheresmyserver.co.nz/storage/media/faq-files/ clouddef- v15.pdf, Accessed April 2011.
[3] Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010).
[4] IDC, "IDC Ranking of issues of Cloud Computing model,"ed, 2009, http://blogs.idc.com/ie/?p=210, Accessed on July2011.
[5] Cloud Computing Use Case Discussion Group, "CloudComputing Use Cases Version 3.0," 2010.
[6] Cloud Security Alliance (CSA). (2010). Available: http:// www.cloudsecurityalliance.org/
[7] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi LoIacono, "On Technical Security Issues in Cloud Comput- ing," in IEEE ICCC, Bangalore 2009, pp. 109-116.
[8] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.
[9] Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings ofthe 2009 IEEE International Conference on Services Com-puting, 2009, pp. 517-520.
[10] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human-oriented and Person- alized Mechanisms, Technologies, and Services, 2010, pp.344-349.
[11] S. Subashini, Kavitha, V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. In Press, Cor- rected Proof.
[12] Lohr, Steve. "Cloud Computing and EMC Deal." New YorkTimes. Feb. 25, 2009. pg. C 6.
[13] McAllister, Neil. "Server virtualization." InfoWorld. Feb. 12, 2008. Retrieved March 12, 2008.
[14] http://www.infoworld.com/article/07/02/12/07FEvirtualserv_1.html
[15] Markoff, John. "An Internet Critic Who Is Not Shy About Ruffling the Big Names in High Technology." New York Times. Apr. 9, 2001. pg.C6
[16] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, h t t p : / / w w w .theregister.co.uk/ 2009/03/16/azure_cloud_crash/
[17] P. Ferrie, Attacks on Virtual Machine Emulators, White Pa-per, Symantec Corporation, January 2007, http://www.symantec.com/avcenter/reference/Virtual_Ma- chine_Threats. pdf
[18] G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal,March 26, 2010
[19] L. Youseff, M. Butrico, D. D. Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environ- ments Workshop, held with SC08, November 2008.
[20] http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOn- tology.pdf
[21] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik. Scalable and e_cient provable datapossession. In Proceed- ings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08), pages 1{10, New York, NY, USA, 2008. ACM.
[22] Hodges, A. (2005), 'Can quantum computing solve classi- cally unsolvable problems"
[23] H.K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrary long distances. Science 1999;283(5410): 2050-2056.
[24] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/ spb3/
[25] L. Lydersen, Wiechers, C., Wittman, C., Elser, D., Skaar, J.and Makarov, V. Hacking commercial quantum cryptogra-phy systems by tailored bright illumination. Nat. Photonics4, 686, 2010.
[26] K. Inoue, Quantum Key Distribution Technologies. IEEE Journal of Selected Topics in Quantum Electronics, vol. 12, no.4, July/August 2006.
[27] http://ewh.ieee.org/r10/bombay/news4/Quantum_Comput-ers.htm
[28] http://www.bbc.co.uk/news/scienceenvironment-16636580
[29] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm
[30] G. Brassard, T. Mor and B. C. Sanders, "Quantum cryp- tography via parametric downconversion", in QuantumCommunication, Computing, and Measurement ,P. Kumar, G. Mauro D'Ariano and O. Hirota (editors), Kluwer Aca- demic/Plenum Publishers, New York, 2000, pp. 381.
[31] P. D. Townsend, \Experimental investigation of the perfor- mance limits for first telecommunications-window quan- tum cryptography systems", IEEE Photonics Technology Letters, Vol. 10, 1998, pp.1048.
[32] J. Brodkin. Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartnerseven- cloud-computing-security-risks-853, 2008.