Strategic Survey on Security and Privacy Methods of Cloud Computing Environment

[1]Sai Srinivas Vellela, Research Scholar, Dept. of CSE Saveetha School of Engineering,
Chennai - 602105
[2]Dr.R.Balamanigandan, Asst.Professor, Dept. of CSE, Saveetha School of Engineering,
Chennai – 602105
[3]Dr.S.Phani Praveen, Asst.Professor, Dept. of CSE, PVP Siddhartha Ins-Vijayawada,
Andhra Pradesh, India – 520007

Email id: sais1916@gmail.com[1], balamanigandanr.sse@saveetha.com[2], phani.0713@gmail.com[3]

Article Received: 05 May 2022 *Article Accepted: 08 May 2022* *Article Published:10 May 2022*

Citation
Sai Srinivas Vellela , Dr.R.Balamanigandan, Dr.S.Phani Praveen (2022), “Strategic Survey on Security and Privacy Methods of Cloud Computing Environment”, Journal of Next Generation Technology, 2(1), 70-78

Abstract

This analysis implements a strategic review on cloud computing environment confidentiality and privacy approaches. In an IT sector, the recently discovering phenomenal technology is the Cloud Computing (CC) as it has a capability of accessing data anytime from to anywhere. There is a rapid improvement in cloud computing process. Large organizations are used to save and make data accessible in cloud infrastructure. Information is stored in very effective way to obtain the dynamic storage and flexible data. In this cloud computing environment is utilized with privacy methods. To overcome the problems of security, different privacy preserving techniques are introduced. In cloud storages the integrity of data mechanism is provided and for client’s data security is provided. Hence the study says that privacy preserving techniques provide better security.

Key words: - Cloud Computing (CC), security and privacy, Privacy preserving techniques.

I. Introduction

By using the applications of services, processes extraction of cloud computing resources will be done. Based on the user device or location consequences of services will be introduced. Actual data hardware is established in the cloud environment for hardware and software business. Based on the cloud services entire structure is build and resources will be used the pay per basis. Fast access is provided for the entire structure to lower the price of service in CC process. Based on the internet connectivity the CC is separated dependent on connectivity of internet and visualization techniques.

Untreated cloud servers are avoided by every cloud server to hack the malicious medical reports. Cloud provider will debit and credit the reports of hackers from insiders. To satisfy the requirements of cloud data storage data is accessed from the creation of services. The service provided by the cloud data is high security and data integrity in all cases.

Computing devices will be reliable in nature by making the infrastructure more powerful. Internal and external threats are utilized for facing the data integrity ranges.

The status of out sourced data is motivated regarding to the cloud user's faithfulness. Fault tolerance technique is added to the outsourced data for data protection and reduction of errors. Integrity checking plays very important role in cloud computing process. Regenerating-code-based cloud storage is used based on the scheme of public auditing [13] [14].

To provide the opportunities of online services confidential and private information is utilized. This is rapidly increasing the growth in very effective way. Valuable knowledge is enabled for collecting the data by exploiting the mining of data. Private datasets are utilized to control the data mining process leakages. Data is shared by the parties to prevent the privacy concerns. Few data is provided to the system for providing the security and increasing the integrity.

In medicine, banking and scientific researcher's data will be mined in real time applications. Knowledge discovery is needed to perform the mining of data because of knowledge discovery. Different perceptive are utilized in very large-scale application to get high integrity. Classification is most widely used in the mining applications for better efficiency.

For the users to store the data cloud is most widely utilized. Therefore, in technical world cloud computing plays very important role. By using the encryption form the data is secured in the cloud and this will be the major issue in the cloud. Data is leaked after encryption of data and time will be consumed very effectively by using the privacy preserving techniques in cloud computing systems [15] [16].

Cloud computing applications require users to privately store information in the cloud. Cloud storage security is the important CC security concerns. This protects privacy of user's data as well as the need to keep cloud data in an encrypted state. The data on the cloud service providers cannot be kept confidential because they are unreliable third parties therefore cloud service providers are used to complete various operations on data [17].

II. SECURITY ISSUES IN CLOUD COMPUTING

The challenges in CC is addressed in three levels which are given below:

2.1 Terminal

Wireless access is allowed for open type operating system for internet at any time anywhere. Personalization and software are the third-party services which will support the system in very effective way. Hence in malware, vulnerabilities and software terminals provide the issues in cloud environment.

1) **Malware:** the information in malware will be automatically downloaded and save the data of personal users. Different types of malware software are introduced but limited sources are given to the terminals of cloud environment.
2) **Software Vulnerabilities:** the vulnerabilities are transferred by the applications to the network to get high integrity. By using cipher text context, the data is stored in very effective way. The data is transferred to the network using software application by using user name and password. Mobile phones are allowed illegally based on the same networks. But in this the information is not secured effectively. Mobile phones are destructed by the attackers in some conditions in an operating system [18] [19] [20].

2.2 Network Security

Any device can access the network and provide communication through SMS (Sending Messaging Services), phone services and other internet services. Smart phones will be accessed by the Bluetooth networks. Security threats and malicious attacks are accessed by using these models.

2.3 Cloud computing

Based on two issues the security in cloud computing is addressed they are data privacy protection and reliability. The two issues are discussed in below:

1) **Platform Reliability:** Valuable information resources are provided to the cloud data. Because of that attacks will be performed for the data. The attacks obtained from cloud users or insiders and outside malware. Cloud services are destroyed by attacking the target. Denial of Service is one of the services which will destroy the platform in very effective way.
2) **Data and Privacy Protection:** Based on different locations the data is managed and ownership. But this data will be available at different locations. In the same way exact location cannot reside by the user. In this data will be stored in very effective way. Hence in CC environment the privacy and data protection will be performed.

III. LITERATURE REVIEW

A Secure and Efficient Query Processing Algorithm over Encrypted Database in Cloud Computing [1]

Databases must be encoded prior being outsourced to cloud, according to investigation on privacy-preserving database outsourcing that has recently highlighted in CC context

Table. 1: Parameters Used

Parameter	Description
n	Number of records data (4000 to 28000), default (28000) and for synthetic data 30000.
h	Tree depth of kd tree (7 for real data, 11 for synthetic data)
k	Number of nearest neighbors for KNN (5,10,15,20)
m	Number of attributes in a record

As a result, several KNN query processing algorithms that protect privacy have been suggested for use with encrypted databases. The current plans, however, are either ineffective or insecure. In this analysis, it therefore suggests a reliable and effective KNN query processing technique [21] [22].

Achieving Efficient and Privacy-Preserving Set Containment Search over Encrypted Data [2]

A set containment search, which aims to find all entries in a given query set, has drawn a lot of interest. In the meantime, due to the exponential growth of data, data owners commonly outsource the content to the cloud and develop a cloud server to offer set containment search operations. But since the cloud server cannot be completely trusted and the information could be sensitive, the owners of the data can simply encrypt the information before outsourcing it. The set containment search's functionality is invariably hampered by the encryption technology, despite the fact that it can protect data privacy.

There are still problems with search effectiveness and security in numerous current observations on confinement set search on outsourced content. In this investigation, they address the aforementioned problems and offer a set confinement search strategy that is effective and protects privacy. Set containment or intersection encryption (SCIEEnc) is created by first employing an asymmetric scalar-product-preserving encryption approach they developed. After that, radix tree is constructed to indicate records collection. According to security analysis as well as performance evaluation, they provide method for successfully performing set containment search with maintaining the privacy of set entries, query parameters, and query results. This method is dependent on radix tree and SCIE-Enc construction.

Efficient Privacy-Preserving Similarity Range Query based on Pre-Computed Distances in e Healthcare [3]

A rising number of healthcare facilities are moving their patient data to the cloud due to the development of smart e Healthcare and CC technologies. Healthcare facilities frequently encrypt data prior outsourcing it to protect confidentiality of private details. Even though data encryption can protect user privacy, it invariably limits the functionality of queries on the outsourced data. The most often utilized query operations are similarity range queries out of all the practical ones.

To the best of our knowledge, many current investigations on similarity range queries over external data still experience query process effectiveness problems. Because of this, they offer an effective privacy-preserving similarity range query technique in this investigation that is dependent on the pre-computed distance approach and aims to increase query efficiency. To be more specific, they start by explaining the Pre DSQ-algorithm, which can speed up queries by figuring out some distances ahead of time. Then, using an asymmetric scalar-product-preserving encryption technique, they suggest privacy-preserving similarity query approach, protecting the Pre DSQ-algorithm’s confidentiality. Our suggested method is effective and can effectively protect the confidentiality of data records as well as query requests, according to both security assessment and performance analysis results.

Efficient and Privacy-Preserving Federated QoS Prediction for Cloud Services [4]

The extensive use of cloud computing has led to the deployment of massive web applications made up of services in many important fields. To ensure the proper operation of cloud applications, Quality of Service (QoS) is a vital indication that is regularly used for service acquisition and modification.

To estimate the values of personalized QoS, previous investigations have suggested collaborative QoS prediction algorithms. However, in practice, collaborative QoS estimation suffers privacy issues. As a result, the threat to privacy has emerged as a major obstacle to the viability of QoS prediction methods. In this analysis, they addressed this major difficulty by presenting this QoS prediction technique using federated learning approaches. By lowering system overhead, they increase prediction effectiveness even more and enable the implementation of suggested method. The experimental findings support the efficiency and reliability of the suggested method, which is assessed using a sizable real-world QoS dataset.

Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-healthcare [5]

Effectiveness as well as accessibility of e-health systems have been greatly enhanced by the combination of wearable wireless gadgets and cloud computing. The cloud allows patients to submit Personal Health Information (PHI) files, from which Health Service Providers (HSPs) may access the necessary data to assess the patient's health. This technology not only lowers healthcare expenses but also offers prompt diagnoses to prevent deaths.

However, sharing sensitive information raises a number of privacy issues. In this review, they present a novel patient health data sharing framework that protects patient privacy and enables HSPs to securely and quickly access and lookup PHI files. Utilizing multi-keyword and keyword range searches, they employ the searchable encryption approach. Different kinds of a numeric comparison inquiry on encoded information are permitted by the privacy-preserving equality check protocol that is being developed. They also categorize PHI files, remove erroneous data, and check the validity of search outcomes using a Bloom Filter variant and a message authentication code. System's viability and effectiveness are demonstrated through simulations utilizing synthetic and actual information, as well as its privacy-preservation capabilities are demonstrated through security analysis.

Privacy-Preserving Techniques for Big Data Analysis in Cloud [6]

Due to digital technology, a wide range of enterprises, including hospitals, retail, e-commerce, supply chains, banks, are producing enormous quantity of information. Data is created by both machines and humans. Examples of this include closed-circuit television streaming and website logs. Smart phones and social media create enormous amounts of data every minute. Decision-making can be supported by the processing and analysis of the vast amounts of data produced from the many sources. Nevertheless, data analytics can violate people's privacy.

The usage of recommendation algorithms by e-commerce websites like Amazon and Flip kart to provide product recommendations to users based on their purchasing patterns might result in inference threats.

Making decisions can be aided by data analytics, but they can raise significant privacy issues. As a result, privacy-preserving data analytics became crucial. This review examines a variety of privacy issues, privacy preservation strategies, and models, as well as their inadequacies. It suggests a modernistic privacy preservation method dependent on a data lake to deal with unstructured information.

Distributed Model Predictive Control for Hybrid Energy Resource System with Large-Scale Decomposition Coordination Approach [7]

It is becoming increasingly vital to use Dynamic Economic Emission Dispatch (DEED) of hybrid energy resources systems in power system operation because of the rising use of renewable energy resources. This analysis presents a large-scale decomposition coordination Distributed Model Predictive Control (DMPC) strategy for hybrid energy resources. And dynamic economic optimal dispatch.

When coping with intermittent energy sources, a rolling optimization method may be useful, which can be implemented using a DEED predictive control approach. Additionally, the computational complexity of the predictive control approach is significantly reduced by splitting it up into a number of smaller systems and using LaGrange multipliers to coordinate those systems.

Third, model predictive control may dynamically optimize randomized or ambiguity problems along with rolling optimization mechanisms because intermittent power supply is unpredictable or random. These subsystem optimization issues are also solved using adaptive dynamic programming, that can optimum the random or unpredictable problem under real-time conditions.

Privacy-Preserving Multi-Channel Communication in Edge-of-Things [8]

Network-oriented apps have undergone a revolution as a result of the Internet's current explosive growth. The fusion of many technologies, like edge computing, CC, internet of things, is driven by a linked setting.

A range of privacy issues, plenty of which are result of communication methods with low levels of security, have emerged throughout the information transmission strategy. Because there are so many processing workloads and communication manipulations, strong security protection techniques often require a higher amount of computational power.

Table 2: Experiment Settings for Main Parameters.

	Data Package	Channel
Setting 1	4	2
Setting 2	8	4
Setting 3	12	4
Setting 4	12	8
Setting 5	20	8
Setting 6	40	12

Table 3: How Much Times DMC2's Generation Time Longer.

Setting 1	Setting 2	Setting 3	Setting 4	Setting 5	Setting 6
4.69	37.02	57.85	66.72	79.45	4576.54

In this case, the Dynamic Multi-Channel Communications (DMC2) architecture is used. Once the bulk of the data becomes extremely large, high-security communications cannot be implemented. This analysis focuses on the issue of the contradiction between effectiveness and privacy preservation and suggests the most recent method for delivering multi-channel communications with higher-level security. Organizations tend to do experiment evaluations to look at how the intended strategy performs.

Privacy-Preserving Outsourced Collaborative Frequent Item set Mining in the Cloud [9]

The way that businesses gather, store, analyse, and retrieve enormous volumes of data has been completely transformed by big data management and analytics. Organizations frequently ought to cooperate and evaluate their combined information in order to fully realize the capability of big data, increasing the accuracy of outcomes. Organizations, however, are unable to easily communicate their information with one another due to legal restrictions and internal privacy standards. The secure multiparty computation methods that are currently available in this direction are quite expensive. In this investigation, they design a technique that allows several users to cooperatively and secretly outsource the encrypted database and regular item set mining tasks to a cloud environment.

Privacy-Preserving Multi-Keyword Search over the Encrypted Data for Multiple Users in Cloud Computing [10]

Data owners are shifting to cloud for outsourcing of own data CC technology gains in popularity. It offers significant computing and storage capacity with simple access and cost savings. The cloud server, however, has various issues, including privacy and access control, so the information is not secure there. As a result, the data is encoded before being uploaded to the cloud to protect the confidentiality of sensitive data, however searching through the encrypted data can be difficult.

The high level of privacy can only be maintained by using a searchable encryption technology. There have recently been a lot of searchable encryption systems suggested, although they were mostly designed for single owner as well as single user scenarios. In this review, they provide a novel method for protecting the privacy of cloud-based data that has been outsourced and supports numerous owners and users. On attribute-based encryption and a tree-based index, the design is based. By doing security and performance analysis, they demonstrate the safety and effectiveness of plan.

Dynamic Data Operations with Deduplication in Privacy-Preserving Public Auditing for Secure Cloud Storage [11]

The use of cloud storage has grown in prominence as CC becomes more prevalent in the IT industry. By outsourcing the storing and processing of massive data files to cloud servers, users can be freed from the load. From the perspective of cloud service providers, it is advisable to use data deduplication approaches to lower the expenses of maintaining huge storage systems and to lower the energy usage on cloud servers.

Table. 4: Performance under Different Number of Sampled Blocks c for High Assurance

S=1	**OUR SCHEME**
Sampled block c	460
Comm. cost (Byte)	160
TPA Comp. time (ms)	533.60
S=10	**OUR SCHEME**
Sampled block c	460
Comm. cost (Byte)	1420
TPA Comp. time (ms)	547.39

Due to the dynamic state of data in cloud storage device, the integrity of data is not the only thing that has to be ensured with such an auditing guideline supporting dynamic data functions for users, but users should also take into account using data deduplication techniques in dynamic data activities for cloud service suppliers to obtain the goal of cost reduction. In order to preserve privacy while allowing for open audits of cloud storage to ensure its security, they present a mechanism in this work that integrates data deduplication by dynamic data activities. Suggested mechanism is incredibly effective and indubitably secure, according to the security and performance assessment.

Privacy Preserving in TPA for Secure Cloud by Using Encryption Technique [12]

All cloud data services involve not only storing data but also sharing it with several users or clients, raising concerns about its integrity because of the possibility of both human and hardware error. Numerous ways are available that enable data owners and public validators to precisely, quickly, and successfully audit the integrity of cloud information without having to see the entire server's contents. Since previous existing procedures will be used to audit the shared data's integrity publicly, the shared data's integrity would be able to be verified by the public verifiers and privacy of the identity included within. In this investigation, they meant a description for TPA employing three-way handshaking mechanism via the Extensible Authentication Protocol (EAP) with freed encryption standard to achieve the privacy-preserving public for auditing. They use Verify Proof implemented by TPA to examine and certify appropriately from cloud. In addition to this approach, the public verifiers cannot see the identification of any section in shared data. Additionally, this will be able to execute multiple auditing tasks concurrently rather than one at a time.

IV. Conclusion

Therefore, a strategic review of security and privacy techniques used in the CC environment was effectively investigated in this analysis. Data validity checking is done under the privilege of data owners. This will provide effective security to the cloud computing environment. Based on auditing process, coefficients are placed randomly. Therefore because of that privacy preserving techniques plays important role in entire system to provide efficient security.

V. References

[1]. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "*Privacy Preserving Public Auditing for Regenerating-Code-Based Cloud Storage*", 2015.

[2]. Henry C.H. Chen and Patrick P.C. Lee, "*Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation*", 2014.

[3]. Henry C.H. Chen, Yuchong Hu, Patrick P.C. Lee, and Yang Tang, "*NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds*", 2014.

[4]. Kan Yang, XiaohuaJia, "*An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing*", 2013.

[5]. Srinivasu, P. N., JayaLakshmi, G., Jhaveri, R. H., & Praveen, S. P. (2022). Ambient Assistive Living for Monitoring the Physical Activity of Diabetic Adults through Body Area Networks. Mobile Information Systems, 2022.

[6]. Cong Wang, Qian Wang, and KuiRen, Wenjing Lou, "*Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing*", 2010.

[7]. J.He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "*Distributed data possession checking for securing multiple replicas in geographically dispersed clouds*" J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1345–1358, 2012.

[8]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "*Toward secure and dependable storage services in cloud computing,*" Apr./Jun. 2012.

[9]. S. G. Worku, C. Xu, J. Zhao, and X.He, "*Secure and efficient privacy preserving public auditing scheme for cloud storage*", 2013.

[10]. A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "*Network coding for distributed storage systems,"* Sep. 2010.

[11]. Y. Zhu, H. Hu, G.-J.Ahn, and M. Yu, "*Cooperative provable data possession for integrity verification in multicloud storage,*" IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012.

[12]. A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "*A survey on network codes for distributed storage,*" Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.

[13]. H. Shacham and B. Waters, "*Compact proofs of irretrievability,*" in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.

[14]. Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., & Vellela, S. S. (2021). Challenges and Issues of Data Analytics in Emerging Scenarios for Big Data, Cloud and Image Mining. Annals of the Romanian Society for Cell Biology, 412-423.

[15]. C. Wang, Q. Wang, K. Ren, and W. Lou, "*Privacy preserving public auditing for data storage security in cloud computing,*" in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[16]. Praveen, S. P., & Rao, K. T. (2019). An effective multi-faceted cost model for auto-scaling of servers in cloud. In Smart Intelligent Computing and Applications (pp. 591-601). Springer, Singapore.

[17]. Phani Praveen, S., & Rao, K. T. (2018). Client-Awareness Resource Allotment and Job Scheduling in Heterogeneous Cloud by Using Social Group Optimization. International Journal of Natural Computing Research (IJNCR), 7(1), 15-31.

[18]. P. Sherubha, S. P. Sasirekha, A. Dinesh Kumar Anguraj, J. Vakula Rani, R. Anitha et al., "*An efficient unsupervised learning approach for detecting anomaly in cloud,*" Computer Systems Science and Engineering, vol. 45, no.1, pp. 149–166, 2023.

[19]. Sindhura, S., Praveen, S. P., Syedbi, S., Pratap, V. K., & Krishna, T. B. M. (2021). An effective secure storage of data in cloud using ISSE encryption technique. Annals of the Romanian Society for Cell Biology, 5321-5329.

[20]. Phani Praveen, S., & Thirupathi Rao, K. (2018). An optimized rendering solution for ranking heterogeneous VM instances. In Intelligent Engineering Informatics (pp. 159-167). Springer, Singapore.

[21]. Praveen, S. P., Tulasi, U., & Teja, K. A. K. (2014). A cost efficient resource provisioning approach using virtual machine placement. Int. J. Comput. Sci. Inf. Technol, 5(2), 2365-2368.

[22]. Praveen, S. P., Krishna, T. B. M., Chawla, S. K., & Anuradha, C. (2021). Virtual Private Network Flow Detection in Wireless Sensor Networks Using Machine Learning Techniques. International Journal of Sensors Wireless Communications and Control, 11(7), 716-724.