A Review Paper on Data Encryption Challenges and Recommendations in Cloud Computing

Amit B. Kale[1] Prof. Mrs. Pratibha Adkar[2]
[1,2]Department of Master of Computer Applications
[1,2]P.E.S.'s Modern College of Engineering, Pune, India

Abstract— The Cloud Computing offers service over internet with dynamically scalable resources. Cloud Computing services provides benefits to the users in terms of cost and ease of use. Cloud Computing services need to address the security during the transmission of sensitive data and critical applications to shared and public encrypted cloud environments. The cloud environments are scaling large for data processing and storage needs. When it comes to cloud data protection methods, no particularly new technique is required. Protecting data in the cloud can be similar to protecting data within a traditional data center. Authentication and identity, access control, encryption, secure deletion, integrity checking, and data masking are all data protection methods that have applicability in cloud computing. This paper will briefly review few methods, data encryption's challenges and its recommendations, and will note anything that is particularly unique to when these are deployed in a cloud. This paper discusses the security of data encryption in cloud computing. It is a study of data in the cloud and aspects related to it concerning data encryption security. The paper gives an idea of data protection methods and challenges while data encryption used throughout the world to ensure maximum data encryption efficiency, performance of data protection by reducing risks and threats in key management.

Key words: Cloud Computing, Data Encryption, Data Challenges, Recommendations, Techniques

I. INTRODUCTION

A. Cloud Computing

Cloud computing (so-called, cloud) represents one of the magnificent shifts in information technology which can enhance collaboration, agility, scaling and availability, and provide the potential for cost reduction through optimized and efficient computing. Different from the existing technologies and computing approaches, cloud is defined with five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), SPI service models (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)), and deployment models (Public, Private, Hybrid, Community)[1].

Due to its characteristics and models, Gartner Inc. expected worldwide cloud services revenue to reach $148.8 billion in 2014, and estimated that over the next five years entrepreneurs would spend $112 billion on SaaS, PaaS and IaaS [2].

Organizations are increasingly turning to the cloud for data processing and storage. Storing data in the cloud is advantageous for numerous reasons: the elasticity of cloud environments ensures that only storage used is paid for, while tasks such as backup, replication, and geographic diversification of data are effectively outsourced to cloud storage providers. However, unfettered access to this environment and arbitrary migration of data means that determining the origin of information, or equally importantly, determining the modifications and chain of custody undergone by this information before it has assumed its current form, is a virtually intractable problem given the current tools available to us. Such a state of the art becomes increasingly worrisome when issues such as regulatory compliance are brought to bear on information in the cloud [3].

B. Data Encryption for Cloud

As show in below Figure1, Cloud encryption is a service offered by cloud storage providers whereby data, or text, is transformed using encryption algorithms and is then placed on a storage cloud. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers [4]. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud [4].

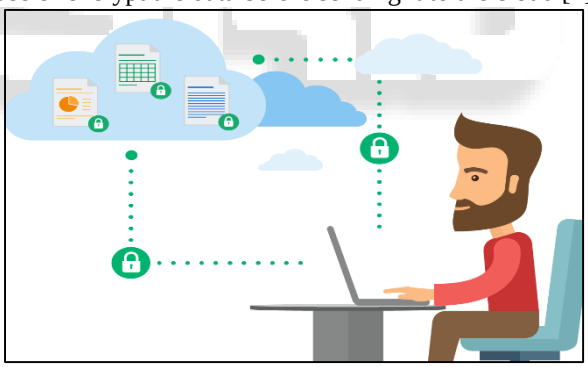

Fig. 1: Data Encryption for cloud storage

Encryption is considered a best practice for any security-conscious organization, including those that need to meet specific industry compliance requirements such as healthcare, ecommerce and retail, and financial reporting. Recurring data breaches are increasing, particularly in the healthcare industry that reports an estimated $7 billion loss due to data breaches. Even those organizations that determine their risk of data loss is minimal often choose encryption to mitigate the risk of having to report a data breach, since the loss of encrypted data may not be considered a reportable event if the encryption keys remain safe [5].

II. DATA ENCRYPTION IN CLOUD

Cloud storage providers offer cloud encryption services to encrypt data before it is transferred to the cloud for storage. Typical cloud encryption applications range from encrypted connections to limited encryption only of data that is known

to be sensitive (such as account credentials) to end-to-end encryption of any data that is uploaded to the cloud. In these models, cloud storage providers encrypt data upon receipt, passing encryption keys to the customers so that data can be safely decrypted when needed [5].

Encryption drives costs for cloud storage providers (and ultimately their customers) due to the additional bandwidth required to encrypt data before it is transferred to the cloud. As a result, many providers limit their cloud encryption services while some cloud storage customers simply encrypt their own data on-premises before it is moved to the cloud. Some cloud customers will choose this approach regardless, as it can save costs while keeping the entire encryption process and all keys within their environment, transferring data to the cloud only after it has been encrypted [6].

Whenever possible, sensitive data that is to be uploaded to the cloud should be encrypted on-premises, prior to upload. This ensures that data will be secure in the cloud even if your account or the cloud storage provider is compromised.

Secure encryption key management – both for your keys and any keys provided by a cloud vendor – is critical as well. Encryption keys should be stored separately from the encrypted data to ensure data security. Key backups also should be kept offsite and audited regularly. Other encryption key best practices include periodically refreshing keys, especially if keys are set to expire automatically. Some companies choose to encrypt keys themselves, but that can add unnecessary complexity in some cases. Another best practice for key management is to implement multi-factor authentication for both the master and recovery keys [4].

While there are some challenges associated with cloud encryption, business regulations and data security requirements make it a necessity. Privacy and data security experts agree that encryption is a critical tool for information security, and cloud providers offer different applications of encryption to fit a range of data security needs and budgets. Taking the time to understand your cloud data protection needs, research the encryption services offered by different cloud vendors, and plan for secure cloud adoption will enable your business to reap the benefits of cloud storage and computing without putting your data at unnecessary risk [6].

For instance, Office 365 Message Encryption is a built-in service that encrypts all messages both inside and outside of the platform. Encryption services like these prevent unauthorized free access to your system or file data without the decryption key, making it an effective data security method.

Keeping information secure in the cloud should be your top priority. Just taking a few preventative measures around data encryption can tighten security for your most sensitive information.

A. Follow these Encryption Tips to Lock Down Your Information in the Cloud.

1) Encrypt Data Before You Upload It

If your cloud service does not automatically encrypt data before its uploaded, make sure to encrypt these files beforehand. You can find a third-party encryption tool that will apply passwords and encryption to files after you are finished editing so they are encrypted before upload [6].

2) Secure Access with Cloud Cryptography

Cloud cryptography is another way to secure your cloud computing architecture. Cloud computing service providers like Azure employ cryptography to offer a layer of information security at a system level and enables secure access to whoever needs shared cloud services. This layer of encryption is based on the Quantum Direct Key system, which is an advanced system of symmetric encryption keys. Users receive a public and private key pair with a specific ID. Cryptographic cloud computing can also minimize network congestion [6].

3) Protect Data at Rest & In Transit with a Cloud Access Security Broker

A cloud access security broker (CASB) is another way you can encrypt data and control your own keys. A CASB offers a single point of visibility and access control into any cloud app in a large enterprise. The control comes through contextual access control, encryption for data at rest and leakage protection of data. A CASB mediates the connections between cloud apps and the general public through several API connectors and proxies [7].

B. Some Common Encryption Algorithms which are used in Cloud Computing

1) AES:

The Advanced Encryption Standard, AES, is a symmetric encryption algorithm and one of the most secure. The United States Government use it to protect classified information, and many software and hardware products use it as well. This method uses a block cipher, which encrypts data one fixed-size block at a time, unlike other types of encryption, such as stream ciphers, which encrypt data bit by bit. AES is comprised of AES-128, AES-192 and AES-256. The key bit you choose encrypts and decrypts blocks in 128 bits, 192 bits and so on. There are different rounds for each bit key. A round is the process of turning plaintext into cipher text. For 128-bit, there are 10 rounds; 192-bit has 12 rounds; and 256-bit has 14 rounds. Since AES is a symmetric key encryption, you must share the key with other individuals for them to access the encrypted data. Furthermore, if you don't have a secure way to share that key and unauthorized individuals gain access to it, they can decrypt everything encrypted with that specific key [7].

2) 3DES:

Triple Data Encryption Standard, or 3DES, is a current standard, and it is a block cipher. It's similar to the older method of encryption, Data Encryption Standard, which uses 56-bit keys. However, 3DES is a symmetric-key encryption that uses three individual 56-bit keys. It encrypts data three times, meaning your 56-bit key becomes a 168-bit key. Unfortunately, since it encrypts data three times, this method is much slower than others. Also, because 3DES uses shorter block lengths, it is easier to decrypt and leak data. However, many financial institutions and businesses in numerous other industries use this encryption method to keep information secure. As more robust encryption methods emerge, this one is being slowly phased out [8].

3) RSA:

This asymmetric algorithm is named after Ron Rivest, Adi Shamir and Len Adelman. It uses public-key cryptography to share data over an insecure network. There are two keys: one public and one private. The public key is just as the name suggests: public. Anyone can access it. However, the private key must be confidential. When using RSA cryptography, you need both keys to encrypt and decrypt a message. You use one key to encrypt your data and the other to decrypt it. According to Search Security, RSA is secure because it factors large integers that are the product of two large prime numbers. Additionally, the key size is large, which increases the security. Most RSA keys are 1024-bits and 2048-bits long. However, the longer key size does mean it's slower than other encryption methods [8].

4) Blowfish:

Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain. Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available [8].

5) Twofish:

Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed. Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, you'll find it bundled in encryption programs such as PhotoEncrypt, GPG, and the popular open source software TrueCrypt [8].

III. Few Encryption Techniques and Mechanisms to Secure Cloud

A. Proxy re-encryption (PRE):

Proxy re-encryption (PRE) schemes are cryptosystems which allow third parties (proxies) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another.

Proxy Re-encryption a proxy re-encryption algorithm transforms cipher-text ck1 to cipher-text ck2 with a key rkk1->k2 without revealing the corresponding clear - text, where ck1 and ck2 can only be decrypted by different key k1 and k2, respectively, and rkk1->k2 is a re-key issued by another party, e. g., the originator of cipher-text ck1.

B. Data Masking:

Data masking supports heterogeneous environments without the need to modify applications or data. They also complement existing data security controls such as encryption and tokenization without the need to modify settings or configurations.

Data masking is a method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required[7].

C. Authentication and Identity:

Authentication of users takes several forms, but all are based on a combination of authentication factors: something an individual knows (such as a password), something they possess (such as a security token), or some measurable quality that is intrinsic to them (such as a fingerprint). Single factor authentication is based on only one authentication factor. Stronger authentication requires additional factors; for instance, two factor authentications is based on two authentication factors (such as a pin and a fingerprint) [8].

D. Access control mechanisms:

1) Mandatory access control

Mandatory access control (MAC) mechanism is the traditional mechanism to define the access rights of users. MAC gives access permission through the operating system or security kernel. It controls the ability of data owners to grant or deny access rights to clients for the file system. All access control rights are set by the system manager and imposed by the security kernel or operating system. Clients have no rights to alter these access rights. In mandatory access control model, each file system object has a classification label such as, secret, top secret or confidential level. Each device and client is assigned a similar classification and clearance level. The security kernel determines the classification label of clients and resources. The operating system or security kernel checks the credentials of each person or system while accessing a particular resource to determine the access rights of that specific person or device [9].

2) Discretionary access control

Discretionary Access Control (DAC) is a security access control mechanism which controls the access permissions through data owner. In DAC, the access rights of each user are performed during authentication by validating the username and password. DACs are discretionary as owner determines the privileges of access. In DAC, file or data has owner and the data access policies are controlled by data owner. DAC provides more flexibility than MAC however, DAC provides less security than MAC [9].

3) Task based access control

Entitlement or task based access control is one of the minute level access control mechanism. A specific access permission is required for each task, action or process that is represented by an entitlement or task. This model has capabilities to handle complex access conditions to determine whether the access rights need to be granted or denied. The major concern about entitlement access control model is the maintenance of large number of entitlement sets. The users also need to raise separate request and get the approval for each entitlement [9].

IV. CLOUD ENCRYPTION: CHALLENGES AND RECOMMENDATIONS

A. Challenges:

Cloud computing has evolved as an important solution for many enterprises by providing reliable, efficient and cost effective resources as service. The service provider offers resources to the user based on either pay and use or pay as you need. Cloud computing offers many benefits to the user by providing dynamic scalability, flexibility, reduced IT costs and by minimizing the time for implementation. Cloud computing offers on-demand, self-service, pay-per-use and scalable computing resources and services, thereby reducing the capital and operational expenditures for hardware and software as well. Despite the potential benefits of the cloud computing, the enterprises are slow in adopting it due to security issues and challenges associated with it. Security and privacy are the major concerns in adopting cloud. Since the cloud provider offers Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), storage as a service and other services, the idea of handing of user data to the service provider is worrisome [10]. The Major Challenges that are Preventing the Enterprises from Adopting Cloud Computing are as follows:

1) Unavailability of Encrypted Key:

With the expansion of mobile applications, customers should consider having their service provider or a third-party proxy provider manage the encryption keys rather than the company's own IT department. The problem companies run into, is that if data is encrypted before being uploaded to a cloud storage provider and that data is then needed on a mobile or remote device that does not already have the decryption key, the resulting download will be useless, encrypted data. This becomes make worse. When a company tries to share data with a business partner, but does not want the partner to have direct access to decryption keys [7].

2) Adds more complex layer:

Key rotation and destruction also becomes more complex when a company is managing its own keys for what can entail millions of files. A third-party proxy provider can add a layer of protection by keeping the keys separate from the encrypted data at a cloud provider, but this also adds another layer of complexity, as well as the additional cost of a second third-party provider for the company [11].

3) Old/ outdated protocols:

Companies should ask to their providers and potential SaaS partners what protocols they use for transmitting data. The Secure Socket Layer (SSL) approach, which had been the standard for years, has fallen out of favor since the discovery in 2014 of the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack, a man-in-the-middle exploit that effectively was designed into the SSL code[10-11].

4) Legacy systems:

Implementing TLS (Transport Layer Security) rather than SSL (Secure Sockets Layer) eliminates the vulnerability, but some legacy systems running older operating systems, such as Windows XP, are unable to implement TLS. As a result, some retailers still have some servers running SSL to support these older systems, even though there is the possibility of confidential data being compromised. The only way to eliminate the risk entirely is to disable SSL entirely either on the client system or the server which gets rid of the problem but also makes the servers inaccessible to systems that only have SSL capabilities.

Beyond key management, the largest issue SMBs (Server Message Block) must grapple with is believing that a cloud provider is better at protecting sensitive data than they are and is as vested in protecting the company's data as is the data's owner.

Cloud providers are not subject to the same data breach disclosure laws as are banks, government's agencies, and other entities. And breaches that do occur might not be widely publicized or associated with cloud providers. However, the organization that owns the data is responsible, even when the cause of the data breach lies with the cloud hosting organization. If such a data breach is publicized, the negative attention will be focused more on the data owner than on the cloud computing provider. It is, ultimately, the obligation of the enterprise to protect its data, wherever and however it is processed. This is why the Cloud Security Alliance, in its Security Guidance for Critical Areas of Focus in Cloud Computing, Recommends that sensitive data should be:

1) Encrypted for data privacy with approved algorithms and long, random keys;
2) Encrypted before it passes from the enterprise to the cloud provider;
3) Should remain encrypted in transit, at rest, and in use;
4) The cloud provider and its staff should never have access to decryption keys.

This last stipulation can be the most challenging for SMBs, depending on their use of cloud. For simple file sharing, there are some good add-ons for Dropbox and similar offerings, such as Viivo or SafeMonk. When an SMB moves processing to the cloud, things become a bit more complex. When processing of sensitive data takes place in the cloud, users take advantage of the cloud's economy of scale and elasticity. The data should remain encrypted up to the moment of use and that both the decryption keys and the decrypted versions of the data should be available in the clear only within a protected transient memory space. Both the keys and the clear text versions of the sensitive data must be auditable wiped so that no copies are ever written to disk. The processing must never write copies of the clear text sensitive data to any logs or other persistent records [11].

B. Recommendations:

Implementing the following recommendations should facilitate more efficient and effective storage encryption solution design, implementation, and management of keys.

1) When selecting a storage encryption technology, organizations should consider solutions that use existing system features (such as operating system features) and infrastructure.

There are many factors for organizations to consider when selecting storage encryption solutions, such as the platforms they support, the data they protect, and the threats they mitigate. Some solutions involve deploying various servers and installing software on the devices to be protected, while other solutions can use existing servers, as well as software built into the devices to be protected. Generally, the more

extensive the changes are to the infrastructure and devices, the more likely it is that the storage encryption solution will cause a loss of functionality or other problems with the devices. When evaluating solutions, organizations should compare the loss of functionality with the gain in security capabilities and decide if the trade-off is acceptable. Solutions that require extensive changes to the infrastructure and end user devices should generally be used only when other solutions cannot meet the organization's needs [11].

2) Organizations should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments.

Centralized management is recommended for most storage encryption deployments because of its effectiveness and efficiency for policy verification and enforcement, key management, authenticator management, data recovery, and other management tasks. Centralized management can also automate deployment and configuration of storage encryption software to end user devices, distribution and installation of updates, collection and review of logs, and recovery of information from local failures [12].

3) Organizations should ensure that all cryptographic keys used in a storage encryption solution are secured and managed properly to support the security of the solution.

Storage encryption technologies use one or more cryptographic keys to encrypt and decrypt the data that they protect. If a key is lost or damaged, it may not be possible to recover the encrypted data from the computer. Therefore, organizations should perform extensive planning of key management processes, procedures, and technologies before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery, and destruction. Organizations should carefully consider how key management practices can support the recovery of encrypted data if a key is inadvertently destroyed or otherwise becomes unavailable. Organizations planning on encrypting removable media also need to consider how changing keys will affect access to encrypted storage on removable media and develop feasible solutions, such as retaining the previous keys in case they are needed [11-12].

4) Organizations should select appropriate user authenticators for storage encryption solutions.

Storage encryption solutions require users to authenticate successfully before accessing the information that has been encrypted. Common authentication mechanisms are passwords, personal identification numbers, cryptographic tokens, biometrics, and smart cards. Organizations should consider leveraging existing enterprise authentication solutions (e.g., Active Directory, public key infrastructure [PKI]) instead of adding another authenticator for users [12].

5) Organizations should implement measures that support and complement storage encryption implementations for end user devices.

Storage encryption by itself cannot provide adequate security for stored information; additional security controls are needed. Organizations should select and deploy the necessary controls [12].

V. CONCLUSION

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges are still existing in this technology. Security is the most challenging issue in this technology. In this paper we have discussed various encryption algorithms to overcome this security issue. Although encryption is not a gold bullet of data or system security, it is one key tool that can be accompanied by a full arsenal of security services for a layered-defense approach to ensuring data is protected, even if accessed by unauthorized individuals. Additional security options to add to your IT solution will be covered.

REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M."A view of cloud computing. Communications of the ACM", 53(4), 50-58, 2014.

[2] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems", 25(6), 599-616. 2009.

[3] Tim Mather, Subra Kumaraswamy, Shahed Latif "Cloud Security and Privacy", O'Reilly Media, 2009

[4] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2 (3), 242-249, 2012.

[5] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing" , Page(s): 1 – 9, 2009.

[6] Manpreet Kaur, Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", IJCA , Volume 70 - Number 18, 2013.

[7] Cong Wang; Qian Wang; Kui Ren; Wenjing Lou, "Ensuring data storage security in Cloud computing," QualityofService, 2009. IWQoS. 17th International Workshop on , vol., no., p 1,9, 13-15 July 2009

[8] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG)", CSI Sixth International Conference, 8-13 Sept. 2012.

[9] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, IJCSIT Vol. 2 , 1836-1840, 2011.

[10] Eystein Mathisen. "Security Challenges and Solutions in Cloud Computing", in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), p.208-212, 2011.

[11] Wentao Liu. "Research on Cloud Computing Security Problem and Strategy", in: 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), p.1216-1219, April 2012.

[12] Karen Scarfone, Murugiah Souppaya, Matt Sexton, "Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-111, p.1-5, 2007.

