ISSN: 2366-1313

NAPA: SECURE AND EFFICIENT CLOUD DATA PROCESSING THROUGH DISTRIBUTED EXECUTION

[1]Mrs. B.Mounika,[2]R.Devi Sri Prasad,[3]P.Ranjith

[1]Assistant Professor, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

mounikagoudgundlapally@gmail.com

[2, 3, BTech] Student, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad

Radamdevisriprasad@gmail.com,ranjithnani282@gmail.com

ABSTRACT:

With the popularity of cloud computing, applications are being hosted remotely more and more for a variety of reasons, necessitating effective scheduling and low-latency execution. Since users no longer have control over their data on distant servers, this raises questions around instance data security. Although encryption provides anonymity, server-side assaults cannot always be prevented by it. We provide the Network Attentive Payload Allocation (NAPA) method as a solution to this. It splits instances up into smaller payloads, which are then run simultaneously on several servers. To ensure efficient execution and data protection, our method arranges instances among fog servers, cloud servers, and local PCs. Effective hash functions are used in our strategy to protect instance data during distribution. Our technique is validated by theoretical analysis and simulation, which shows that it is successful in securing instance data.

Keywords*:*Network Attentive Payload Allocation (NAPA),cloud computing.

I INTRODUCTION

When the twenty-first century began, computer technology advanced quickly. An new technology called cloud computing was initially introduced by San Jose at SES 2006 (Search Engine Strategies 2006) and defined by NIST (National Institute of Standards and Technology). Ever since its proposal, cloud computing has garnered significant interest from many societal segments. Cloud computing has developed throughout time thanks to the efforts of several individuals. Next, various cloud-based technologies that originate in cloud computing are described. One significant component of these is cloud storage. The amount of user data is growing exponentially due to the quick expansion of network capacity. The local machine's capacity is no longer sufficient to meet the user's needs. As a result, individuals look for novel approaches to data storage. A rising number of customers use cloud storage in search of stronger storage capacity. The trend of storing data on public cloud servers is expected to continue in the coming years, as cloud storage technology becomes more widely used. A cloud computing system that offers data management and storage is called cloud storage. Cloud storage combines distributed file systems, network technologies, and a cluster of applications to facilitate the coordinated operation of several storage devices. Many businesses now provide a range of cloud storage services, including Baidu Cloud, iCloud, Dropbox, Google Drive, and others. These businesses succeed by drawing in amusing subscribers with their big storage capacities and array of services linked to other well-known apps. There are still a number of security issues with cloud storage services, though. The privacy issue is the most important of those security-related concerns. A few well-known instances of cloud storage privacy leaks occurred in the past. For instance, during the 2014 Apples Cloud leak, a large number of Hollywood actresses' personal images that were kept on cloud storage were taken. Users were concerned about the protection of their data kept on cloud servers because of the commotion this occurrence produced. The user directly uploads data to the cloud server, as seen in Fig. 1. After that, the Cloud Server Provider (CSP) will handle data management instead of the user. As a result, users have no real control over how their data is physically stored, leading to a division between data ownership and management. The data saved in the cloud is freely accessible to and searchable by the CSP. To get the user's data, the attackers might also target the CSP server in the interim. Users run the risk of data loss and information leakage in the two scenarios mentioned above. Conventional approaches to protect cloud storage for the aforementioned issues often center on data encryption or access limits. In actuality, these techniques can solve the majority of these issues. But no matter how good the algorithm gets, none of these techniques can effectively counteract the internal attack.

II. LITERATURE SURVEY

1."Maintaining the Balance between Privacy and Data Integrity in Internet of Things" by Bhuiyan et al. (2017)

Explores the critical issue of balancing privacy and data integrity in IoT systems. The writers discuss the difficulties in guaranteeing data integrity and privacy in Internet of Things settings and offer ways to allay these worries. They emphasize the significance of putting strong security measures in place to protect sensitive data and preserve data integrity in Internet of Things applications through their research. This study makes a significant contribution to the continuing discussions about how to handle privacy and security issues in the quickly changing IoT environment.

2."Fog Computing and Its Role in the Internet of Things" by Bonomi et al. (2012)

Explores the concept of fog computing and its significance in supporting the Internet of Things (IoT). The writers talk about the difficulties typical cloud computing architectures have in providing the high bandwidth and low latency needed for Internet of Things applications. As a potential remedy, they suggest fog computing, which brings cloud services closer to Internet of Things devices at the network's edge. This work offers insightful information on the nascent topic of fog computing and how it could be able to meet the particular needs of Internet of Things applications.

3. "Wireless Sensor Network Survey" by Yick et al. (2008)

Provides a comprehensive survey of wireless sensors networks (WSN). The writers examine the development, uses, and difficulties associated with WSNs, addressing subjects including network architecture, security, energy efficiency, and communication protocols. They provide insightful information on the state-of-the-art in WSN research and development through their survey, emphasizing significant developments and suggesting topics for more investigation. For academics and practitioners interested in learning about the features and possible uses of wireless sensor networks, this article is an invaluable resource.

4."Cloud Computing: Distributed Internet Computing for IT and Scientific Research" by Dikaiakos et al (2009).

Gives a summary of cloud computing and the ways it may be used for scientific and IT research in distributed internet computing. The writers go over the features and benefits of cloud computing, such as its cost-effectiveness, scalability, and flexibility. They also look at the difficulties and possible developments in cloud computing, emphasizing how it may completely transform a number of industries.

5."Reliable Wireless Connections for Fast-Moving Rail Users Based on a Chained Fog Structure" by T. Wang et al. (2017)

Investigates the usage of a linked fog structure to establish stable wireless connections for fast-moving rail passengers. The authors provide a novel architecture that makes use of fog computing to improve the dependability and continuity of wireless connections, especially in busy settings like railroads. By tackling the difficulties of providing mobile consumers moving at fast speeds with continuous connectivity, this research advances the area of information science.

III SYSTEM ANALYSIS

EXISTING SYSTEM

- **Real-world incidents:** The essay highlights the vulnerability of cloud infrastructures with examples from events like the Amazon outage (2012), Google DoS attack (2009), and Akamai assault (2004).

- **Loss of control**: When customers turn their data over to cloud providers or brokers, they forfeit control over their instances, which raises privacy issues.

- **Unrestricted access:** Unrestricted access to data is granted to providers and brokers, and data theft attempts can be made by anonymous attackers.

- **Limited focus on privacy:** Current resource allocation techniques disregard data privacy concerns in favor of efficiency and local data encryption.

ISSN: 2366-1313

- **Need for secure instance management:** The necessity of data management and secure instances in cloud environments is emphasized throughout the literature.

PROPOSED SYSTEM

This text introduces NAPA and I NAPA, proposed solutions to address data privacy concerns in cloud environments.

- **NAPA:** This method splits up application instances so they can run more effectively on distant computers.
- **Data protection:** According to their level of computing load (high, moderate, or light), fragmented instances are categorized.
- **NAPA**: After analyzing instance payloads, this clever method schedules them at the proper times:
- **Data partitioning and encryption:** Complete data theft is made more difficult by fragmentation and different encryption for every site.
- **Unauthorized access protection:** Even cloud providers with limited access are unable to get all of the data.
- **Adaptive behavior:** I NAPA manages demanding and delicate jobs with intelligence.

IV IMPLEMENTATION

Architecture:

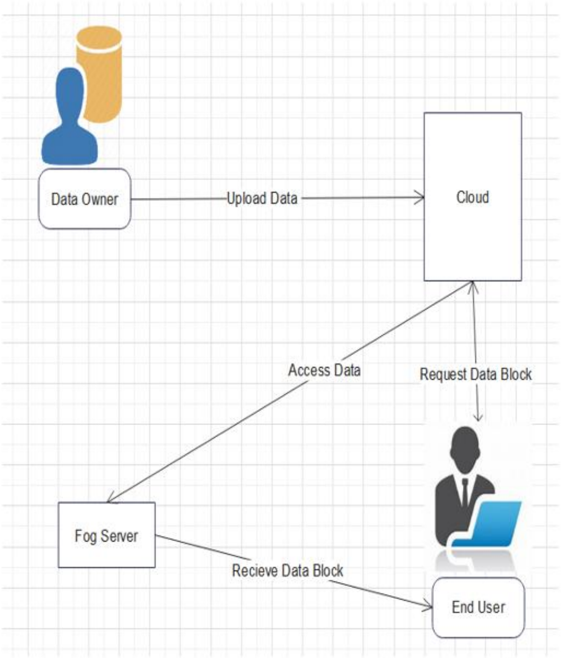


Fig-1. Architectures of the system model

MODULES

Data Owner

He enters his or her login credentials in this module. The owner can upload data and view file blocks after logging in.

End User

He enters his or her login credentials in this module. The user may perform many tasks after logging in, including downloading files,

ISSN: 2366-1313

seeing all files, and requesting search permissions.

Fog Server

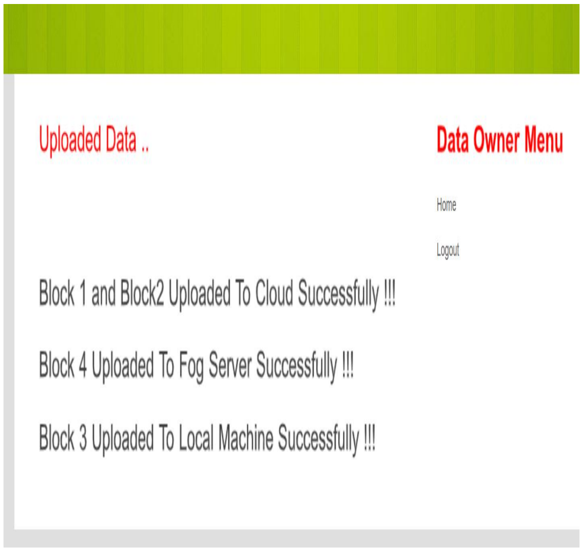
The Fog Server may do the following tasks in this module, including viewing file blocks, seeing all Fog user details, and processing end user actions to deliver data blocks.

Cloud Server

In addition to acting as a server for data storage, the cloud server may perform the following functions: view end users and authorize, view data owners and authorize, Examine Every Stored Record, View the following: Transactions, Attackers, Search Request, Download Request, Files Rank, Time Delay, and Throughput charts.

V RESULT AND DISCUSSION

Data Owner:



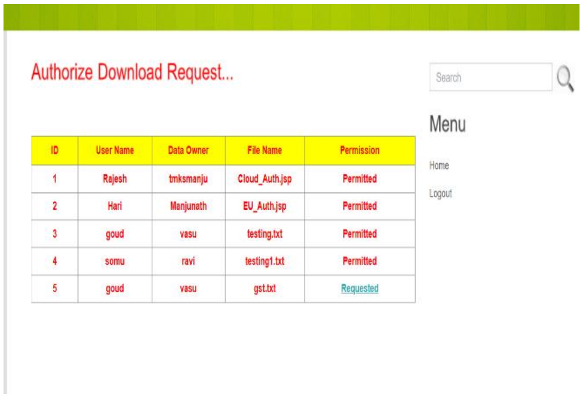
Block 1 and Block2 Uploaded To Cloud Successfully !!!

Block 4 Uploaded To Fog Server Successfully !!!

Block 3 Uploaded To Local Machine Successfully !!!

Cloud Server:

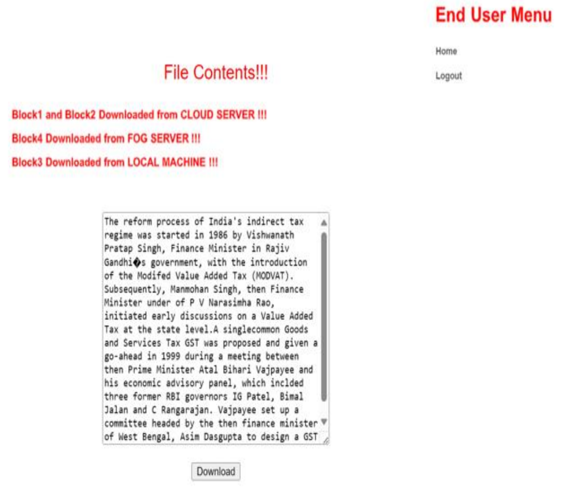
The data is stored in the cloud when the data owner uploads it, and the end user requests access to the cloud in order to receive the data.



ID	User Name	Data Owner	File Name	Permission
1	Rajesh	tmksmanju	Cloud_Auth.jsp	Permitted
2	Hari	Manjunath	EU_Auth.jsp	Permitted
3	goud	vasu	testing.txt	Permitted
4	somu	ravi	testing1.txt	Permitted
5	goud	vasu	gst.txt	Requested

End User:

If the cloud grants the end user's request then. As seen in the illustration, the end user can obtain the owner's data from the cloud.



Block1 and Block2 Downloaded from CLOUD SERVER !!!

Block4 Downloaded from FOG SERVER !!!

Block3 Downloaded from LOCAL MACHINE !!!

```
The reform process of India's indirect tax
regime was started in 1986 by Vishwanath
Pratap Singh, Finance Minister in Rajiv
Gandhi�s government, with the introduction
of the Modifed Value Added Tax (MODVAT).
Subsequently, Manmohan Singh, then Finance
Minister under of P V Narasimha Rao,
initiated early discussions on a Value Added
Tax at the state level.A singlecommon Goods
and Services Tax GST was proposed and given a
go-ahead in 1999 during a meeting between
then Prime Minister Atal Bihari Vajpayee and
his economic advisory panel, which inclded
three former RBI governors IG Patel, Bimal
Jalan and C Rangarajan. Vajpayee set up a
committee headed by the then finance minister
of West Bengal, Asim Dasgupta to design a GST
```

VI CONCLUSION

We gain a lot from the evolution of cloud computing. One practical technology that allows customers to increase their storage space is cloud storage. But cloud storage also brings with it a number of security issues. Users that use cloud storage experience a separation of ownership and management of their data as they no longer have actual control over the data's physical storage. To address the issue of privacy protection in cloud storage, we develop a Hash-Solomon algorithm and suggest a TLS framework based on the fog computing concept. This theoretical safety study shows that the concept is workable. We can guarantee the privacy of data on each server by equitably assigning the ratio of data blocks kept on various servers. However, technically speaking, it is impossible to crack the encoding matrix. Additionally, incomplete information can be protected by employing hash transformation. This approach may effectively finish encoding and decoding during the experiment test without affecting the cloud storage efficiency. Moreover, we devise a rational comprehensive efficiency measure to get optimal efficiency, and we also discover that the Cauchy matrix exhibits greater efficiency throughout the coding procedure.

FUTURE ENHANCEMENT

1. Enhanced Security Protocols: enhancing security procedures on a constant basis to meet changing risks and weaknesses in cloud computing settings. To further improve data safety, this may entail investigating cutting-edge encryption methods, intrusion detection systems, and anomaly detection algorithms.

2. Integration of Machine Learning: use machine learning techniques to forecast threats and detect anomalies in order to proactively spot any security breaches and take immediate corrective action.

3. Scalability and Performance Optimization: Improving the Network Attentive Payload Allocation (NAPA) technique's scalability and performance to effectively manage massive installations and huge data volumes while reducing latency and resource overhead.

4. Privacy-Preserving Techniques: investigating and putting into practice new privacy-preserving measures to guarantee user data integrity and confidentiality, especially in situations where sensitive data is processed and stored on the cloud.

5. Compatibility with Emerging Technologies:

To future-proof the project against technological improvements, it is imperative to ensure compatibility with upcoming cloud computing standards and technologies including edge computing, blockchain-based solutions, and quantum-resistant cryptography.

6. User-Friendly Interfaces:

creating intuitive tools and user interfaces to streamline the NAPA method's deployment, setup, and management and increase its accessibility for a larger group of people and organizations.

7. Continuous Monitoring and Improvement:

Putting in place a system for ongoing project monitoring, assessment, and enhancement in order to handle changing security risks, performance snags, and user input. Regular updates, fixes, and improvements based on user input and real-world usage may be part of this.

VII REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloudcomputingenvironments,"inProc.IEEEInt.Conf.Commun.,2014, pp. 2969–2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.

[5]Y.Li,T.Wang,G.Wang,J.Liang,andH.Chen,"Efficientdatacollection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.

[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[8] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[9]R.Kulkarni,A.Forster,andG.Venayagamo orthy,"Computationalintelligenceinwirelesss ensornetworks:Asurvey," IEEE Commun. Surv. Tuts., vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Comput., vol. 41, pp. 219–230, 2017.

[12]Z.Fu,F.Huang,K.Ren,J.Weng,andC.Wan g,"Privacy-preservingsmart semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

[13] J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.

[14] Prasadu Peddi (2015) "A review of the academic achievement of students utilisinglarge-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

[15] Prasadu Peddi (2017) "Design of Simulators for Job Group Resource Allocation Scheduling In Grid and Cloud Computing Environments", ISSN: 2319-8753 volume 6 issue 8 pp: 17805-17811.

AUTHORS

Mrs.B.Mounika,AssistantProfessor Dept. of CSE, Teegala Krishna Reddy Engineering College Meerpet, Hyderabad.

Email: mounikagoudgundlapally@gmail.com

Mr. R.Devi Sri Prasad, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: Radamdevisriprasad@gmail.com

Mr. P.Ranjith, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: ranjithnani282@gmail.com