International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Security and Storage Management of Data on Cloud using Fully Homomorphic Encryption and Adaptive Compression Approach

Bikramjeet Singh Bumrah[1], Gurbind Kaur[2]

[1]M.Tech, Department of Computer Science, Punjabi University, Patiala, India

[2]Assistant Professor, Department of Computer Science, Guru Nanak College, Batala, India

Abstract- ***Cloud computing depends on sharing of assets to accomplish intelligibility and economies of scale, like a utility (like the power matrix) over a network. At the establishment of cloud computing is the more extensive idea of met foundation and imparted administrations. Data is uploaded on the cloud. Data is encrypted using some type of encryption. Encryption data is encrypted using fully Homomorphic Encryption. With the help of FHE, the owner does not need to decrypt the data or provide the private key to the trusted third party for computation. The third party can themselves perform the computation, the result of which will be sent to the owner of the data. The owner will then decrypt the result using its private key and will send back the result in decrypted form. This can be achieved by using OTP (One Time Password). OTP is generated at each login and it is sent to the party's registered mobile or email address. Using the OTP, one can successfully login. Another problem that is created is the size of data using FHE increases tremendously which needs to be solved using some kind of lossless compression technique.***

Keywords: Cloud Computing, Fully Homomorphic, OTP

1. Introduction

Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The cloud computing landscape continues to realize explosive growth. The worldwide public cloud services market was projected to grow nearly 20 percent in 2012, to a total of $109 billion, with 45.6 percent growth for Infrastructure as a Service (IaaS), which is the fastest growing market segment. Yet for security professionals, the cloud presents a huge dilemma: How do you embrace the benefits of the cloud while maintaining security controls over your organizations' assets? It becomes a question of balance to determine whether the increased risks are truly worth the agility and economic benefits. Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers. Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity.

1.1 Cloud Computing Security Challenges

Data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value, reports the 2012 Computerworld "Cloud Computing" study, which measured cloud computing trends among technology decision makers. When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility into sensitive data.Derek Tumulak, vice president of product management at Vormetric, explains, "Everyone wants to use the cloud due to cost savings and new agile business models. But when it comes to cloud security, it's important to understand the different threat landscape that comes into play."

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concern
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data

The fundamental key to data security is to protect what matters. Solutions that enable companies to confidently transition to the cloud while still leveraging many of their traditional infrastructure and investments offer significant advantages. Vormetric Data Security solves the enterprise cloud security conundrum by protecting data inside of the operating environment while establishing security policies and maintaining control through a centralized management interface. One key differentiator is that Vormetric works with cloud providers and enterprises to protect data regardless of whether it is located in physical, virtual, or cloud environments. This architecture enables enterprises to

control access to the data itself, even as the virtual machine migrates to the virtual and cloud world. Organizations can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments.By providing a solution that protects both data and encryption keys, Vormetric Data Security provides the necessary safeguards to keep companies from facing breach notifications, and protects their most valuable business assets—their customers, brand, and the bottom line.

2. Related Work

Ahmed Dheyaa Basha et al (2013) Author propose mobile application and computing is picking up a high momentum and assuming an important part in upgrading the web figuring foundation. What's more, the cell phones and their applications have high procedure in the service ever had, and grew quickly. Mobile cloud computing is required to produce altogether more inventive with multi applications. Mobile computing includes versatile correspondence, versatile equipment and portable programming, and presently there are numerous portable cloud applications, for example, web perusing, email access, feature playback, Cisco's web EX on the I Pad, record altering, picture altering, Google's Map, Gmail for I Phone, and so forth.

Alabbadi, M.M et al (2011) Author present Cloud figuring, regardless of its buildup, is as a rule broadly sent, with its dynamic versatility and use of virtualized assets, in numerous associations for a few applications. It is imagined that, soon, distributed computing will have a critical effect on the instructive and learning environment, empowering their own particular clients (i.e., learners, educators, and heads) to perform their undertakings viably with less cost by using the accessible cloud-based applications offered by the cloud administration suppliers. This paper talks about the utilization of distributed computing in the instructive and learning coliseum, to be called "Training and Learning as a Service" (E LaaS), underlining its conceivable advantages and offerings. It is key for an instructive and learning association, with its financial plan confinements and maintainability difficulties, to utilize the cloud development ideally equipped for a specific IT movement.

Cong Wang et al (2009) Author proposes concentrated on cloud information storage security, which has dependably been a vital part of nature of administration. To guarantee the rightness of clients' information in the cloud, they propose a powerful and adaptable conveyed plan with two striking highlights, contradicting to its ancestors. By using the homomorphism token with appropriated confirmation of deletion coded information, our plan accomplishes the joining of capacity accuracy protection and information blunder confinement, i.e., the recognizable proof of making trouble server(s). Not at all like most former works, the new plan further backings secure and proficient element operations on information squares, including: information overhaul, erase and attach.

FarzadSabahi. et al (2002) Author Examined Cloud registering worries about basic issues, (for example, security) that exist with the across the board execution of distributed computing. These sorts of concerns start from the way that information is put away remotely from the client's area; truth be told, it can be put away at any area. Security, specifically, is a standout amongst the most contended about issues in the distributed computing field; a few endeavors take a gander at distributed computing carefully because of anticipated security dangers. The dangers of bargained security and protection may be lower in general, on the other hand, with distributed computing than they would be if the information were to be put away on individual machines rather than in an alleged "cloud".

Gaurav Raj1 et al (2012) Author propose recommended that the fundamental goal of our study is to propose a new approach for burden adjusting which can adjust the approaching solicitations from worldwide clients which live in diverse geological areas to recover the data from an appropriated information sources utilizing powerful planning and virtualization strategies. We are using the mix of Batch Mode Heuristic Priority and Round Robin Scheduling for decreasing the heap on server. This paper give great results as we analyze Batch mode and Online Mode need, and close with recommendation to utilize Batch Mode set up of online mode for better load adjusting.

3. Problem Formulation

There are different types of encryption techniques but by implementing them the user cannot use that data unless it is decrypted. For example suppose mathematical data is uploaded on the cloud. Data is encrypted using some type of encryption. Now if the owner wants some other trusted party to use that data for some computation then the owner will have to provide full access of the data to the third party. Owner of the data will have to share the private key with them. Or owner of the data will have to get their query and process entire query after decrypting the data. Here Fully Homomorphic Encryption comes into picture. In this approach data is encrypted using Fully Homomorphic Encryption. With the help of FHE, the owner does not need to decrypt the data or provide the private key to the trusted third party for computation. The third party can themselves perform the computation, the result of which will be sent to the owner of the data. The owner will then decrypt the result using its private key and will send back the result in decrypted form. As the data on the cloud is accessible publicly some kind of security mechanism needs to be there so that only trusted people can be given access to the cloud. This can be achieved by using OTP (One Time Password). OTP is generated at each login and it is sent to the party's registered mobile or email address. Using the OTP, one can successfully login. Another problem that is created is the size of data using FHE increases tremendously which needs to be solved using some kind of lossless compression technique.

4. Proposed Work

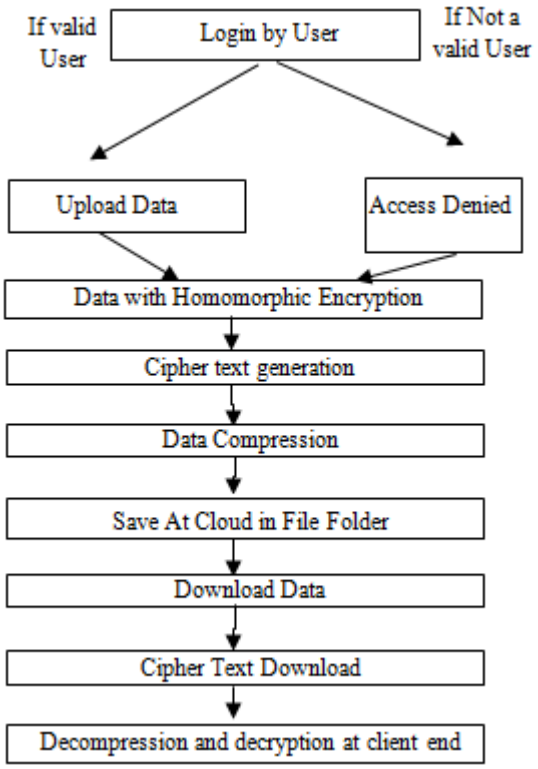

Figure 1: Flow of Work

Step 1: In the proposed work, the first step that is implemented by the user is that the user has to register himself /herself in the system. Once the user registers then he/she can login anytime. If the user is authenticated then the system will allow to login. And in case the user enters the wrong password then an error message will be displayed. The authentication is done for the security purpose. This is counted to be the main advantage of the system. There are two options in the main page one is register and other is login.

Step 2: Once the user registers then after filling the appropriate user name the pin code is automatically generated and the pin code generated will be sent to the particular email id of that individual. The authorization of the users has been evaluated by providing different user name and email id. The user request transmit the cloud the cloud sends a secret key to the user and after this if the authorized user provide that key then the user can access the account.

Step 3: After login id page in which user will fill the pin code. After which One Time Password is generated and is mailed to the email id. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. One-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device.

Step 4: In the next step stores data on the cloud in secure manner by using a technique called homorphic encryption. The homomorphic encryption use different arithmetical and logarithmic formulas for conversion of data from secret information to cipher text. These operations provide the security to data because these are without key operations that have to be transmitted to the user. Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

Step 5: After the process of encryption the major issue occurs in the cloud is storage due to encryption storage of the data has been increased. That occupies much space on cloud. To reduce the storage on the cloud loss less compression has been implement that reduces the file size. The file size has been get reduced and stored on the cloud.

Step 6: After this process when ever user want to access that data then the de-compression have to be done to decrypt the data. After decryption the logical and arithmetical formulas have to be implemented on the user side.
These formulas have been implemented on user side. After this process the user can get the plain text and use this for different operations.

5. Results and Discussions

Represents the server window page in which first step is to choose any text file and upload it as shown in Fig. 2. After that the user can encrypt that text file into Cypher text whose size is increased which is shown in Fig 3, to decrease the size of that text file user can press the compress button after which the size of that file will be decreased as shown in Fig. 4. Before decrypting the file user need to decompress the file as shown in Fig. 5. After that user can decrypt that file by pressing the decrypt button as shown in Fig. 6.

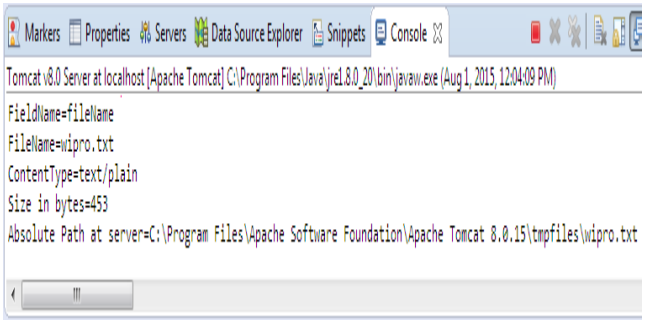

Figure 2 Uploading file for data compression

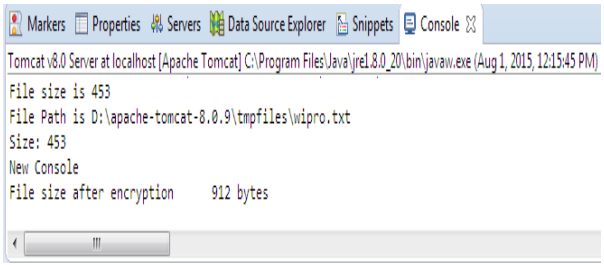

Figure 3 File size after encryption

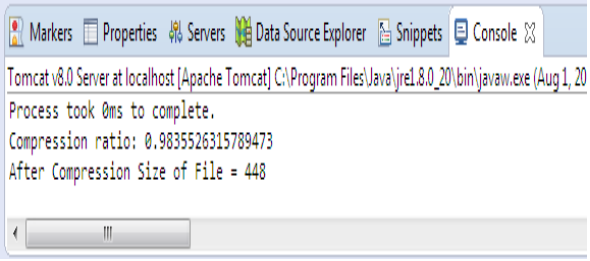

Figure 4 File after data compression

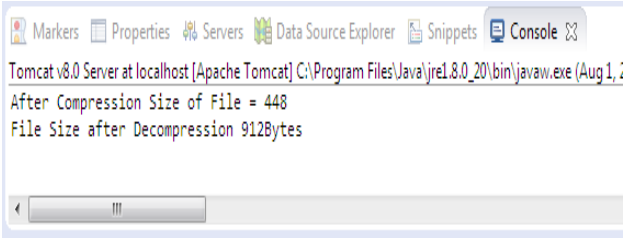

Figure 5 File after data decompression

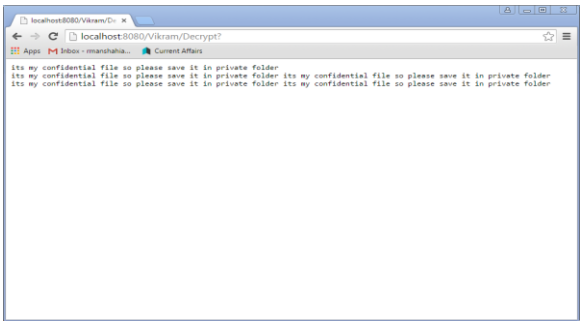

Figure 6: File data after decryption

Table 1: Computation time for encryption of data of different sizes and Compressed File Size

Sr. No	Files (in bytes)	Encrypted Files (in bytes)	Time (in ms)	Compressed File size
1	2481	4976	95	1820
2	3231	6464	110	2320
3	4186	8384	114	3020
4	5146	10304	120	5146
5	20588	41184	122	14044
6	412 KB	828 KB	157	257 KB
7	989 KB	1980 KB	273	657 KB
8	1.13 MB	2.27 MB	300	0.71 MB
9	1.56 MB	3.12 MB	416	1.06 MB

Table 2: Computation time for encryption of data of different sizes

Sr. No.	Files (in bytes)	Proposed work	Semi Homomorphism	Percentage Improvement
		Time (in ms)		
1	2.4 KB	95	111	16.8 %
2	3.2 KB	110	125	13.63 %
3	4 KB	114	136	19.29 %
4	5 KB	120	148	23.33 %
5	2 MB	122	156	27.86 %

Table 3: Compression file size for files of encrypted data of different sizes

Sr. No.	Files (in bytes)	Proposed work	Semi Homomorphism	Percentage Improvement
		Compressed File Size (in bytes)		
1	2481	1820	2248	23.51 %
2	3231	2320	2888	24.48 %
3	4186	3020	3728	23.44 %
4	5146	4168	4864	16.69 %
5	20588	14044	17048	21.39 %

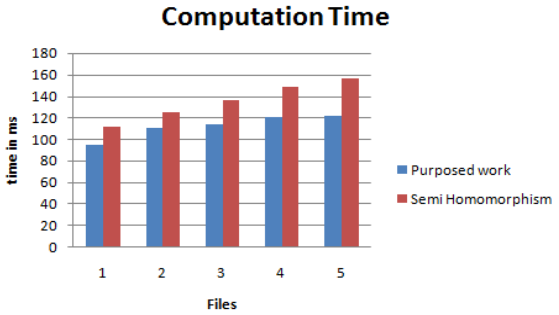

Figure 7: Graphical representation of computation time in encryption

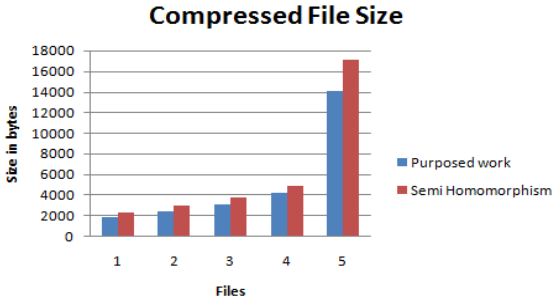

Figure 8: Graphical representation of compressed file size after encryption

6. Conclusion

Cloud computing is the framework that provides various applications for the users for data storage. In the cloud computing environment different frameworks have been embedded to perform speedy transactions. Cloud computing environment provides different storage management for information storage. In the cloud the charges have been paid on the basis of storage allocated to a single user. In the proposed work the data has been stored on the cloud by different users for secure purpose. The authorization of the users has been evaluated by providing different user name and email id. The user request transmit the cloud the cloud sends a secret key to the user and after this if the authorized user provide that key then the user can access the account. After this user have to store data on the cloud in secure manner by using homorphic encryption. The homomorphic encryption use different arithmetical and logarithmic formulas for conversion of data from secret information to cipher text. These operations provide the security to data because these are without key operations that have to be transmitted to the user. After the process of encryption the major issue occurs in the cloud is storage due to encryption storage of the data has been increased. That occupies much space on cloud. To reduce the storage on the cloud loss less

compression has been implement that reduces the file size. The file size has been get reduced and stored on the cloud.After this process when ever user want to access that data then the de-compression have to be done to decrypt the data. After decryption the logical and arithmetical formulas have to be implemented on the user side. These formulas have been implemented on user side. After this process the user can get the plain text and use this for different operations. The proposed work provides better storage management of the data on the cloud environment. It reduces the storage capacity of the data and can be easily stored on data. In the proposed work the encryption size and compution time has been used for performance evaluation. This work provide 12 % more efficiecy than previous work using semi homomorphism approach.

References

[1] Ahmed DheyaaBasha, "Mobile Applications as Cloud Computing: Implementation and Challenge", IEEE Conf. on Cloud Computing and Intelligence Systems (CCIS) , 2013, pp 467 – 471.
[2] Alabbadi, M.M "Cloud computing for education and learning: Education and learning as a service (ELaaS)", IEEE Conf. on Interactive Collaborative Learning (ICL),2011, pp 589 – 594.
[3] Cong Wang, "Ensuring Data Storage Security in Cloud Computing" IEEE Conf. on Parallel Distributed and Grid Computing (PDGC) , 2009, pp 217 - 222.
[4] Farzad Sabahi, "Cloud Computing Security Threats and Responses" IEEE Trans. on Cloud Computing, 2002, pp 245 – 249.
[5] Gaurav Raj, "Using Batch Mode Heuristic Priority in Round Robin (PBRR) Scheduling", IEEE Conf. on Confluence 2013: The Next Generation Information Technology Summit , 2012, pp 308 – 314..
[6] Jianfeng Yang, Zhibin Chen "Cloud Computing Research and Security Issues", IEEE Conf. on Computational Intelligence and Software Engineering (CiSE), 2010, pp 1-3.
[7] Jaber, A.N. "Use of cryptography in cloud computing", IEEE Conf. on Control System, Computing and Engineering (ICCSCE) , 2013, pp 179 - 184.
[8] Kalagiakos, P. Karampelas, P "Cloud computing learning" IEEE Conf. on Application of Information and Communication Technologies (AICT) , 2011, pp 1 – 4.
[9] Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth "A Layered Security Approach for Cloud Computing Infrastructure" 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009, pp 4-10.
[10] Md. Imrul Kayeset al. "Test Case Prioritization for Regression Testing Based on Fault Dependency" IEEE Conf. on Electronics Computer Technology (ICECT), 2013, pp 48 – 52.
[11] Mohammed Achemlal, Saıd Gharoutand Chrystel Gabber "Trusted Platform Module as an Enabler for Security in Cloud Computing" IEEE Conf. on Network and Information Systems Security (SAR-SSI), 2011, pp 1 – 6.
[12] Sravan Kumar R, AshutoshSaxena "Data Integrity Proofs in Cloud Storage" IEEE Conf. on Communication Systems and Networks (COMSNETS), 2011, pp 1 - 4