**IMPACT: International Journal of Research in Applied, Natural and Social Sciences (IMPACT: IJRANSS)**
**ISSN(E): 2321-8851; ISSN(P): 2347-4580**
**Vol. 2, Issue 4, Apr 2014, 123-126**


# TOWARDS SECURING DATA IN THE CLOUD

**SHORUNKE MUYIWA MUSADDIQ**

Department of Mathematics & Computer Science, Elizade University, Ilara-Mokin, Ondo State, Nigeria

## ABSTRACT

Clouds are rapidly becoming a platform of choice for hosting increasingly complex application software and services. Among the attractive features they offer are elasticity and pay-as-you-go model, which allow businesses to gain access to vast computing resources with minimum upfront investment, and operational costs. Although a great deal of progress has so far been made with respect to the low-level technological underpinning of the clouds, today's clouds are still considered to be insufficiently trustworthy to serve as a computing platform for critical infrastructure (such as e.g., financial or power grid) operators and public administration sectors. Cloud computing has evolve to minimize IT expenses and to provide agile IT services to individual users as well as organizations. It moves computing and data away from desktop and portable PCs into large data centers.

This technology provides the opportunity for more innovation in lightweight smart devices and it forms an innovative method of performing business. Cloud computing relies on the internet as a medium for users to access the required services at any time on pay-as-you-go pattern. Nevertheless this technology suffers from threats and vulnerabilities that hinders the users from solely relying on it. Various malicious activities from illegal users have threatened this technology such as data misuse, inflexible access control and limited monitoring. The occurrence of these threats may result into damaging or illegal access of critical and confidential data of users. This research paper describes the various types / methods of cryptographic encryption that would benefit users who might want to switch to the cloud or are currently using the cloud platform.

**KEYWORDS:** Cloud, Data, Cryptography, Encryption, Security

## INTRODUCTION

Security in the cloud is, of course, a major challenge. A CIO (Chief Information Officer) might legitimately fear losing control over a company's data assets. 'How can I protect my data?' is one of the most important questions every individual or organization should ask before moving to the cloud. Cloud data protection policy should be rooted in cryptography, which time and time again has proven to be the most effective means of securing data. Not all data needs the same level of protection.

Companies need to evaluate their data assets before they move to the cloud so that they can bestow an appropriate level of protection to each one. Which employees need access to a particular data set? Which data are the most sensitive? In the past, a perimeter-based security model relying on firewalls, antivirus software and monitoring systems was deemed sufficient to protect a company's data. Such models are inappropriate for the cloud where boundaries are not clearly delineated. In a cloud environment, it is vital that data assets themselves are protected, not just the infrastructure and systems they travel through.

Cryptography is the practice of rendering data unreadable to anyone except authorized personnel. This means that if a data breach does occur, the data is useless to the intruder. Data can only be read with the correct 'key', the string of bits that decrypts that data in conjunction with the correct algorithm. This means that storing and protecting the keys is anessential element of protecting the data. Cryptography is the solution to many of the security challenges posed by the cloud. When deployed properly, using best practices, strong algorithms and appropriate key lengths, cryptography is effectively unbreakable because, if data is lost or stolen, it is unreadable without the associated key.

Likewise, when properly deployed cryptography is used to digitally 'sign' messages or other data, the validation process provides mathematical proof that the signature could only have been created by someone with the private signing key.

## UNDERSTAND DIFFERENT TYPES OF CLOUD ENCRYPTION

Below are four types of encryption that may be of great benefit when moving to the cloud:

### Network Encryption

This applies cryptography when data is in transit. Data has to move between private networks and a cloud, within a cloud or between clouds themselves. Any data in transit is vulnerable because networks generally cannot be assumed to be secure. Network encryption is thus essential for protecting data in the cloud. Fortunately, it can be easily utilized, and when properly implemented, is transparent to users and has minimal impact on performance.

### Storage Encryption

This is the encryption of data stored in the cloud, whether that data resides in an archive, a temporary cache or a live database. It is also transparent and relatively easy to deploy. However, there are issues concerning key management. A balance has to be struck between security and availability. If data is to be available at all times, it means keeping the keys accessible at all times, which can be challenging when implementing proper measures to secure those same keys.

### Application Level Encryption

This is the selective encryption of specific data used by specific applications. This type of encryption is very closely linked to the applications being used. Instead of protecting the whole stream of data moving in the cloud like network encryption, it just protects specific items when processed by the application. Different applications may or may not require encryption based on the type of data they handle, reinforcing the need to adequately evaluate data assets before they are put into the cloud. As application level encryption requires the integration of cryptography with particular applications, it can be harder to set up and manage than other types of encryption.

### Edge of Cloud Encryption

This is the blanket encryption of sensitive data before it leaves a company's control and moves into the cloud. The great benefit of 'edge of cloud' is that all data that is heading to the cloud is encrypted prior to leaving the enterprise premises, so it is never exposed to the cloud at all. This sort of encryption is likely to be what many organizations will feel most comfortable with. Yet there are downsides. It requires extra management and greater overheads depending on the volume of data passing into the cloud and the accessibility of that data which a company requires.

## STRONG CRYPTOGRAPHY

When cryptography is deployed well, it is virtually unbreakable, even to the most skilful and determined attacker. Weak cryptography, on the other hand, is easily broken and renders your data vulnerable. Whatever method of cryptography is chosen, good key management is what separates strong cryptography from weak cryptography. The lock to your house might be unbreakable, but it is useless if you leave the key under the mat. Organisations should use strong algorithms recognised by industry standards. History has shown that the best way of managing keys, and therefore protecting data, is through the implementation of hardware security modules rather than software solutions.

## BEST PRACTICES

Beyond the implementation of cryptography, there are many other 'best practices' which contribute to an effective cloud security strategy. While too numerous to list here, it is worth Security noting that in the vast majority of cases, a tiered data access policy is extremely important in protecting data. Companies should be aware of malicious insiders or the possibility of negligence on the part of employees when handling sensitive data. A simple technique is to avoid 'super users' with access to all of a company's data. By separating responsibilities, there is no single point of attack for an intruder to exploit.

## MOVING TO THE CLOUD

The cloud affords numerous opportunities for businesses, but its key characteristic of sharing resources like storage, networks and applications between organisations carries with it new risks and challenges. Cryptography should be the bedrock of any company's security policy when moving data in the cloud. When deployed properly, it offers fail- safe protection. However, companies have to make a compromise between the security of their data and its availability and chose the right level of cryptography for their needs. Encryption is a powerful technology, but without careful management of keys, users will have a false sense of security. This makes key management a top priority when it comes to protecting data in the cloud.

## CONCLUSIONS

In this research paper have discussed the characteristics of cloud and data security. Cloud computing has a dynamic nature that is flexible, scalable and multi-shared with high capacity that gives an innovative shape of carrying out business. However, beside these benefits there are vulnerabilities with the cloud platforms in ensuring data security. Therefore, we believe there is still tremendous opportunity for researchers to make revolutionary contributions in this field and bring significant impact of their development to the industry.

There is need to develop and design in-depth security techniques and policies in terms of people, processes and technology. By considering the contributions from several IT industries worldwide, it's obvious that cloud computing will be one of the leading strategic and innovative technologies in the near future.

## REFERENCES

1. G., Petri. "Vendor Lock-in and Cloud computing", [Online], Available: http://cloudcomputing. sys-con.com/node/1465147, 2010, [Accessed: 6-June-2013].

2. Beth, R.E. (2012, January 20). Predictions about the future of cloud computing: Possibilities and Issues. Retrieved May 24, 2012, from out sourcing centre: http://www.outsourcing- center.com/2012-01-predictions-about-the-future-of-cloud-computing-possibilities-and-issues- article-46825.html

3. IBM Corporation the Benefits of Cloud Computing: Anewera of responsiveness, effectiveness and efficiency in IT service delivery. IBM Dynamic Infrastructure Group, New York.2009.

4. N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In Proceedings of the Workshop on Hot Topics in Cloud Computing, HotCloud'09. USENIX Association, 2009.

5. Cloud Security Alliance y –Security Guidance For Critical Areas of Focus in Cloud Computing. [online]https://cloudsecurityalliance.org/research/security guidance/ 2011 [Accessed: 6-June-2013].