

Encryption Based Framework for Cloud Databases Using AES algorithm

¹R. Ganga Sagar,² N. Ashok Kumar

¹PG Scholar (CSE), Narayana Engineering College, Nellore

²M.Tech., Assistant Professor, Department of CSE, Narayana Engineering College, Nellore.

Abstract: *A Cloud database management system is a distributed database that delivers computing as a service (Caas) instead of a product. Improving confidentiality of information stored in cloud database .It is very important contribution to cloud database. Data encryption is the optimum solution for achieving confidentiality. In some normal methods, encrypt the whole database through some standard encryption algorithm that do not allow in sql database operations directly on the cloud. This formal solution affected by workload and cost would make the cloud database service inconvenient. We propose a novel architecture for adaptive encryption of public cloud database. Adaptive encryption allow any sql operation over encrypted data. The novel cloud database architecture that uses adaptive encryption technique with no intermediate servers. This scheme provides cloud provider with the best level of confidentiality for any database workload. We can determine the encryption and adaptive encryption cost of data confidentiality from the research point of view. Index Terms Adaptive Encryption Technique, AES(Advanced Encryption Standard), Metadata.*

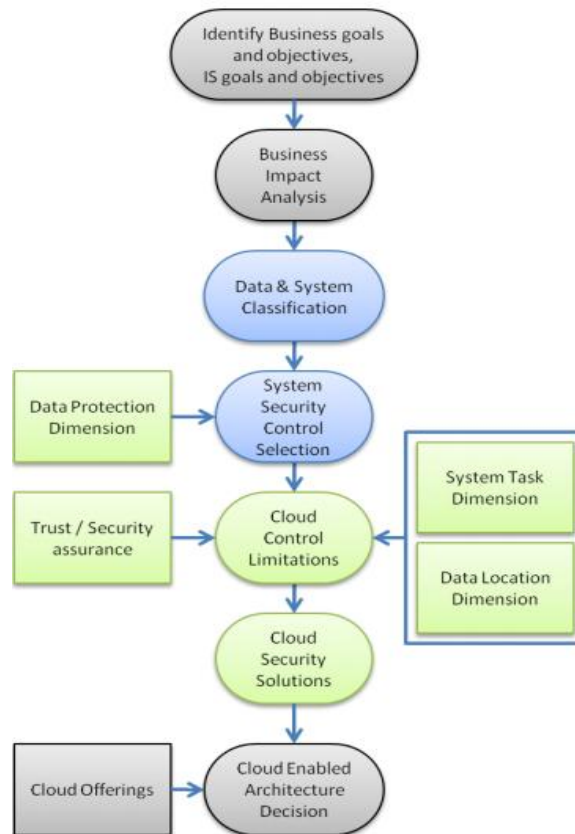
1. INTRODUCTION

The most thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. These days, you're frequently processing, storing, or transmitting data that's subject to regulatory and compliance requirements. When that data falls under regulatory or compliance restrictions, your choice of cloud deployment (whether private, hybrid or public) hinges on an understanding that the provider is fully compliant. Otherwise, there's the risk of violating privacy, regulatory or other legal requirements. The implications for maintaining the security of information are significant when it comes to privacy.

Today almost all PC users have access to the internet. More and more users are using at least some cloud services, like e-mail, Facebook, Google Docs and so forth. But not only private users are switching to cloud services, also companies and governments are adopting them. Cloud computing offers many benefits for its users, e.g. cost savings, increased flexibility and ubiquitous access to the data just to mention a few. There have been enough privacy violations outside the realm of cloud computing for there to be concern about any system—cloud-based or traditional—when storing, processing or transmitting sensitive information. The cloud has its own examples as well. In 2010, several cloud privacy information exposures occurred with a number of cloud-based services, including Facebook, Twitter and Google.

Privacy concerns within the cloud model aren't new. As a tenant with legal privacy obligations, your handling of privacy issues is no different if you use the cloud. Just as you wouldn't store such information on a server without adequate controls, you wouldn't select any cloud provider without verifying it meets the same benchmarks for how it protects data at rest, in transmission or while processing.

Your policies may exclude any external provider managing sensitive information for you, including cloud providers. While there may be a perception that the computer on your desk is safer than a public cloud, it's probably not (unless you're taking unusual technical and procedural precautions). Safety and governance are two separate issues, and as part of due diligence, you'll need to fully understand your provider's privacy governance, as well as its security practices and guidelines.



The Cloud Computing Confidentiality Architecture

A. Cloud Computing Technology: Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Parallels to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service. Cloud computing is different from hosting services and assets at ISP data center. It is all about computing systems are logically at one place or virtual resources forming a Cloud and user community accessing with intranet or Internet. So, it means Cloud could reside in-premises or off-premises at service provider location. There are types of Cloud computing like 1. Public clouds 2. private Clouds 3. Inter-clouds or Hybrid Clouds,

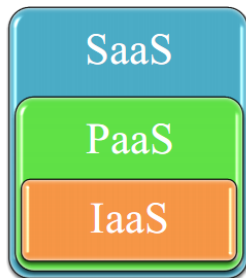
B. Cloud Working Progress: Cloud computing has been changing how most people use the web and how they store their files. It's the structure that runs sites like Face book, Amazon and Twitter and the core that allows us to take advantage of services like Google Docs and Gmail. But how does it work. Before we dig further into how does cloud computing work, first let's understand what the term "cloud" refers to. The concept of the cloud has been around for a long time in many different incarnations in the business world. It mostly means a grid of computers serving as a service-oriented architecture to deliver software and data. Most websites and server-based applications run on particular computers or servers. What differentiates the cloud from the way those are set up is that the cloud utilizes the resources from the computers as a collective virtual computer, where the applications can run independently from particular computer or server configurations. They are basically floating around in a "cloud of resources", making the hardware less important to how the applications work. With broadband internet, the need to have the software run on your computer or on a company's site is becoming less and less essential. A lot of the software that people use nowadays are completely web-based. The cloud takes advantage of that to bring it to the next level.

C. Characteristics of Cloud Computing: Characteristics Cloud computing is cost-effective. Here, cost is greatly reduced as initial expense and recurring expenses are much lower than traditional computing. Maintenance cost is reduced as a third party maintains everything from running the cloud

to storing data. Cloud is characterized by features such as platform, location and device independency, which make it easily adoptable for all sizes of businesses, in particular small and mid-sized. However, owing to redundancy of computer system networks and storage system cloud may not be reliable for data, but it scores well as far as security is concerned. Some of the most important five key characteristics are, On-demand Self Service Broad Network Access Resource Pooling Measured Service Selection of Provider.

Software as a Service (SaaS)

This is the level which consumers are most familiar with. Providers are gaining access to an application running on their web servers, usually as web application. Common examples are email, social networking and other software applications like word processing.



. Platform as a Service (PaaS)

Providers are as a platform where the consumers can deploy and run their own applications on without having to manage the underlying hardware. Tools and libraries as well as the network and storage space are also provided. Examples are Windows Azure and Google App Engine.

. Infrastructure as a Service (IaaS)

Raw computing power and storage space is provided. Consumers can fully control the underlying virtual machines, including operating system, network and storage space. Providers in this category are Amazon EC2 and Rackspace Cloud Services.

2. PROPOSED ALGORITHM

A. Advanced Encryption Standard: It also uses Symmetric Key Algorithm. AES uses 128, 192, or 256-bit length keys. Adopted by National Institute of Standards and Technology (NIST) on May 26, 2002. AES uses the Rijndael algorithm developed by Joan Daemen and Vincent Rijmen of Belgium. AES is a simple design, a high speed algorithm, with low memory costs. AES is a symmetric block cipher. The same key is used to encrypt and decrypt the message. The plain text and the cipher text are the same size. AES is restricted to use a block size of 128 bits with AES uses permutation substitution method which involves a series of substitution and permutation steps to create the encrypted block. AES encryption on the other hand is still not breakable through there are some theoretical discussions about breaking the AES is relatively new. Time required to check all the possible keys at 50 billion keys per second.

B. Adaptive Encryption Schemes: Adaptive encryption methods for public cloud database service, where distributed and concurrent clients can issue direct SQL operations. By avoiding an architecture based on one or multiple intermediate servers between the clients and the cloud database, the proposed solution guarantees the same level of scalability and availability of the cloud service a scheme of the proposed architecture where each client executes an encryption engine that manages encryption operations. This software module is accessed by external user applications through the encrypted database interface.

3. IMPLEMENTATION

A. Modules and Module description

1. User Application First of all the client have to select the data. The data re useful for the clients in cloud. The original data is not transferred to the server directly. Before that client have to encrypt the data and then transfer it to the server. Because of this encryption the data is very secure. And also the metadata is created. Using the metadata the server can verify easily.

2. Client-Side Encryption Engine Sending original data to the server is vulnerable to the data. To avoid this problem the original data should be encrypted. Also the client can't send the original meta data to server. The metadata is also encrypted for the security purpose. These process are done in the client side encryption engine.

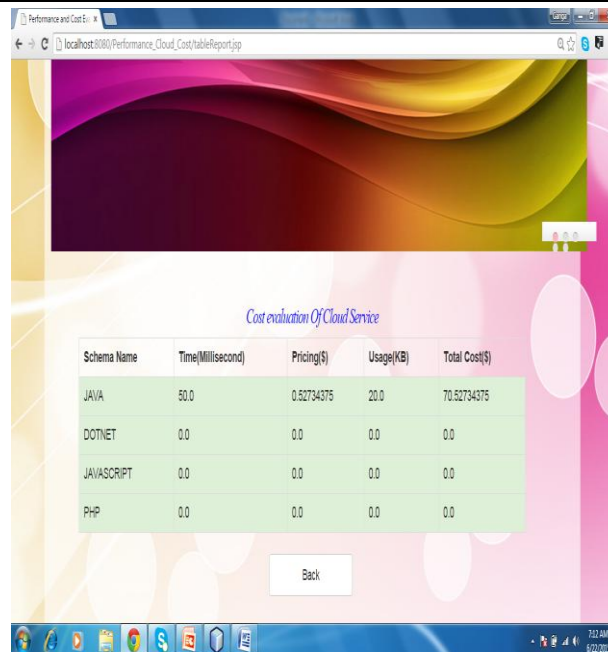
3. Client Encrypted Database Interface These encrypted original data are transferred to the server. And the encrypted metadata are also transferred to the server. Using the metadata the client request is processed in the server side. The these data are stored in the data base. The searching process is done over the encrypted metadata. Metadata is useful forget the encrypted original data to the client.

4. Cloud Database Engine The client request is generated in the client side. And this request is transferred to the server. The server searches for the related data to the query. This searching is done by the encrypted metadata. Using the meta data the original data is referred in the server side. And transfer the encrypted metadata to the client who send the request to the server. Using the encrypted data the client decrypts and get the original data.

5. Cloud Authentication and Connection Services The client receives the data from the server. And get the key for decrypting the data. Using the key the data is decrypted. The original data is visible to the client only. Server transfers the data to the client. But client does not know about the original data. Using the security and the metadata the data is transferred to the client.

B. Results:





Schema Name	Time(Millisecond)	Pricing(\$)	Usage(KB)	Total Cost(\$)
JAVA	50.0	0.52734375	20.0	70.52734375
DOTNET	0.0	0.0	0.0	0.0
JAVASCRIPT	0.0	0.0	0.0	0.0
PHP	0.0	0.0	0.0	0.0

4. CONCLUSION

Data confidentiality is very important in sharing. The data is encrypted in client side and transferred to the server. Then client send request to the server. Server processing for that request and transfers it to the client. Then client uses the key and decrypts the data.

REFERENCES

- [1]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.
- [2]. T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. O'ReillyMedia, Incorporated, 2009.
- [3]. H.-L. Truong and S. Dustdar, "Composable cost estimation and monitoring for computational applications in cloud computing environments," *Procedia Computer Science*, vol. 1, no. 1, pp. 2175 – 2184, 2010, iCCS 2010.
- [4]. Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R. et al. (2009). *Above the clouds: A Berkeley view of cloud computing*. *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28*.
- [5]. Baralis, E. and Chiusano, S. (2004). Essential classification rule sets. *ACM Transactions on Database Systems*, 29(4): 635-674.
- [6]. Bardin, J., Callas, J., Chaput, S., Fusco, P., Gilbert, F. et al. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing v2.1*, Retrieved January 28, 2010, from Cloud Security Alliance, from <http://www.cloudsecurityalliance.org/guidance/>
- [7]. NIST SP 800-145, "A NIST definition of cloud computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
- [8]. NIST SP 800-146, "NIST Cloud Computing Synopsis and Recommendations", <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>
- [9]. NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations", http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- [10]. *Federal Cloud Computing Strategy*, <http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>
- [11]. Chief Information Officers Council, "Privacy Recommendations for Cloud Computing", <http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx>

- [12]. Office of Management and Budget, Memorandum 07-16, <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>
- [13]. NIST SP 800-144, “Guidelines on Security and Privacy Issues in Public Cloud Computing”, http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
- [14]. NIST Cloud Computing Use Cases, <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseCopyFromCloud>
- [15]. Gartner, “Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services”, <http://www.gartner.com/it/page.jsp?id=1064712>.
- [16]. IETF internet-draft, “Cloud Reference Framework”, <http://tools.ietf.org/html/draft-khasnabish-cloud-reference-framework-00>

AUTHORS' BIOGRAPHY



R. Ganga Sagar pursuing M.Tech in Computer Science and Engineering from NARAYANA ENGINEERING COLLEGE, NELLORE, A P, India. His areas of interests are network security and cloud computing.



N. ASHOK KUMAR did his B.Sc and M.Sc from SV university and M.Tech from JNTU specialization in Computer Science and Engineering. He is currently working as an assistant Professor in Dept of Computer Science and Engineering, NARAYANA ENGINEERING COLLEGE, NELLORE, A P, India. He has 6 year of experience in Teaching and 3 year of experience in industrial, he published 3 papers in international journals.