International Journal of Scientific Research in Science, Engineering and Technology
© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
doi : https://doi.org/10.32628/IJSRSET

AIS-Based Data Security Strategy for Cloud Computing

B. Kavitha
Lecturer, Department of Computer Engineering, IRT polytechnic college, Chennai, India

ARTICLEINFO

Article History:
Received : 07 June 2017
Accepted : 25 August 2017

Publication Issue :
Volume 3, Issue 5
July-August-2017
Page Number :
851-855

ABSTRACT

Data security is crucial to cloud computing because of its rapid development and broad range of applications. In this paper, a novel data security approach based on an artificial immune system on the HDFS architecture for cloud computing was presented. First, the key elements that affect data security in cloud environments were taken for analysis. Next, an enhanced cloud computing security model, the HDFS architecture, and a data security model were analyzed. The artificial immune algorithm's relationship to the dynamic selection and negative selection algorithms utilized in the suggested system, as well as how they relate to cloud computing, are finally illustrated in full. The suggested system attests to the efficacy of the cloud computing data security strategy based on AIS-artificial immune system algorithm.

Keywords: Data Security, Cloud Computing, AIS, HDFS

I. INTRODUCTION

A new computing paradigm, cloud computing is the result of the development of load balancing, virtualization, network storage, and distributed and parallel computing. It is also the evolutionary descendant of grid, utility, and parallel computing. The primary goal of cloud computing is to provide infrastructure, platform, and software services while centralizing an enormous number of network-connected computer resources into a virtualized pool. The term "cloud" refers to this network that provides a range of computing resources. Cloud computing, an Internet-based supercomputing paradigm, lets users share large amounts of data, software, and hardware on-demand and pays them based on actual consumption. As a result, just like gas, electricity, and water, computer power can be easily bought and sold over the network at a reasonable cost. Comparable to the innovation of electric power, which moved from a single generator to a centralized electric power plant, is cloud computing. Security issues with cloud computing have been reported. The goal of this paper is to implement a cloud computing security strategy.

II.RELATED WORKS

Vision for computing in the twenty-first century, [1] describes many paradigms that promise to realize this vision for computing utilities, defines cloud computing, and offers the architecture needed to build market-oriented clouds using VM technology.[2] Map reduce scalable algorithms and various technologies were discussed.[3] The stability

and stabilization issues for a particular class of uncertain time-delay systems are examined in this study.[4] Discusses computing issues in cloud environment.[5] suggested a technique that achieves a balance between diversity and convergence speed, enhancing speed and accuracy while preventing premature convergence.[6] Speaks about secure virtual machines in cloud computing.[7] This work is concerned with file integrity, stronger and faster encryption algorithms, and authentication.

III.PROPOSED SYSTEM

The issues with data security in cloud computing are more serious. Data security aims to use technological means to ensure that data is managed under reasonable control and that it is not unlawfully accessed or altered while being processed.

The next Apache fundamental software project, Hadoop, is open source and has many uses in today's world. The Hadoop distributed file system, or HDFS, is a fundamental component that offers data redundancy in applications, potentially leading to advancements in data security strategies. Because of Google's backing and the benefits of open source, HDFS—which is typically utilized in distributed file systems architecture for large-scale cloud computing—has been implemented as the foundation for cloud infrastructure. Its design objective is to operate on commercial hardware. A cloud computing system may be vulnerable to data security threats for a number of reasons, such as an unstable cloud network, a failed network node, extremely high user traffic, and inconsistent data.

Data would become insecure in one of the aforementioned scenarios. In order to keep each node's data block addressable, it is ensured data consistency. Hence, to ensure viewgraph consistency rather than data accessible on every online node, maintain system consistency is necessary.

A) ADVANTAGES

- It has been utilized as the foundation for cloud computing services.
- By keeping distinct files, data block granularity determines the file system's efficiency.
- To guarantee data block addressability on every node, data consistency is maintained.

IV. SYSTEM ARCHITECTURE

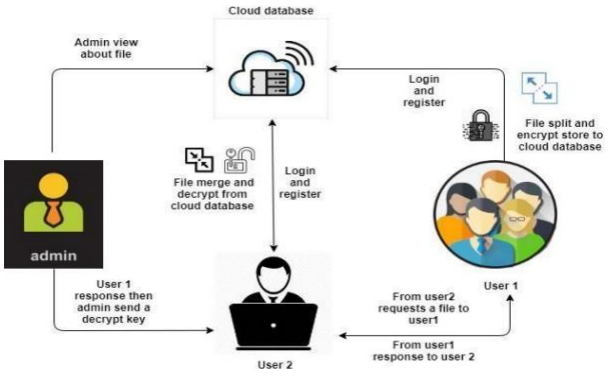


Fig 1. Architecture

Data Flow Diagram

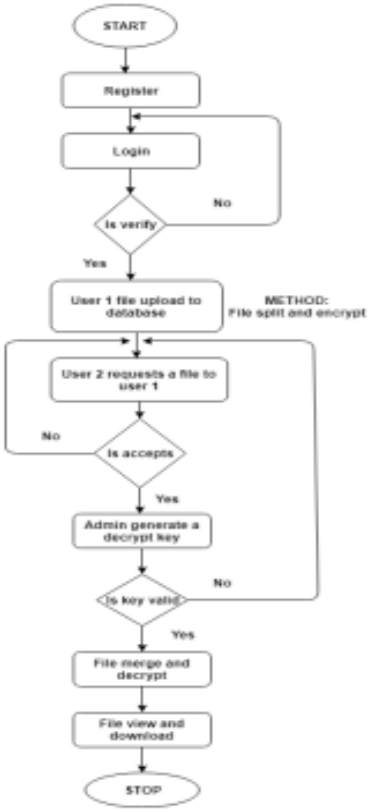


Fig. 2 Data Flow Diagram

Use Case

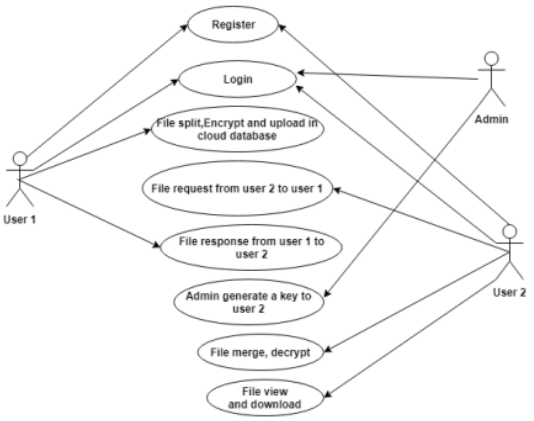


Fig 3. Use Case diagram

Sequence Diagram

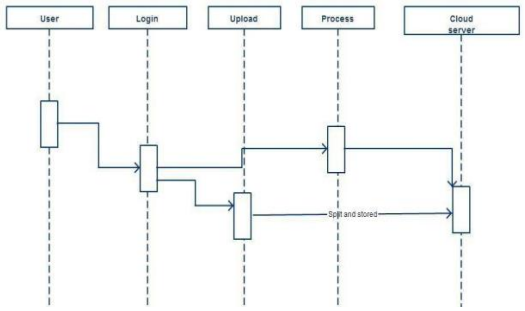


Fig 4. Sequence Diagram

CLASS DIAGRAM

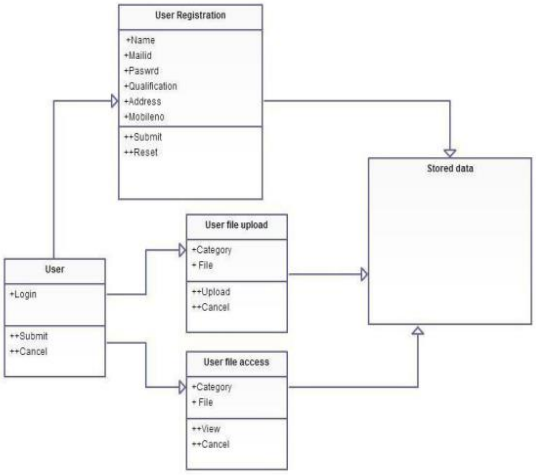


Fig 5. Class Diagram

A) MODULE DESIGN

- User Registration
- File Uploading
- HDFS architecture
- Data security strategy based on AIS

MODULES DESCRIPTION

User Registration

The user has to have a cloud account. The data of the logged-in user will be kept on cloud storage. Each registered user will receive a unique User ID. After that, the registered user can upload files, safely store them on the cloud, and quickly obtain the necessary data.

File Uploading

The procedure of uploading files is done in this module. The specific file that the cloud user wishes to upload will be encrypted. The public and private keys for the encrypted file will be produced. After that, the user can upload the encrypted file to many clouds.

HDFS Architecture:

Master/slave architecture supports HDFS. A single Name Node, a master server that controls client access to files and maintains the file system namespace, makes up an HDFS cluster. Furthermore, numerous Data Nodes—typically one for each cluster node—manage storage that is connected to the nodes they operate on.

User data can be saved in files thanks to HDFS, which also makes a file system namespace visible. A file is divided internally into one or more blocks, each of which is kept in a collection of Data Nodes. File system namespace activities, such as opening, shutting, and renaming files and directories, are carried out by the Name Node. Additionally, it establishes how blocks are mapped to data nodes.

The read and write requests from the file system clients are fulfilled by the Data Nodes. In addition, the Data Nodes create, remove, and replicate blocks in response to commands from the Name Node.

The approach is based on Monte Carlo methods, a class of randomized algorithms. It specifically makes use of simulated annealing and Monte Carlo integration. In our work, files saved in the data node might be recognized and organized in the optimized node while the negative selection method is used to mature the antibody. Assumed to be k is the file block number. An algorithm of negative selection was used to mature the k randomly produced antibodies.

AIS based Data Security

Artificial immune systems (AIS) are a subset of rule-based, computationally intelligent machine learning systems in artificial intelligence that draw inspiration from the concepts and mechanisms of the vertebrate immune system. For usage in problem solving, the algorithms are usually based on the learning and memory properties of the immune system.

V. OUTPUT AND RESLUTS

Fig 6. User Login

Fig 7. User Registration

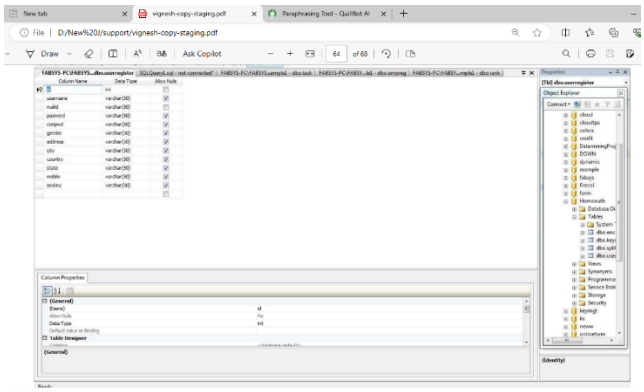
Fig 8. File Upload

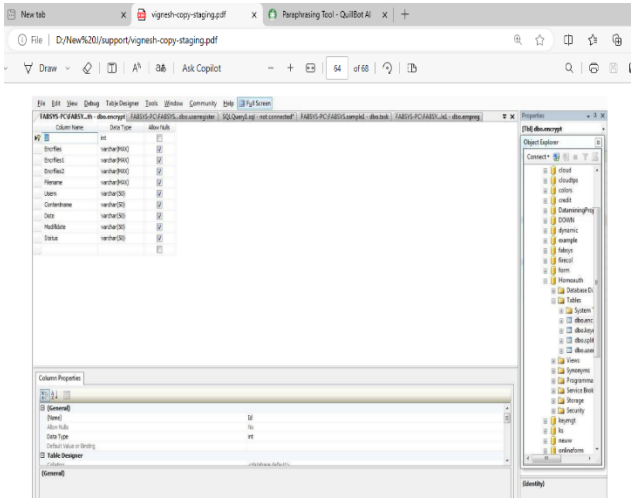
Fig 9.Block Split

Fig 10.File Encrypt

Fig 11. Encrypted File Upload

DATA TABLES





VI. CONCLUSION

Security concerns have elevated to the top of the priority list as cloud computing grows. This study analyzes the security requirements of HDFS, a cloud computing framework, to explore the cloud computing environment and related safety issues. A cloud computing model for data security is finally concluded.

II. REFERENCES

[1]. Rajkumar Buyya Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities (2008), 322-326.

[2]. Jean-Daniel Cryans, Criteria to Compare Cloud Computing with Current Database Technology (2008), 23-26.

[3]. Shun-Hung Tsai, Y.-H. Chang, Sliding Mode Control for A Class of Uncertain Time Delay System, Applied Mathematics & Information Sciences. (2012), 53S-59S. [4] Mladen A. Vouk Cloud Computing Issues, Research and Implementations Journal of Computing and Information Technology - CIT 16, (2008), 235246

[4]. Huantong Geng, Yanhong Huang, Jun Gao and Haifeng Zhu. A Self-guided Particle Swarm Optimization with Independent Dynamic Inertia Weights Setting on Each Particle. Applied Mathematics & Information Sciences. (2012), 31S-34S.

[5]. Cloud Computing Security: making Virtual Machines Cloud- Ready, www.cloudreadysecurity.com (2008), 34-45. [7] Dai Yuefa,Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, “Data Security Model for Cloud Computing”, Proceedings of the 2009 InternationalWorkshop on Information Security and Application (IWISA 2009), 141-144.

[6]. Dai Yuefa,Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, “Data Security Model for Cloud Computing”, Proceedings of the 2009 InternationalWorkshop on Information Security and Application (IWISA 2009), 141-144.

[7]. David Chappell, Introducing the Azure Services Platform October (2008), 1232-1240