International Journal of Pure and Applied Researches http://ijopaar.com; 2018 Vol. 3(1); pp. 08-14, ISSN: 2455-474X

Review on the Cryptographic Cloud Storage Techniques

Dr. Mohammad Miyan

Head, Department of Mathematics,

Shia P. G. College, Lucknow-20

Email: mabbas_7786@yahoo.com

Abstract

The cloud computing has become phenomena its fancy to be revolution in info technology, the cloud encompasses parts from grid computing, utility computing and involuntary computing, into AN innovative preparation design, Cloud computing giving quick access and high performance computing and storage infrastructure victimization internet service. This fast movement towards the clouds has impact in level of security the $64000 fascinating question is the way to build secure cloud storage wherever service supplier isn't fully trust client. During this paper a comprehensive survey of existing literature for cryptologic storage techniques, edges and disadvantages in cloud computing is bestowed.

Keywords: Cloud computing, Cloud storage, Cryptographic storage architecture, Cryptographic cloud architecture, Cloud storage.

1. Introduction

Cloud computing may be a combination of IaaS, PaaS, SaaS. To construct a secure cloud system, security at infrastructure, service platforms and application software package levels have to be compelled to be studied for a secure cloud system. Data cryptography is one amongst effective means that to realize cloud computing data security. Historically, data cryptography focuses on nominative stages and operations, like encoding. For cloud computing, a system level style must be enforced.

Crypto cloud computing may be a new secure cloud computing design. It will give protection of data security at the system level, and permits users access to shared services handily and accurately. Crypto cloud computing protects individual's connections with the skin world. It will shield the private privacy with none delay of data exchange.

Crypto cloud computing is predicated on the Quantum Direct Key system. Quantum Direct Key (QDK) may be a set of advanced uneven offline key mechanism. During this mechanism, all entities get public and personal key combine per their ID. Every entity solely holds its own personal key, however incorporates a public key generator to get any public key. During this system, AN entity will manufacture the general public key of the other entities offline, no any third-party agency (such as CA) is important. Crypto cloud computing supported QDK will avoid network holdup, and alternative drawbacks mistreatment current cryptography system.

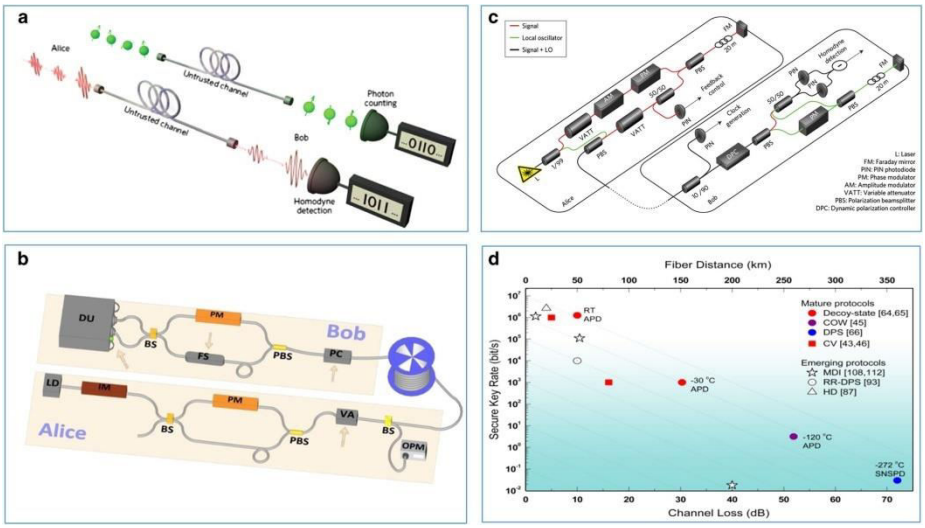

Figure-1 Quantum key distribution (Eleni et al. 2016)

In the crypto cloud system, every entity encrypts knowledge mistreatment his/her own personal key. All parts within the system like cloud computing infrastructure units, platform, virtualization tools and everyone concerned entities have their own keys. Whereas fulfilling their own functions of data exchange and process, of these parts can use the general public key and personal key to perform authentication initial. What's additional, events occur within the cloud computing are assigned a novel key. During this means, crypto cloud system guarantees the protection and quality of data exchange.

Current cloud computing structure is developed for knowledge and computing sharing. Security isn't priority of system. On the contrary, cryptography and security square measure inherently integrated within the crypto cloud computing supported the QDK. QDK licensed operate are bricks of crypto cloud computing. Besides primary operate of information en/decryption, crypto cloud computing conjointly provides several security connected functions. As an example, all channels sign transmit knowledge mistreatment with their own keys, and also the receiving terminals will avoid hijacking by confirmatory signature. What's additional, the precise position of security escape will be known determined by analyzing digital signatures of solid knowledge. Supported such capabilities, crypto-related functions will be provided as services in cloud, that is known as 'Crypto as a service (CAAS)'.

Crypto cloud computing isn't solely the advances in data technology, however conjointly innovation of logical relationship. In crypto cloud system, non-system knowledge isn't allowed to store and transmit. Personal Key and offline public key, play a task of identification and certification within the method of data exchange. During this means, the cloud establishes a relationship of trust with a client. Knowledge identification depends on the logical relationship of mutual trust or would like, and also the logical relationship depends on the cloud client.

2. Literature Review

Yadav et al. (Yadav et al. 2014) style a secure knowledge sharing theme, Mona, for dynamic teams in an untrusted cloud. In Mona, a user is ready to share knowledge with others within the cluster while not revealing identity privacy to the cloud. In addition, Anglesey supports economical user revocation and new user connexion. A lot of specially, economical user revocation is achieved through a public revocation list while not change the personal keys of the remaining users, and new users will directly rewrite files hold on within the cloud before their participation.

Privacy and security in cloud are often same to be achieved once users have management over data they need to make known to cloud and who will access their data. While not guarantee of security and privacy users cannot create shift to cloud solely on the premise of lower value and quicker computing.

Kamara et al. (Kamara et al. 2016) have described at a high level, several architectures which combine recent and non-standard cryptographic primitives in order to achieve the goal. They surveyed the benefits of the architecture, which can provide to both service providers and customers and also give an overview of the recent advances in cryptography motivated by cloud storage specially.

Sridevi et al. (Sridevi et al. 2017) presented a survey of the existing cryptographic storage techniques and the various benefits in the cloud computing.
Hussein et al. (Hussein et al. 2016) have presented a comprehensive survey on the existing literature of the cryptographic storage techniques, benefits and drawbacks in cloud computing.

Vidhya et al. (Vidhya et al. 2017) show however the SSE scheme is often used to guarantee privacy on a public cloud. They have discussed the design of the cryptologic cloud and additionally the operating of SSE scheme. This may be used to fulfill the safety of the many a cloud based mostly service and assure the users of the confidentiality of their data. Such a theme permits users to make a secure storage over the infrastructure of the cloud provider.

The Cloud Storage Encryption (CSE) design and Policy secret writing / decoding and access technique have been known so as to indicate however information will be transfer to cloud computing storage setting. The integrated work flow between secret writing purpose, decryption purpose and searchable secret writing has been presented as CSE discipline elements. (Hamdanet al. 2013)

3. Challenges of Consumer Cloud Storage

While there are drawbacks, many smaller firms still see an advantage to using ready-made cloud storage solutions for their work. How to best approach cloud storage will depend on how those firms are using the files and their available resources.

To ensure version management, engineers should store files in a central location (whether that's on premise or in the cloud) and provide access. That way, everyone knows they are working on the most up-to-date version of the file. For firms using consumer-style cloud offerings, they may need to develop their own protocols for ensuring version control. Industrial scale systems often have features

that automatically manage that function, as well as control read and write access to the files while they are being used.

"For smaller companies that are looking for files to follow them or for collaboration and maybe just have a few seats, they can use something like One Drive or Dropbox with Solid Edge," Staples says. "That can solve the multiple access problems and synch those files to the cloud. Larger companies are going to have an IT person, and they really need more of a PDM environment."

Services like Dropbox and One Drive are easy to use, simple to set up and offer capacity that's in-line with purpose-built, professional storage solutions created for engineering environments.

However, these consumer services don't provide some engineer-specific functionality that can be critical for successfully using cloud storage. A product like Autodesk 360, for example, automatically tracks file versions and provides a viewing platform for sharing files with partners who don't have AutoCAD. It is also integrated directly into other Autodesk products, providing a direct connection from the application to the files.

Without those features, users may wind up deleting files or folders, don't have visibility into the status of task assignments, or could work off the wrong version of a file—which can cost an engineer days or weeks of work.

"The most expensive mistake is working off the wrong file," Kenesto's Minasian says. "If you are working under a system that allows for different copies of files to be made, then everyone struggles to work off the current file. Even if it's just a marketing document that can be a significant challenge." Dropbox and other systems also present challenges when it comes to synchronization. Users may need to manage configuration of folders and define them to synchronize on different machines. If there are data dependencies between files (as is common with CAD projects), then data would be synchronized on all machines within a single organization, which is not terribly efficient. For larger companies, it probably isn't even possible.

This is why tools like A360 Drive and Kenesto Drive were developed—to make it easier for designers to sync data from their desktop to the cloud. Siemens PLM's Solid Edge ST9 includes cloud-enabled file vaulting and built-in data management. The cloud-enabled vaulting lets users share design data in a controlled manner with external partners using services like Dropbox, One Drive, Google Drive or Box.

Dropbox is also trying to solve this problem via its Dropbox Project Infinite, providing access to files anywhere without having to store them on a drive. Users could manage cloud files the same way they manage local files, but without taking up any space on the hard drive. Dropbox has also acquired Pixelapse, a company that provides version control and collaboration tools for designers. (Brian, 2017)

4. Moving up to an Enterprise-Class Solution

While consumer solutions are initially cheaper and easier to use, there are still advantages to using a system built for designers—whether that's one that works in tandem with a service like Dropbox, or one that utilizes a purpose-built infrastructure for engineering applications.

• **Security:** Enterprise-class systems can be configured to encrypt files, decrypt them and allow specific users access to specific directories on the cloud. "There is an active directory component to the file system and storage system to make sure there isn't unauthorized access to the files," ANSYS' Milhem says.

Content can be checked in or out, and entire folder structures can be configured for specific types of sharing. "For example, you can configure it so that anything beneath this folder my team has access to, or external suppliers have access to," Minasian says. "The contents of that folder can have varying levels of permissions." (Patwari et al. 2015)

• **Version control:** If multiple copies of files are created and kept in different locations, or there is no control over who is working on a file at a given time, then there are bound to be problems with versions and revisions. That functionality should be available so that you can automatically track those revisions, retrieve previous versions of files, and lock files when they are being edited.

"A lot of products are synchronizers, so you aren't working with the current version of the file," Minasian says. "That's what we do differently. We also present the current file."

• **Familiar interface:** Using a tool designed for engineering applications will provide your users with an easy to use and familiar interface. These solutions will structure folders and files the way an engineer is used to seeing them.

• **Better file management and sharing:** General file sharing tools aren't designed to track the file dependencies common in CAD and other applications. Industry-specific software tools will do this automatically. They can also make it easier to share files with customers or partners who may not have access to the specific CAD or other program the file was created in. (Brian, 2017)

5. Engineers Embrace the Cloud

The good news for cloud storage and file sharing is that the engineering community has largely embraced the concept. Reliability and security concerns that used to create a barrier to adoption have largely been addressed.

"Most people really get the cloud now," says Bill Boswell, senior director of Cloud Services Marketing and Business Strategy at Siemens PLM Software. "We hear fewer and fewer objections."

One remaining concern is latency—your network and internet connection have to be robust enough to handle the movement of these large files to the cloud, as well as frequent accessing and editing the files.

"The speed at which the network is performing is always going to be important," Minasian says.

"If you are waiting for a file to come across the internet, that's not a place you want to be," Staples adds. "You have to have a strategic approach with standard cloud synchronization tools, using local files, and if not that, then you have to have a caching strategy."

Those concerns will vary depending on where you and affiliates or partners are located. "It can be a tough problem to solve," Boswell says. "In some parts of the world, access is good; in others not so much. Dealing with latency can be challenging, and you have to do your homework in that environment."

Interactive engineering applications also require dynamic storage solutions that allow engineers to access files and perform streaming or rendering without downloading huge files. Autodesk, for one, hopes to address this through transfer avoidance technology that only updates files that have changed (instead of entire assemblies).

And the industry continues to improve, offering new and better tools to manage files in the cloud. "All of the pieces of the puzzle for cloud storage are evolving and changing," Milhem says. "Security is evolving, access is changing and network access latency is getting better. That ensures that the cloud environment is very similar to what engineers have experienced in terms of storing and sharing files on their desktop. This has all come together." (Brian, 2017)

6. Conclusion

The Cloud Storage encoding (CSE) design and Policy encoding / coding and access technique have been known so as to point out however information will be transfer to cloud computing storage surroundings. The integrated work flow between encoding purpose, decryption purpose and searchable encoding has been presented as Communications Security Establishment subject field elements and interaction between elements is explained in the present paper.

References

[1]. Brian. A. (2017); Thinking outside the Cloud Storage Box, Engineering Computing. Available at: https://www.digitalengineering247.com/article/thinking-outside-the-cloud-storage-box/

[2]. Eleni D., Hoi-Kwong L., Bing Qi & Zhiliang Y. (2016); Practical challenges in quantum key distribution, NPJ Quantum Information volume 2, Article number: 16025 https://www.nature.com/articles/npjqi201625

[3]. Hamdan, M. Al-Sabri, Saleh M. Al-Saleem (2013); Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security, IJCSI International Journal of Computer Science Issues, Vol. 10(2), No 1, pp. 259-266.

[4]. Hussein, N. H., Khalid, K. & Khanfar, K. (2016); A Survey of Cryptography Cloud Storage Techniques, Int. Journal of Computer Science & Mobile Computing, Vol. 5(2), pp. 186-191.

[5]. Kamara, S. & Lauter, K. (2016); Cryptographic Cloud Storage, Microsoft Research; pp. 1-14. http://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/crypto-cloud.pdf

[6]. Patwari, R & Choudhary, S. (2015); Security issues and Cryptographic techniques in Cloud Computing, International Journal of Innovative Computer Science & Engineering. Vol. 2(4), pp. 01-06.

[7]. Sridevi, R. & Banupriya, C. B. (2017); A Survey on Cryptographic Cloud Storage Techniques, IJESRT, Vol. 6(7); pp. 602-605. DOI: 10.5281/zenodo.829787

[8]. Vidhya, R., Pathange, M. K. S. & Grandhi, N. (2017); BIG DATA PRIVACY PROTECTION USING CRYPTOGRAPHIC CLOUD STORAGE, International Journal of Pure and Applied Mathematics, Vol. 116(6), pp. 7-11.

[9]. Yadav, M. G., Reddy, N. C., Babu, G. P. & Prabha, I. S. (2014); Cryptographic Cloud Storage with data sharing and security for Multi access network, IJDCST, V-2, I-2, SW-16, pp. 6-14.