IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption

Dinesh Kumar P[1] and Sneha T[2]
Assistant Professor, Department of Science and Computer Engineering[1]
Student, Department of Science and Computer Engineering[2]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *This describes cloud storage system, it support for rapid development of cloud computing data leakage prevention algorithm and it implemented secure storage mechanism. CSSM adopted a hierarchical management approach and combined user password with secret sharing to prevent cryptographic materials leakage. Advanced encryption standard algorithm(AES) is implemented for encryption of data. The proposed scheme ensuring the reduced overhead and latency in system. The objective is to secure the cloud data with reduced leakage system. The main objective of the proposed mechanism is to secure cloud storage against data breach, which may be the result of targeted attack or management negligence (e.g. misconfiguration), in case hackers even some malicious administrator is able to steal user data.*

Keywords: Cloud computing, storage security, key management, data dispersion, data encryption.

I. INTRODUCTION

Cloud computing has shown remarkable development in recent decades. When the storage as a service, it occupies the center stage and backbone for many applications such as pattern recognition, image forensic and forgery detection. As a result, larger volumes of data will be a part of the cloud area. In the cloud industry, Amazon Web Service(AWS) has become the de-facto standard. As the core component of the Open Stack that follows this standard. Swift has become one of the most popular cloud storage mechanism. However, Open Stack Swift mechanism still faces many real security threats. While providing convenient services. According to Cloud Security Alliance's top threat case analysis report released in 2018, two thirds of the cases will cause user data leakage, mainly due to management negligence and malicious attacks. For instance, under default configuration, Open Stack Swift mechanism typically stores data in plaintext for the sake of performance. That will lead unauthorized access to user data at storage layer. In addition, Security Report released by Open stack Vulnerability Management Team VMT, the Swift mechanism may leak. This paper presents CSSM, a Cloud Secure Storage Mechanism. CSSM combines data dispersion with data encryption, so that large-scale cloud data and keys would be stored in chunked cipher texts. On this basis user password and secret sharing are introduced to further protect keys security. We implemented CSSM based on Open Stack Swift mechanism and made several tests.

II. RELATED WORK

In this section we have literatures related to cloud secure storage mechanism.
In [1], authors proposed a industrial control systems that specifies monitor, automate, and operate complex infrastructure and processes that integrate into critical industrial sectors that affect our daily lives.
In [2], authors proposed a sensor-cloud systems with more personal data being hosted in cloud, privacy leakage is becoming one of the most serious concerns. Privacy computing is emerging as a paradigm to systematically enhance privacy protection.
In [3], authors propose a cloud data de-duplication scheme based on certificateless proxy re-encryption. It contains certificateless proxy re-encryption (CL-PRE) and proof of ownership based on certificateless signature (PoW-CLS).
In [4], authors proposed a cloud based big data sharing system utilizes storage facility from a cloud service provider to share data with the legitimate users. In contrast to traditional solutions cloud provider stores the shared data in the large data centers outside the trust domain of the data owner which may trigger the problem of data confidentiality.
Authors of [5] presents the data storage facility provided by the cloud computing enabled business organizations to overcome the burden of huge data storage and maintenance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Authors of [6] examines the Internet of Things (IoT) is an interconnected network of computing nodes that can send and receive data without human participation.

In [7], authors proposed a multi-cloud storage with the optimization parameters to speed up the uploading time spent to store data in several cloud storage services.

III. METHODOLOGY

1. LOGIN / LOGOUT: In this module the user can login by using their unique username and graphical password. The login module verify the user given username and password with the stored username and password in the cloud. If the username and password is matched the user can access the resources. If it does not match the user does not allowed to access the resource.
2. UPLOAD / DOWNLOAD: In this module the buyer and seller can post the ads and also able to download the data's that are post by other sellers. This module is mainly used to upload and also download the big data files.
3. DATA DISPERSION: Two data sets can have the same mean but they can be entirely different. Thus to describe data, one needs to know the extent of variability. This is given by the measures of dispersion. Range, interquartile range, and standard deviation are the three commonly used measures of dispersion**.**
4. ENCRYPTION: There are two basic encryption algorithms for cloud-based data: Symmetric encryption: The encryption and decryption keys are the same. This method is most commonly used for bulk data encryption.

IV. SYSTEM ARCHITECTURE

A system architecture is the conceptual model that defines the structure, behaviour and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system. The point of our framework it constructed a secure distributed storage system based on Hadoop system, which keep the confidentiality of cloud data through data dispersion and encryption. It performs the data decryption and assembly tasks before reading data. To prevent the keys from being stolen, this method requires key cache server and all keys should be stored in memory only. Some approaches introduced independent third party to manage the key. The system architecture of the proposed system is in figure 1.

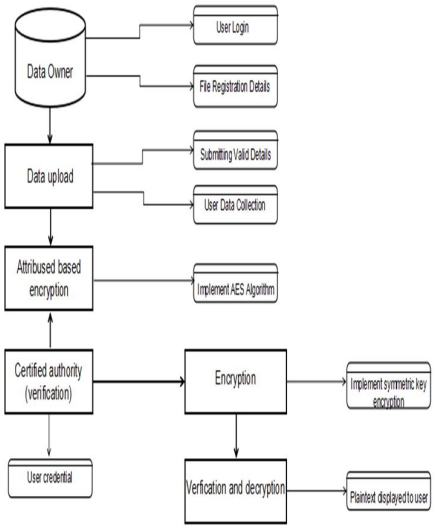

Figure 1. System Architecture

V. EXPERIMENTAL ANALYSIS

PYTHON TECHNOLOGY: Python is an interpreter, high-level and general-purpose programming language. It supports multiple programming paradigms including procedural, object-oriented, and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

PYTHON PROGRAMMING LANGUAGE: Python is a multi-paradigm programming language. Object-oriented programming and structured programming are fully supported and many of its features support functional programming and aspect-oriented programming including by Meta programming and met objects magic methods. Many other paradigms are supported via extensions including design by contract and logic programming. Python packages with a wide range of functionality including easy to learn and use, expressive language, interpreted language, cross-platform language, free and open source, Object-Oriented Language, extensible, large standard library, GUI, programming support, integrated.

Python uses dynamic typing and a combination of reference counting and a cycle-detecting garbage collector for memory management. It also features dynamic name resolution (late binding), which binds method and variable names during program execution.

Rather than having all of its functionality built into its core, Python was designed to be highly extensible. This compact modularity has made it particularly popular as a means of adding programmable interfaces to existing applications. Van Rossum's vision of a small core language with a large standard library and easily extensible interpreter stemmed from his frustrations with ABC, which espoused the opposite approach. Python is meant to be an easily readable language. Its formatting is visually uncluttered and it often uses English keywords where other languages use punctuation. Unlike many other languages, it does not use curly brackets to delimit blocks and semicolons after statements are optional. It has fewer syntactic exceptions and special cases than C or Pascal.

Python's developers strive to avoid premature optimization and reject patches to non-critical parts of the Python reference implementation that would offer marginal increases in speed at the cost of clarity. When speed is important, a Python programmer can move time-critical functions to extension modules written in languages such as C or use PyPy, a just-in-time compiler. Python is also available which translates a Python script into C and makes direct C-level API calls into the Python interpreter. Python uses duck typing and has typed objects but untyped variable names. Type constraints are not checked at compile time rather operations on an object may fail signifying that the given object is not of a suitable type. Despite being dynamically typed, Python is strongly typed forbidding operations that are not well-defined (for example, adding a number to a string) rather than silently attempting to make sense of them.

THE PYTHON PLATFORM: The platform module in Python is used to access the underlying platform's data, such as, hardware, operating system, and interpreter version information. The platform module includes tools to see the platform's hardware, operating system and interpreter version information where the program is running. There are four functions for getting information about the current Python interpreter. python_version() and python_version_tuple() return different forms of the interpreter version with major, minor and patch level components. python_compiler() reports on the compiler used to build the interpreter. And python_build() gives a version string for the build of the interpreter.

Platform() returns string containing a general purpose platform identifier. The function accepts two optional Boolean arguments. If aliased is true, the names in the return value are converted from a formal name to their more common form. When terse is true, returns a minimal value with some parts dropped.

PRODUCTIVITY AND SPEED: It is a widespread theory within development circles that developing Python applications is approximately up to 10 times faster than developing the same application in Java or C/C++. The impressive benefit in terms of time saving can be explained by the clean object-oriented design, enhanced process control capabilities, and strong integration and text processing capacities. Moreover, its own unit testing framework contributes substantially to its speed and productivity.

PYTHON IS POPULAR FOR WEB APPS: Web development shows no signs of slowing down, so technologies for rapid and productive web development still prevail within the market. Along with JavaScript and Ruby, Python with its most popular web framework Django has great support for building web apps and is rather popular within the web development community.

OPEN-SOURCE AND FRIENDLY COMMUNITY: As stated on the official website, it is developed under an OSI-approved open source license, making it freely usable and distributable. Additionally, the development is driven by the community actively participating and organizing conference, meet-ups, hackathons etc. fostering friendliness and knowledge-sharing.

BROAD APPLICATION: It is used for the broadest spectrum of activities and applications for nearly all possible industries. It ranges from simple automation tasks to gaming, web development, and even complex enterprise systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

These are the areas where this technology is still the king with no or little competence. Machine learning as it has a plethora of libraries implementing machine learning algorithms. Web development as it provides back end for a website or an app. Cloud computing as Python is also known to be among one of the most popular cloud-enabled languages even used by Google in numerous enterprise-level software apps.

PYTHON COMPILER: The Python compiler package is a tool for analyzing Python source code and generating Python bytecode. The compiler contains libraries to generate an abstract syntax tree from Python source code and to generate Python bytecode from the tree. The compiler package is a Python source to bytecode translator written in Python. It uses the built-in parser and standard parser module to generate a concrete syntax tree. This tree is used to generate an abstract syntax tree (AST) and then Python bytecode. The full functionality of the package duplicates the built-in compiler provided with the Python interpreter. The package is useful for a variety of purposes. It can be modified more easily than the built-in compiler. AST, it generates is useful for analyzing Python source code.

VI. CONCLUSION

This project describes the cloud data secure storage systems a feasible approach to solve the storage security problem especially prevention from user data leakage at cloud storage layer. CSSM could also effectively protect cryptographic materials from storage perspective with improved data security. We can achieve the better cloud storage management protocol is implemented in this system for best cloud storage management. This proposed algorithm provide the better integrity of data storage management. CSSM adopted a combined approach of data dispersal and encryption technologies, which can improve the data security and prevent attackers from stealing user data. The experimental results show that CSSM can effectively prevent user data leakage at cloud storage layer. In terms of performance, the increased time overhead of CSSM is acceptable to users. This paper provides a feasible approach to solve the storage security problem, especially prevention from user data leakage at cloud storage layer. CSSM could also effectively protect cryptographic materials from storage perspective.

REFERENCES

[1]. A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan and L. Mostarda, "Capturing-the invisible(CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," IEEE Access, vol. 8, pp. 104956–104966, 2020.

[2]. M. Kumar, A. Rani, and S. Srivastava, "Image forensics based on lighting estimation," Int. J. Image Graph., volume 19, no.3, July 2019, Art. no. 1950014.

[3]. M. Kumar, S. Srivastava, and N. Uddin, "Image forensic based on lighting estimation," Austral. J. Forensic Sci., volume 51, no.3, pp. 243–250, August 2017.

[4]. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Computer Secure volume 72, pp. 1–12, January 2018.

[5]. Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," volume 379, pp. 42–61, February 2017.

[6]. The OpenStack Project. OSSA-2015-006: Unauthorized Delete of Versioned Swift Object. Accessed: April. 14, 2015. [Online]. Available:https://security.openstack.org/ossa/OSSA-2015-006.html

[7]. The OpenStack Project. OSSA-2015-016: Information Leak Via Swift Tempurls. Accessed: August 26, 2015. [Online]. Available:https://security.openstack.org/ossa/OSSA-2015-016.html

[8]. The OpenStack Project. Possible Glance Image Exposure Via Swift. Accessed: February 23, 2015. [Online]. Available: https://wiki. openstack.org/wiki/OSSN/OSSN-0025

[9]. Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: August 8, 2018. [Online]. Available:https://downloads.cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloudcomputing-deep-dive.pdf

[10]. The OpenStack Project. OpenStack Security Advisories. Accessed: February 2, 2015. [Online]. Available:https://security.openstack.org/ossalist. Html