How to Cite:
Kholodnaya, V. (2024). Extensive safety measures and performance analysis considering the CPU resource utilization. *Tennessee Research International of Social Sciences*, *6*(2), 7–25. Retrieved from https://triss.org/index.php/journal/article/view/22

Extensive safety measures and performance analysis considering the CPU resource utilization

Verra Kholodnaya
National University of Kyiv-Mohyla Academy, Kiev Oblast, Ukraine

***Abstract*---**In this article, we propose and implement a novel architecture, the first of its kind, providing a high level of security for outsourcing data in a cloud computing environment consisting of multiple independent cloud providers. The framework consists of dual encryption combining Homomorphism encryption at the client end and Blowfish cryptographic technique at the server side for authorization. Also, we deploy the concept of data fragmentation at the client end before uploading the data to cloud storage in view to securely allocate information among multiple clouds. The diverse security issues associated with information integrity, security, confidentiality, and authentication must be addressed. Simulations and analyses were performed on an Oracle virtual machine Virtual-Box and a fog environment on Ubuntu 16.04 platform. Extensive safety measures and performance analysis considering the CPU resource utilization, integrity, cost, and delay demonstrate that our projected proposal is vastly proficient and satisfies the security requirements for secure data sharing and can withstand security attacks. Cloud computing is mentioned to evolve dynamically and cloud transformation is getting easier all the time. Different cloud aspects are emerging efficiently and have the potential to transform the traditional way of computing. With the advent of data sharing in cloud computing, the demand for outsourcing data has rapidly increased in the last decade. However, several security and privacy challenges exist impeding the acceptance of cloud computing. A highly secure system is required to guard an organizational entity, its resources, and assets.

***Keywords*---**Cloud computing, Blowfish crypto- graphic technique, Homomorphism encryption, Authentication, Outsourcing.

Tennessee research international of social sciences © 2024.
ISSN: 2766-7464 (Online)
Publisher: Smoky Mountain Publishing
Manuscript submitted: 09 April 2024, Manuscript revised: 18 May 2024, Accepted for publication: 27 June 2024

Introduction

The abundance of the digital world continues to augment the necessity of novel storage space as well as net utilities, besides with a growing requirement for additional expenditure for effective handling of storage capacities and network bandwidth for information transmitted. The employment of the distant storage method is achieving esteem, specifically the cloud storage based services, as they grant beneficial architecture. This style supports the communication, storage and intensive calculation of outsourced information on a pay per use business model. This extensive significance in cloud storage services primarily arises from agencies looking for further flexibility and outlay valuable systems. That is the profit of cloud espousal is very substantial in a later period of receptiveness, usefulness, and competence in "Information Technology" service delivery. Consequently, expending huge quantity of assets on buying high-priced application is no longer required. These reasonable profits present the chief crucial inspiration for cloud acceptance as they assist the enterprises plummeting the Capital Expenditure (CapEx), kept to procure permanent assets and the Operational Expenditure (OpEx) which is an ongoing expenditure for accepting a product business or a system.

The clause is structured as ensuing: Section 2 discusses the role of cloud computing and the need of multi-clouds. Section 3 illustrates the importance of security in clouds and principles. Section 4 provides the motivational scenario and the main contributions of the paper. Section 5 highlights the literature survey done. Further, Section 6 describes the techniques used to formulate confidential data by means of fragmentation, and hybrid encryption and discusses Blowfish and Homomorphic encryption in detail. Section 7 explains the proposed HBDaSeC system model and operations to be operated on files in multi-clouds. In section 7 a framework for secure data storage on the cloud is proposed. A detailed consequently, expending huge quantity of assets on buying high-priced application is no longer required. These reasonable profits present the chief crucial inspiration for cloud acceptance as they assist the enterprises plummeting the Capital Expenditure (CapEx), kept to procure permanent assets and the Operational Expenditure (OpEx) which is an ongoing expenditure for accepting a product business or a system.

The clause is structured as ensuing: Section 2 discusses the role of cloud computing and the need of multi-clouds. Section 3 illustrates the importance of security in clouds and principles. Section 4 provides the motivational scenario and the main contributions of the paper. Section 5 highlights the literature survey done. Further, Section 6 describes the techniques used to formulate confidential data by means of fragmentation, and hybrid encryption and discusses Blowfish and Homomorphic encryption in detail. Section 7 explains the proposed HBDaSeC system model and operations to be operated on files in multi-clouds. In section 7 a framework for secure data storage on the cloud is proposed. A detailed description of the framework along with all components and phases are described in the chapter. Section 8 provides notes on the implementation of the framework introduced in section 7 and it also describes the performance of the framework. Section 9 provides concluding remarks and as well as routes for possible enhancements.

Cloud Computing

Over the duration, computing models have transformed commencing scattered, similar, and a grid to cloud computing. Cloud computing can be named as an innovation used to convey benefits through the web as a medium. Cloud computing comes with numerous intrinsic abilities such as on- demand resource distribution, abridged management efforts, elastic pricing form, and simple applications and services stipulation. Fig.1 outlines the cloud computing model.

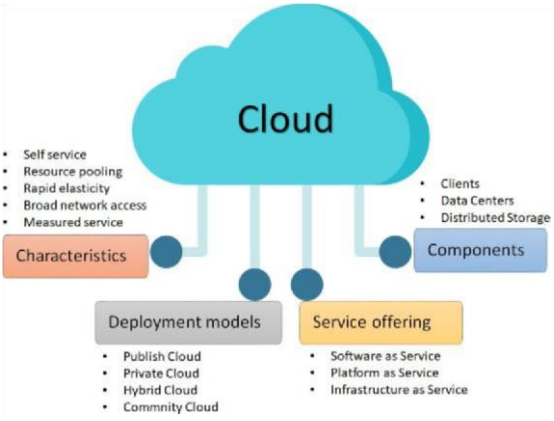

Figure 1. Cloud Computing Paradigm

Cloud computing comprises three key service mod-els: Infrastructure-as-a-Service (IaaS), Platformas-a-Service (PaaS), and Software-as-a-Service (SaaS) and their description are presented in Figure 2. below.

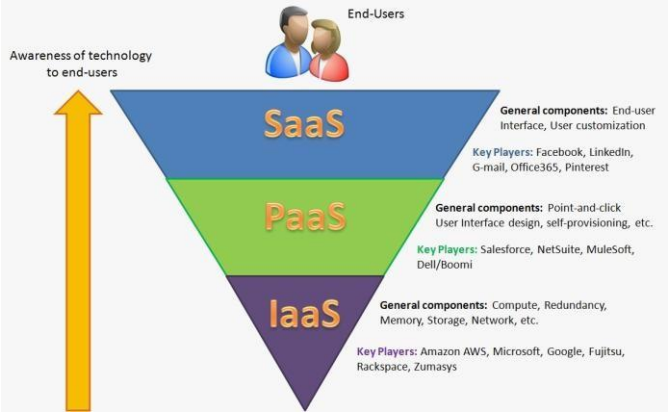

Figure. 2 The SPI Model

Cloud services can be provided as four basic cloud delivery models as shown in Figure 3. Five major cloud actors each concerned with performing diverse roles are cloud broker, the cloud provider and consumer, cloud auditor, and cloud carrier.

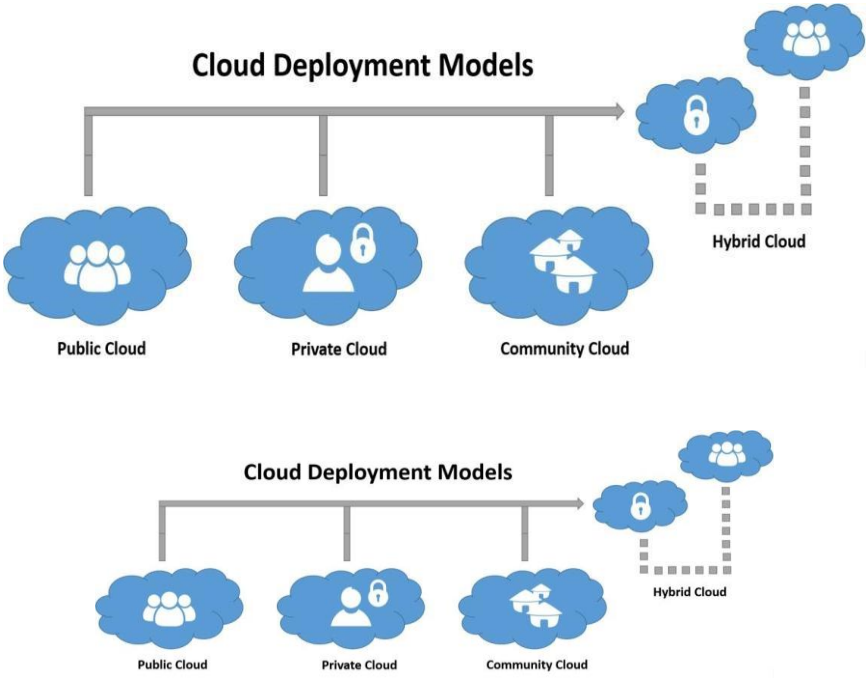

Fig. 3. Cloud Deployment Models

With the arrival of data, both individuals and enterprises are producing a huge amount of data every day, which profoundly influences our living style. On one hand, the explosively increasing data creates the limits for data storage and data transmission; on the other hand, data has become an important productivity resource. Therefore, it is essential to invent a proficient data sharing model to share huge amounts of data among different individuals or organizations. Obviously, cloud computing is certainly a perfect data sharing tool for its vast storage space and reliable distributed storage system. However, even if there are various advantages of cloud computing, security and privacy concerns are the primary obstacles to wide adoption.

Why Multiclouds are essential? The multi-cloud approach employs two or more clouds and consequently avoids depen- dence on one individual cloud. Vukolic stated that multi-clouds encompass improved trust, protection, and dispersed reliability amid several cloud providers. Abu Libdeh prefers multi-clouds so as to elude “vendor lock-in” by storing user’s information amid various clouds. Multicloud scheme has the capability to lessen the hazard of service accessibility collapse, failure and corruption of information, privacy hindrance in addition to the view of malicious insiders in the single cloud, increased virtual power by merging the infrastructure of several cloud providers by offering application programming interface abstractions which has made easy the management of multiple cloud providers at the same time, and increased flexibility by offering hardware, software and infrastructure redundancy and seer traffic from different customers through the fastest possible parts of the network. It has incorporated diverse aspects of security like confidentiality, integrity, availability, proficient retrieval and information sharing.

The main multi-clouds models are DepSky to construct clouds-of-clouds andare considered to be the finest model as it provides all the security issues like availability, integrity, and confidentiality and avoids vendor lock-in problem. HAIL is High Availability and Integrity Layer which provides a software layer by combining cryptographic protocols with erasure codes to provide integrity and confidentiality. RACS is a redundant array of independent disks (RAID) like practice solving vendor lock-in problems but it fails to provide con- fidentiality and security issues. InterCloud Storage (ICStore) implements all client-side functionalities as a library and has three layers which offer confidentiality, integrity, reliability, and consistency. MultiCloudDataBase (MCDB) is considered to be the advance side of DepSky and uses distributed method to grant privacy with database management systems.

Importance of Security in Cloud Computing

The control, suppleness, and easiness of employment of Cloud Computing arrive with a number of challenges/issues. In particular, security has been extensively reported to constitute the main factors which prevent migration to the cloud. Even if a corporation states to include peak class security and does not renovate its security policies from time to time, it will be vulnerable to security breaches in near Vista. In this view, via this manuscript, we intend a novel practice to alleviate the security challenges through Integrated Encryption approach. The distance amid the user and the physical site of his information construct a hurdle as this information can be leaked by a third party affecting the privacy of customers infor- mation. The employment of conventional encryption schemes to encrypt the remote data prior to transfer to the cloud service provider have been extensively used to viaduct this security breach. However, the customer should provide the secret key to the server to decrypt the information prior to carry out the requisite calculations. Homomorphic encryption permits performing computations on encrypted data without decryption.

Motivational Scenario and the Main Contributions of the Paper

Users deduce that cloud service providers certify that while information is in transit commencing clients premises to the cloud servers, its security constraints would not be distorted, and their information can be transmitted securely to corroborate an increased data security. However, the significant security challenges have augmented consequence and should be cautiously addressed. Thus, cloud clients deal with the challenges of selecting appropriate cloud service providers and assess security implementations depending on their security needs. Key contributions of the paper are as follows: The subsequent is an outline of our effort:

1. We intend a procedure for safe allocation of cloud data. This practice adeptly offers the reliability assurance to customers as a cloud service provider is considered reliable in storing all the records and these records cannot be exposed to malicious or illegal users.
2. We verified that security in terms of confidentiality and availability of the projected system against attacks.

3. We authenticate the results of the planned method via analysis and assessment. Our system takes less storage space and execution time to perform the queries and offers better security and is highly efficient.

Related Work

Security is a vital facet of all information processing con- duct and every organization has to extend mechanisms and tools to sustain and guarantee the security of their information resources. Bohli (2013) had mentioned that a lot of research activities are being carried out to address cloud security threats. The paper motivated the need for effective cloud secu- rity countermeasures by discussing the cloud security issues. The motivation of use of multi-clouds was described along with the proposed set of four distinct Multicloud architectures. Each of the introduced architecture provides its own security merits and flaws were started with respect to the security requirements by using diagrammatical presentation. Case stud- ies discussing real-life examples were also mentioned in each scenario. Security, feasibility, and regulation were considered for comparison. Tari (2015) explored cloud security in terms of issues, solutions, and shortcomings.

The author correlated data confidentiality and user authentication. Benzeki (2016) suggested the usage of homomorphic encryption for storage on the cloud. The author described security and privacy con- straints, issues, and approaches. Zafar et al. (2016) aimed to understand the security issues and highlighted the significance of data integrity schemes used for cloud storage. The paper had defined taxonomy to explain all aspects of data integrity considering its attributes like nature of data, deployment model used, and nature of metadata employed. The security attacks and mitigation techniques were discussed. Liu et al. (2018) presented a novel architecture of security which acts as an interface amid end users and private cloud ser- vice providers. The major contributions of the paper included high available cloud storage gateway (HASG) architecture. Data reliability and fault tolerance, file fragment algorithm utilizing information dispersal algorithm divided the file into redundant partitions and stored on different cloud storage. Raval (2018) presented a pioneering method for safe data storage on the cloud through the collective use of cryp- tography and Disintegration Protocol and validated Integrity and Confidentially, security constraints against internal and external attacks. Srisakthi et al. (2015) proposed for a multi- cloud system for encrypting, splitting and storage of data. In case of any failure in existing CSP or two CSP's, a model was proposed for efficient working. The system limitation is increased time but the security is assumed to increase. Balusamy et al. (2017) defined a new scheme called storagecorrectness and fine-grained access provision (SCFAP) which utilized hierarchical structure to allow users an exclusive access. The storage correctness verification of the outsourced data was done using a token granting mechanism. The future work mentioned was to deploy SCFAP scheme for outsourced data decryption techniques. Kolhar et al. (2017) emphasized an auditing process involving a TPA to achieve data integrity and privacy.

The research on cloud data auditing was mentioned to focus on the verification, privacy preservation and integrity of stored data using cryptographic methods.

Subramanian et al. (2017) presented the architecture overview with algorithms for file slicing and encryption and file decryption and Merging. The comparison table of various existing schemes and the proposed model were listed in terms of Turnaround time, encryption process time, eecryp- tion process time, security features (Privacy, Insider attack, secret keys, confidentiality and data integrity) and Reliability features (File formats supported, collusion attack, Key Escrow, Malicious files, File size). The future enhancements suggested implementing dynamic data slicing using 3DES. Weinman (2017) mentioned the use of highly dispersed compute and storage elements in the form of "FOG". Multicloud FOG is a hybrid architecture working together in an integrated fashion providing highly dispersed facilities. A real-life ex- ample is Walmart which uses OpenStack for its private cloud, Rackspace, Azure, and other public clouds. Yan et al. (2017) provided a new efficient remote data possession checking (RDPC) protocol based on Homomor- phic Hash function. The presented scheme was mentioned to be secure against several attacks. The performance anal- ysis showed the computation and communication cost to be reduced. Ali et al. (2017) proposed a model called DaSCE (Data security for cloud Environment) with a semi-trusted third party which provided key management, access control, and file assured deletion functionalities.

DaSCE is mentioned to utilize Shamir's (k, n) threshold scheme. Scyther tool was used to graphically analyze and verify security protocols. Aujla et al. (2018) discussed the problems of big data storage in the cloud like data security, data authentication, data integrity, data availability and data de-duplication. Architec- ture, SecSVA: A secure storage, verification, and auditing for big data in the cloud environment were discussed supporting the data authentication, verification, auditing, integrity and confidentiality for cloud storage. An attribute-based security framework with secure de-duplication for Big data storage in the cloud was discussed. The architecture comprised of various entities like client, data service provider, cloud serviceprovider, trusted party auditor (TPA) and Kerberos server. From the analysis, the proposed scheme was mentioned to withstand different attacks. Wei et al. (2018) suggested for the Multi- cloud environment. The encrypted data block and key blocks are together distributed to multiple cloud service providers. The verification of correctness of data exchange is done using a cryptographic protocol. The erasure correcting code was employed to support reliable data storage for tolerating multiple failures among CSPS. Fu et al. (2018) evaluated the performance of the proposed large universe cipher-text based attribute-based encryptionoutsourcing scheme in two hardware platforms like Intel and ARM and employed key encapsulation variant.

The security analysis and performance evaluation showed the planned scheme to be secure and efficient. Vyas et al. (2017) discussed generic cloud storage architecture and various security require- ments considering confidentiality, integrity, and availability. The presented system encrypted only some bits of each data block instead of encrypting the whole file, thereby eliminating computation overhead. The Integrity was checked by the Meta- data created and inserted at the end of the original file. Metadata was encrypted by applying the AES-256 encryption algorithm and the SHA-256 algorithm was used for generating a hash of the original file. The implementation of the proposed approach was done using

Amazon S3 Live[1] cloud storage and the mechanism was used to validate the integrity check of the uploaded file.

Encryption Techniques Employed

Encryption is the process of translating plaintext into cipher- text and decryption is the reverse of the encryption process. Key size plays a significant role in the encryption and decryp- tion process. Longer the key, more difficult is the process of decrypting the message. Whenever a message is sent from the sender to the des- tination, an intruder denoted by 'I' can interfere with the communication medium who can affect the system in the following ways:

1. A message can be 'blocked' which violates the availabil- ity and thus the message never reaches the destination.
2. Confidentiality can be breached if the message can be 'intercepted' by the intruder which makes it no longer secret.
3. Integrity can be violated if' content' of the message can be changed or a fake message is sent.

Homomorphic encryption is the apt elucidation to resolve cloud computing security issues because its schemes facilitate to execute computations on encrypted information devoid of sharing the secret key essential to decrypt the data. A Homomorphic encryption is: from Enc (P) and Enc (−Q) it is possible to × compute Enc (Func (P, Q)), where 'Func' can be one of the operations: +, exclusive of using the private key. It was developed by Ronald Rivest, Leonard Adle- man, and Michael Detouzosin 1978. Homomorphic encryption (HE) is formed by four functions (MahaTeeba et al., 2012), as shown in Figure 4.

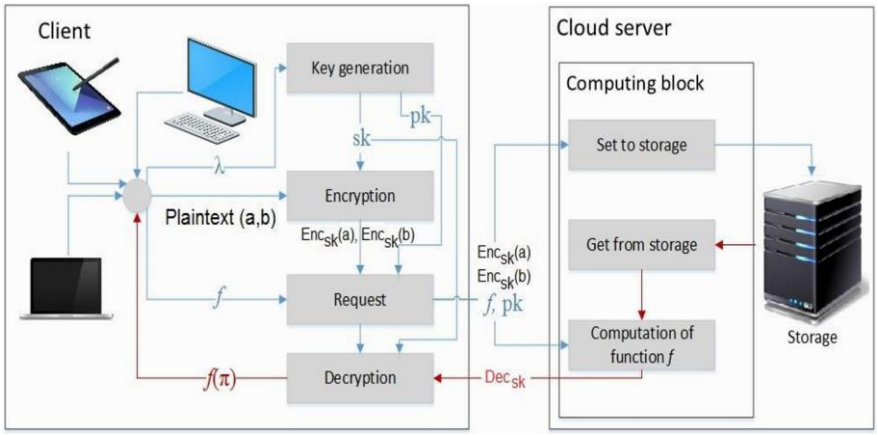

Figure 4. Homomorphic Encryption Functions

Types of Homomorphic Encryption

Homomorphic encryption is of three types as shown in Table I (MahaTeeba et al., 2012). A somewhat Homomorphic performs limited addition and multiplication on encrypted information.

Classification of Homomorphic Encryption

Parameter	Partial HE	Fully HE
Type of operation supported	It allows either addition or multiplication scheme	It allows both addition and multiplication operations
Computation	It allows a limited number of computations	It allows an unlimited number of computations
Computational efforts	It requires less effort	Requires more efforts
Performance	It is faster and more compact	It has slower performance
Versatility	It is low	It has high
Speed	It is fast in speed	It is slow in speed
Ciphertext size	It is small	It is large
Example	Unpadded RSA, ElGamal	Gentry Scheme

Homomorphic Encryption applications is considered to be a consolidated element for information security in cloud computing. Homomorphic Properties of Paillier is a Paillier cryptosystem supports the property of additive homomorphism. In this cryptosystem, the product of two cipher-texts will decrypt to the sum of their corresponding plaintexts. Considering message to be encrypted as m_1 and m_2, Enc () and Dec () are the encryption and decryption functions respectively and n is from the PublicKey= (n, q), and then the additive homomorphism property can be expressed. Graphical representation of the Blowfish algorithm is shown in Figure 5(a) taking into account the fiestal structure. The F function is shown in Figure 5(b).

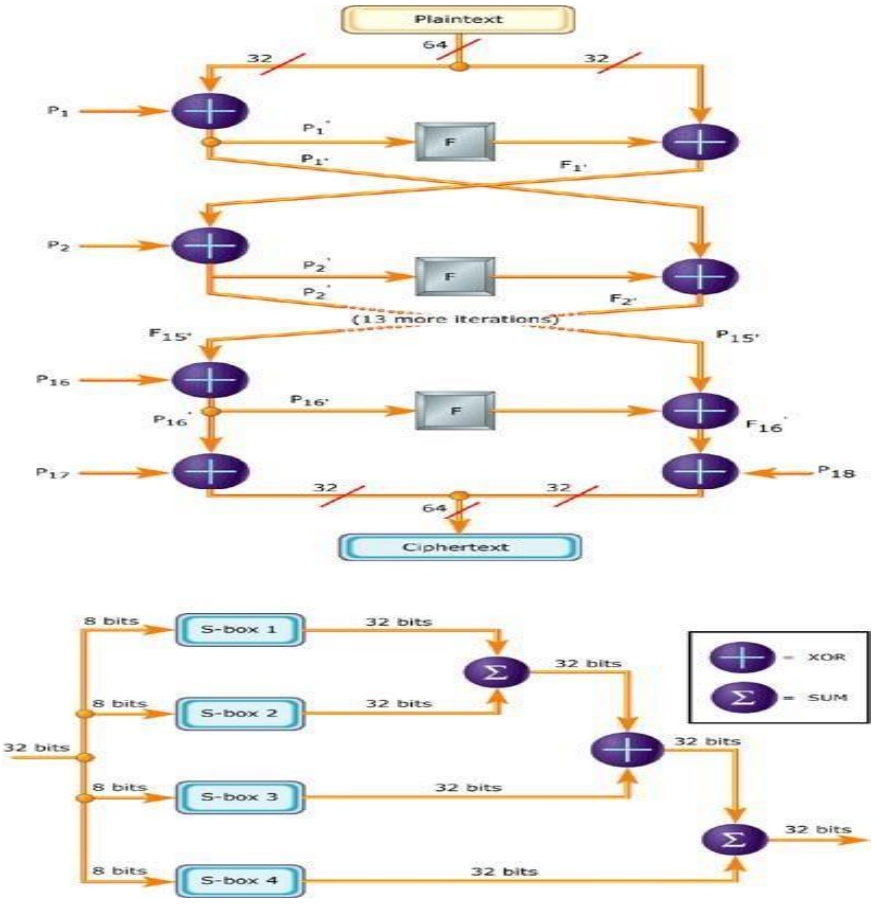

Figure 5.(a) blowfish algorithm (b) function module (f) (Manju, 2016)

The function divides 32-bit input into four bytes and uses them as indices into an S-array. The lookup results are XORed together to produce output. P taken is an array of eighteen 32- bit integers. S is a twodimensional array of 32 bit and stored as 4 × 256.

Fragmentation

The data fragmentation method gives more security to user's data on the cloud. In this, user's data is first divided into multiple parts based on size. It's illustrated in Figure 6.

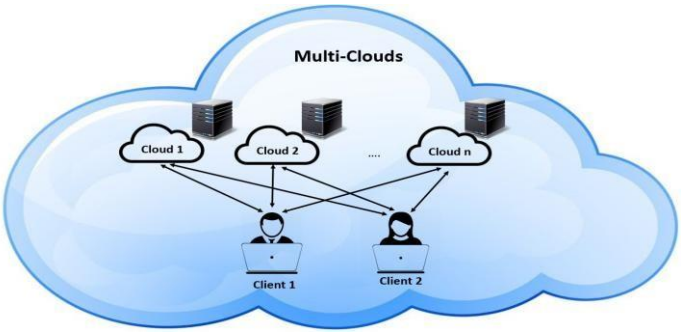

Figure 6. Data partitioning architecture

Proposed HBDaSeC System Model

Cloud storage as a service is an emergent drift with attrac- tive characteristics which are lacking in onpremise storage. Nonetheless, each organization is not competent of control- ling huge secondary storage or constructs their confidential information centers due to the incurred expenditure of con- structing and maintaining such infrastructure. Cloud storage elastic nature can be a vast provision to such organizations. Nevertheless, the failure of managing outsourced data is an intrinsic crisis. Even though the CSP is constrained by a Service Level Agreement to guarantee data security, clients cannot exclusively depend on these agreements. Moreover, dependence on a contractual commitment may fail to identify the malevolent activities of the service provider. So, in addi- tion to the expediency supported by the cloud system, data security issues are also mandatory to be looked upon with a cloud storage service system. Our proposed cloud information storage scheme is illustrated in Figure 7. The user can perform various operations like upload, down- load, delete and view the files.

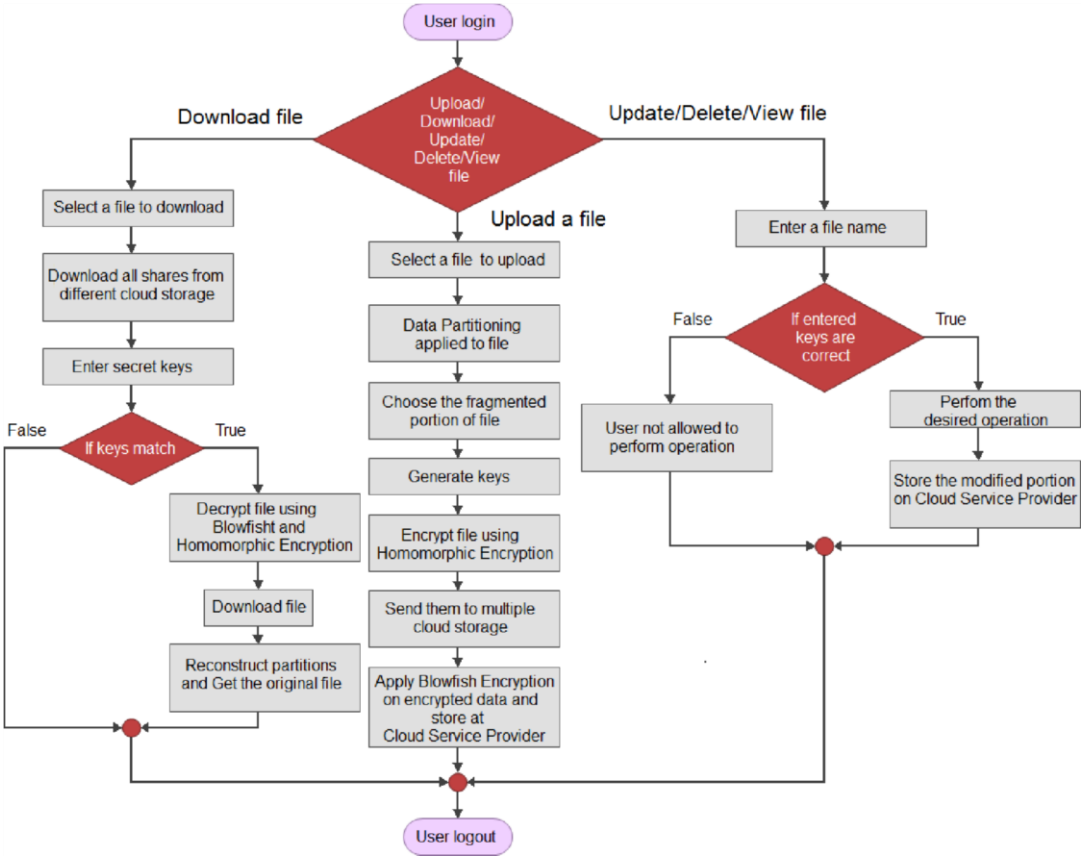

Figure 7. Proposed System Model

HBDaSeC Components

Each time a new user wants to store data in the cloud, the authorized administrator performs the registration of the client. The blend of the encryption techniques helps to diminish the threat of information seepage in multi-clouds even further, in the visage of inquiring or hacked CSPs. Furthermore, the availability of information located in the cloud is increased. The recovery procedure is analogous to the storage course involving authentication of Cloud Service Providers and re- construction of encrypted files. HBDaSeC involves:

1) Secure Storage: The subsequent stride is taken to amass the data given by a data storage provider securely using encryption and trusted authority:
   - Define access rights for user's w.r.t. the files based on role-based access control.
   - Fragment the files into random numbers based on their type.
   - Data files are encrypted using the Paillier algorithm at the client end and using the Blowfish algorithm at the server end and secret keys generated.
   - Signatures for encrypted files are generated by SHA-1 etc.
   - An encrypted chunk and its allied signature are sent to the independent CSPs.

2) Secure Verification: In the proposed HBDaSeC scheme, if a user desires to access the chunk stored by data storage provider, subsequent are the steps for uniqueness and access authentication:
   - The request is sent by a client to the administrator for the desired segment.
   - The administrator verifies the access privileges of the clients by role-based access control policy.
   - The client is denied access on non-confirmation of access rights.
3) Secure Auditing: In the planned design given in Fig.4, after step 1 and 2, the client verifies data integrity by the subsequent steps: • The client seeks the encrypted information from the cloud service provider.
   - The cloud service provider sends the encrypted data to the client. The client generates the hash checksum using GtkHASh[2] GUI.
   - The generated checksums are checked against the checksum stored in its database.
   - The data integrity is confirmed if a match occurs.
   - After confirmation of data integrity, the download operation is said to be complete when the split shares of data are regenerated and merged to get the original file.

System Architecture Overview

In the next section, we will provide an outline of a design in Figure 4 comprising the storage course from a solitary Healthcare unit (HU) including the data flow and security measures. The system will consist of major components: Cloud service providers, Data users, and Trusted Third Party Auditor. A novel style of security, as a proficient distributable cloud storage gateway acting as an interface between end users and private Cloud service providers, is provided. The progress of a security system HBDaSeC: "A Novel Approach integrating Homomorphic and Blowfish encryption techniques for Secure Data.

Storage in Cloud" combining Ho- momorphic and asymmetric encryption is illustrated in Fig.8 below. At the client end, the client sends the fragmented and encrypted data with personalized keys on the cloud storage. The work of the server is to re-encrypt the encrypted data. The provision for storing the encrypted file with and without compression is provided at the server side. The client requests for data to the cloud storage server. The server sends the double encrypted data to the client. The client decrypts the obtained results and reconstructs all the partitions to attain the original file.

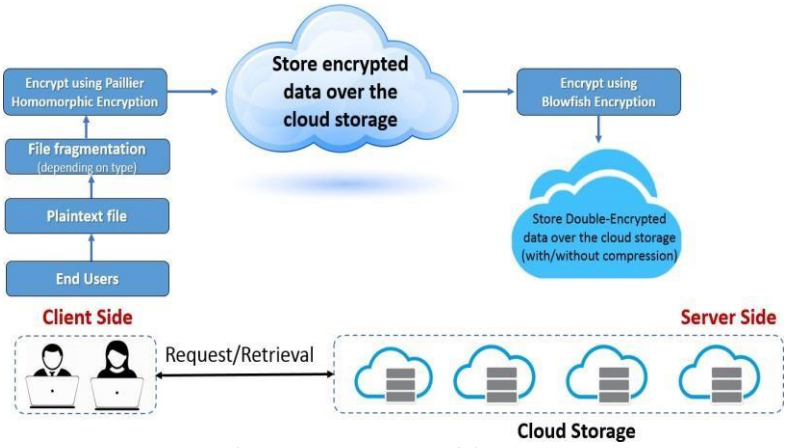

Fig. 8. System Architecture

Our approach will convey the latest facet to cloud storage. It assures confidentiality, integrity to the data as in no stage information is exposed in plaintext. The data fragmentation method gives more security to user's data on the cloud. In this, user's data is first divided into multiple redundant partitions based on size. After partitioning, the user's data are encrypted and scattered each share over the Internet to different Cloud service providers. The use of multiple cloud servers provides more security to user's data. If an attacker gets any part of the file, it is impossible to get complete data because the data will be divided and stored on different servers. The following architectural diagram shows the concept of data partitioning and storage on different cloud servers. The deployment of the cloud has twofold benefits for such an approach:

1. The user can retrieve his file in case of temporarily/permanent unavailability of the provider.
2. Providers can't access the file stored within them.

Only the authorized users are supposed to have full control of the overall security of the data. The clients have the right to access their own specific data and can't overlook other user's data. The cloud service providers are not provided any knowledge about the stored information as the data is stored in encrypted form. Role of Trusted Third Party Authority at the server side Third party authority has been assigned the authority for changing the attributes is used to set/unset certain attributes to a file to secure accidental deletion or modification of important files and folders. The file can be made immutable i.e. no renaming, no execution, no symbolic link creation, no writable is allowed. We can secure the entire directory and its file content using different switches like +r with +i flag along with the full path of the folder. To synchronously update changes on the disk on any file modification, the 's' attribute set can be used.

HBDaSeC Phases

The scheme can be achieved by creating a safe and completely automated information storage and transfer protocol amid CSPs and users having access to numerous storage volumes on the cloud to accumulate his information. The protocol can be implemented in two phases:

1. Upload phase
2. Retrieve phase

The send phase occurs when the file is being saved or restructured in the public cloud storage and retrieve phase occurs when the file is accessed or downloaded from the cloud infrastructure. The file can be stored among available virtual volumes V_1, V_2, ..., V_n with each having certain storage space.

Upload Phase

A file to be uploaded is split into numerous smaller chunks to be stored in the existing volumes such that reconstruction of the initial file becomes difficult.

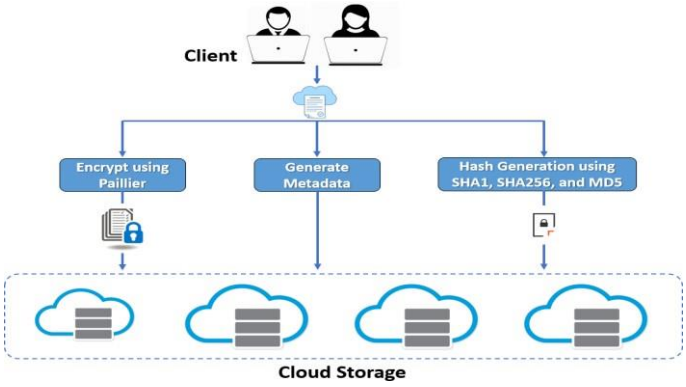

Figure 9. HBDaSeC Upload Phase

Retrieving phase

The chunks are randomly selected in the retrieved phase. When all the chunks are obtained, an integrity check is carried out and using the information in the Index field, the chunks are precisely arranged to generate the original file.

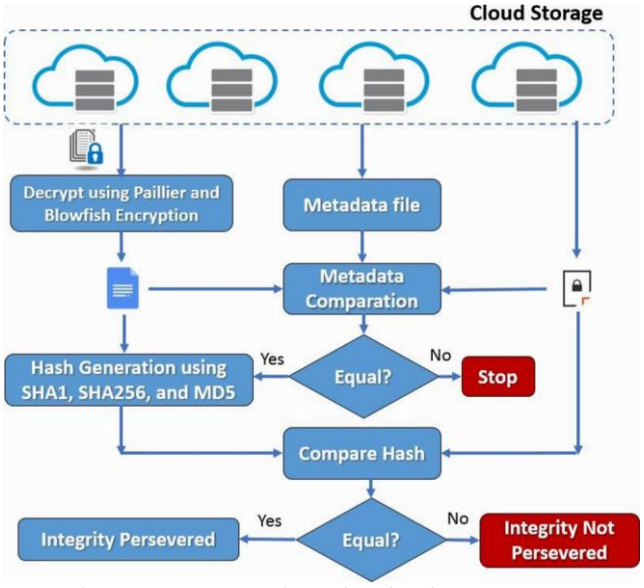

Figure 10. Integrity Check Phenomenon

We have chosen three cloud security aspects abbreviated as CIA i.e. Confidentiality, Integrity and Availability out of six security principles. Their significance is shown in the Fig.11 below:

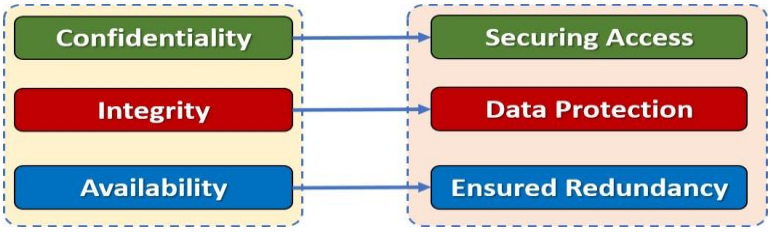

Figure 11. Cloud Security Aspects

Confidentiality: Confidentiality refers to the prevention of unauthorized access of the data and making sure that only the user who has the permission can access the data. This way the CSP can guarantee the user that his data doesn't get into wrong hands and also increases the users trust in cloud computing and helps it grow faster. Data confidentiality can be ensured through better encryption technique.

Integrity: When the integrity of outsourced data is to be checked, it is not practicable to download all records from the distant server and confirm as it incurs huge communiqué and computational cost. To evade this great cost, generally, the integrity schemes execute "blockless verification" which allows downloading only metadata and not the real information from the cloud; which is generated by the CSP and verified at the client end. Efficiency is a major issue in data integrity schemes is calculated as computation, communication and storage expenses incurred.

Availability: Availability is ensured by storing the files both on the clients and server.

Conclusion

Cloud computing is a concept shifting in the approach how computing resources are deployed and purchased. Even though the cloud has a capable, elastic, and consistent design, several security concerns restrain customers to completely accept this novel technology and move from traditional computing to cloud computing. In the article, we aspire to present a form of a novel architectural model for offering protection to numerous cloud service providers with the intention to devise and extend security means for cloud computing. In this work, we presented a two-tier architecture for security in multi-clouds; one at the client side, and other at the server side. The article presented a security domination outline for multi-clouds and supports security needs like Confidentiality, Integrity, Availability, Authorization, and Non-repudiation for cloud storage. Through this document we have anticipated, HBDaSeC, a securecomputation protocol to ease the challenges of enforcing the protection of data for information security in the cloud. To the paramount of our acquaintance, it is the foremost effort that together utilizes two encryption techniques for data storage security and computation in the cloud. Our execution and assessment by numerous experiments suggest the convenient viability and ease of use of the system. By the extensive security analysis and performance simulation in our developed SecHDFS prototype, it is apparent that our procedure is effectual and competent for achieving a secure cloud computing. In addition, we intend to execute them in the real cloud platform such as NetCloud. Also, storage capacity improvements in case of pdf and video files are considered as future work.

References

Beloglazov, A., & Buyya, R. (2012). Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers. Concurrency and Computation: Practice and Experience, 24(13), 1397-1420.

Benevenuto, F., Fernandes, C., Santos, M., Almeida, V., Almeida, J., Janakiraman, G. J., & Santos, J. R. (2006, December). Performance models for virtualized applications. In International Symposium on Parallel and Distributed Processing and Applications (pp. 427-439). Springer, Berlin, Heidelberg.

Coarfa, C., Druschel, P., & Wallach, D. S. (2006). Performance analysis of TLS Web servers. ACM Transactions on Computer Systems (TOCS), 24(1), 39-69.

Dejun, J., Pierre, G., & Chi, C. H. (2009, November). EC2 performance analysis for resource provisioning of service-oriented applications. In Service-Oriented Computing. ICSOC/ServiceWave 2009 Workshops (pp. 197-207). Springer, Berlin, Heidelberg.

Esteve, M. A., Katoen, J. P., Nguyen, V. Y., Postma, B., & Yushtein, Y. (2012, June). Formal correctness, safety, dependability, and performance analysis of a satellite. In 2012 34th International Conference on Software Engineering (ICSE) (pp. 1022-1031). IEEE.

Gkantsidis, C., Miller, J., & Rodriguez, P. (2006, October). Comprehensive view of a live network coding P2P system. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement (pp. 177-188).

Henia, R., Hamann, A., Jersak, M., Racu, R., Richter, K., & Ernst, R. (2005). System level performance analysis–the SymTA/S approach. IEE Proceedings-Computers and Digital Techniques, 152(2), 148-166.

Iosup, A., Ostermann, S., Yigitbasi, M. N., Prodan, R., Fahringer, T., & Epema, D. (2011). Performance analysis of cloud computing services for many-tasks scientific computing. IEEE Transactions on Parallel and Distributed systems, 22(6), 931-945.

Kalyvianaki, E., Charalambous, T., & Hand, S. (2009, June). Self-adaptive and self-configured CPU resource provisioning for virtualized servers using Kalman filters. In Proceedings of the 6th international conference on Autonomic computing (pp. 117-126).

Koh, Y., Knauerhase, R., Brett, P., Bowman, M., Wen, Z., & Pu, C. (2007, April). An analysis of performance interference effects in virtual environments. In 2007 IEEE International Symposium on Performance Analysis of Systems & Software (pp. 200-209). IEEE.

Li, X., Qian, Z., Lu, S., & Wu, J. (2013). Energy efficient virtual machine placement algorithm with balanced and improved resource utilization in a data center. Mathematical and Computer Modelling, 58(5-6), 1222-1235.

Maier, G., Sommer, R., Dreger, H., Feldmann, A., Paxson, V., & Schneider, F. (2008, August). Enriching network security analysis with time travel. In Proceedings of the ACM SIGCOMM 2008 conference on Data communication (pp. 183-194).

Mei, Y., Liu, L., Pu, X., Sivathanu, S., & Dong, X. (2011). Performance analysis of network I/O workloads in virtualized data centers. IEEE Transactions on Services Computing, 6(1), 48-63.

Pu, X., Liu, L., Mei, Y., Sivathanu, S., Koh, Y., & Pu, C. (2010, July). Understanding performance interference of i/o workload in virtualized cloud environments. In 2010 IEEE 3rd International Conference on Cloud Computing (pp. 51-58). IEEE.

Pu, X., Liu, L., Mei, Y., Sivathanu, S., Koh, Y., Pu, C., & Cao, Y. (2012). Who is your neighbor: Net i/o performance interference in virtualized clouds. IEEE Transactions on Services Computing, 6(3), 314-329.

Ramesh, A., & Suruliandi, A. (2013, March). Performance analysis of encryption algorithms for Information Security. In 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT) (pp. 840-844). IEEE.

Schad, J., Dittrich, J., & Quiané-Ruiz, J. A. (2010). Runtime measurements in the cloud: observing, analyzing, and reducing variance. Proceedings of the VLDB Endowment, 3(1-2), 460-471.

Syafrudin, M., Alfian, G., Fitriyani, N. L., & Rhee, J. (2018). Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing. Sensors, 18(9), 2946.

Villari, M., Fazio, M., Dustdar, S., Rana, O., & Ranjan, R. (2016). Osmotic computing: A new paradigm for edge/cloud integration. IEEE Cloud Computing, 3(6), 76-83.

Wandeler, E. (2006). Modular performance analysis and interface-based design for embedded real-time systems (pp. 1-207). ETH Zurich.

Wandeler, E., Thiele, L., Verhoef, M., & Lieverse, P. (2006). System architecture evaluation using modular performance analysis: a case study. International Journal on Software Tools for Technology Transfer, 8(6), 649-667.

Xavier, M. G., Neves, M. V., & De Rose, C. A. F. (2014, February). A performance comparison of container-based virtualization systems for mapreduce clusters. In 2014 22nd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (pp. 299-306). IEEE.

Yasin, A. (2014, March). A top-down method for performance analysis and counters architecture. In 2014 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS) (pp. 35-44). IEEE.

Zeng, L., Veeravalli, B., & Li, X. (2015). SABA: A security-aware and budget-aware workflow scheduling strategy in clouds. Journal of parallel and Distributed computing, 75, 141-151.

Zhou, Z., Abawajy, J., Chowdhury, M., Hu, Z., Li, K., Cheng, H., ... & Li, F. (2018). Minimizing SLA violation and power consumption in Cloud data centers using adaptive energy-aware algorithms. Future Generation Computer Systems, 86, 836-850.

Zonouz, S., Houmansadr, A., Berthier, R., Borisov, N., & Sanders, W. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. Computers & Security, 37, 215227.