International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Enhancing Data Security of Data on Rest in Cloud using RSA and BLOWFISH Algorithm

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

[1, 2]Department of Computer Science, Punjabi University, Patiala, India

Abstract: ***In the cloud space different users provide their secret information on cloud environment or secure the information. In the purposed paper different approaches have been used for the security of the data. In this firstly the validation of the user has been done. In this the user want to access the data then firstly himself have to be provide username and secret key that has been transmitted via email on authorized mail address. The user cans upload and download data after the validation process get complete. In this user uploads its data and contents of the file has been extracted for encryption process. In the purposed approach RSA and BLOWFISH algorithm has been used for encryption of the data. In the purposed work key generator generates a private key and the RSA approach use the modules function to convert cipher text into plain text. After RSA on the cipher text the blowfish algorithm has been implemented that that reconvert the cipher text into the blowfish cipher text. After this the data can be stored on cloud and can be downloaded by authorized user. If any authorized user can be able to get secret data then due to encryption user will not be able to extract the information without decryption key.***

Keywords: Cloud computing, Cloud security, Blow fish algorithm

1. Introduction

Storing data into the cloud, gives great convenience to users as they don't have to care about the complexities of resource management. Cloud pioneers like Amazon Simple Storage.

Service (S3) and Amazon Elastic Compute Cloud (EC2), gives huge amounts of storage space and customizable computing resources. Due to this, responsibility of local machines for data maintenanceis eliminating. As a result, cloud users are at the mercy of their service providers for the availability and integrity of their data, downtime of Amazon's S3 is an example. From the perspective of data security, which has always been an important aspect of QOS(quality of service), Cloud Computing inevitably poses new challenging security threats for numberof reasons.

Some of these are:

1) Traditional cryptographic primitives for the purpose of data security protection can't be directly adopted, due to this user control lose on data on cloud.
2) Ensure storage correctness under dynamic data update(can be insertion, deletion and modification) of stored data.
3) Deployment of Cloud Computing powered by data centers running in a simultaneous, cooperated and distributed manner.
4) Analyzing the above threats we have constructed a system which can handle these threats. System Consist of different components and some of these components ensures safety from above threats.

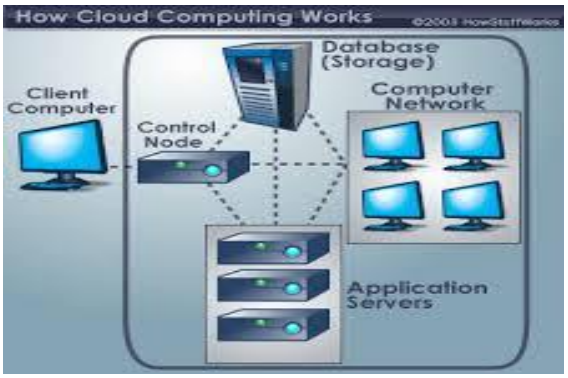


Figure 1: Working of Cloud Computing

Hardware and software demands on the user's side decrease. The only thing the user's computer required to be able to run is the cloud computing systemsinterface software**,** which can be as simple as a Web browser and the cloud's network takes care of the rest. They are already used some form of cloud computing. If you have an e-mail account with a Web-based e-mail service like Hotmail, Yahoo! Mail or Gmail, then you've had some experience with cloud computing. You can log in to a Web e-mail account remotely Instead of running an e-mail program on your computer. The software and storage for your account doesn't exist on your computer it's on the service's computer cloud.

As the data is in the cloud different companies and countries have different requirements as well as controls placed on access because we may not realize that the data must reside in some physical location.

- Every cloud provider should have all the agreements in writing to provide maximum transparency to provide the different level of security required by different customers.
- Every cloud provider must have fixed service level agreements regarding various things such as data privacy, limit of third party access to the confidential data etc.
- Access control is a key concern as insider attacks also possess a huge risk. Anyone who has been entrusted with proper authentication to the cloud could be a potential hacker. If anyone doubts this, consider in 2009 an insider

was accused of planting a logic bomb on Fannie Mae servers, if launched it would have caused massive damage.
- The standards have been defined to ensure that third parties have sufficient control in handling data. ISO 27001 and SAS 70 have been adapted to ensure maximum cloud security

1.1 Cloud Computing Security

Cloud computing is becoming very popular computing paradigm for network applications in open distributed environments.[8] In essence, the idea is to host various application servers in a virtual network environment ("cloud") and offer their use through the concept of (Web) and other services. Contrary to classical network applications approach in the form of client–server model, in a cloud environment users do not access individual application servers, do not establish direct connections with them, do not send request messages directly to those servers, and do not receive direct replies from them. Instead, clients access those application servers through cloud access proxies, special servers that perform publishing and exporting various (usually Web) services available in a cloud. In such environments, security has much more important role than in classical network, client– server, environments. Not only that the same, standard, security services are needed (authentication, authorization, confidentially, integrity, authorization, etc.), but their provision must be offered to clients transparently and in an environment comprising distributed components and delegated authorities. Cloud computing makes security not only much more important, but also much more difficult to organize and manage, due to the transparent nature of cloud resources, components, and services.

There are still many open and interesting issues regarding cloud computing paradigm and standards are still evolving. But, it is a general opinion that security is indeed one of the most important issues. In the recent IDC report over 74% of users think that security is dominant issue for widespread use of cloud computing services:

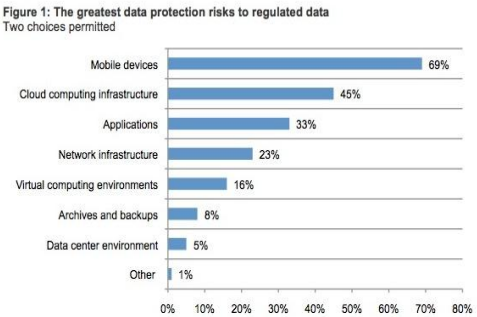


Figure 2: Importance of Security for Cloud Computing Environments

1.2 Major Risks of cloud computing security

There are a lot of security issues in cloud computing service environments such as virtualization, distributes big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs user authentication and access control model for integrated management and control in cloud computing environments [8]

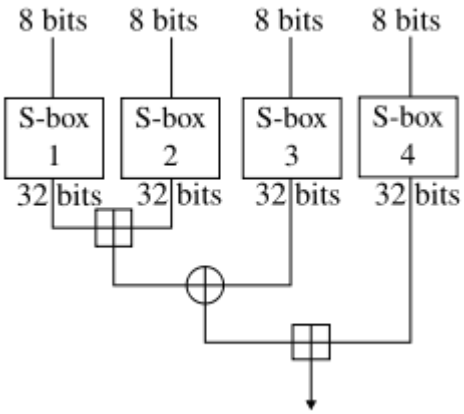
Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic in specific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:
- Data Storage
- Legal and Regulatory Risks
- Privacy and Confidentiality
- Availability
- Integrity
- Computationally feasible
- Proper usage metering
- Internal and external attacks
- Abusing cloud's resources

Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc. Blowfish is a symmetric block encryption algorithm designed in consideration with.
- **Fast:** It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
- **Compact:** It can run in less than 5K of memory.
- **Simple:** It uses addition, XOR, lookup table with 32-bit operands.
- **Secure:** The key length is variable, it can be in the range of 32~448 bits: default 128 bits key length.
- It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor.
- Unpatented and royality-free.

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.it will follows the feistel network and this algorithm is divided into two parts.
1. Key-expansion
2. Data Encryption

Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes.

The diagram to the left shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.



The Feistel structure of Blowfish

The diagram to the right shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order.

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern. The secret key is then XORed with the P-entries in order (cycling the key if necessary). A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P1 and P2. The ciphertext is then encrypted again with the new subkeys, and P3 and P4 are replaced by the new ciphertext. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4KB of data is processed.

2. Methodology

Problem formulation/Need and significance of proposed research work

The idea behind cloud computing is similar that The user can simply use storage, computing power, or specially crafted development environments, without having to worry how these work internally. Cloud computing is a systems architecture model for Internet-based computing. The main problem which was faced during cloud computing is that data accessed using various resources needs user authentication and access control model for integrated management and control in cloud that environments. Security is a main issue for cloud computing, its interestingness and recognition created a great problem for researches to pursue this topic in detail. Many security concerns evolved while benefits of using cloud computing. Integrity for data checking was also a problem in the work done till now. So, due to these internal and external attacks of security and integrity we need to put security checks and one time password.

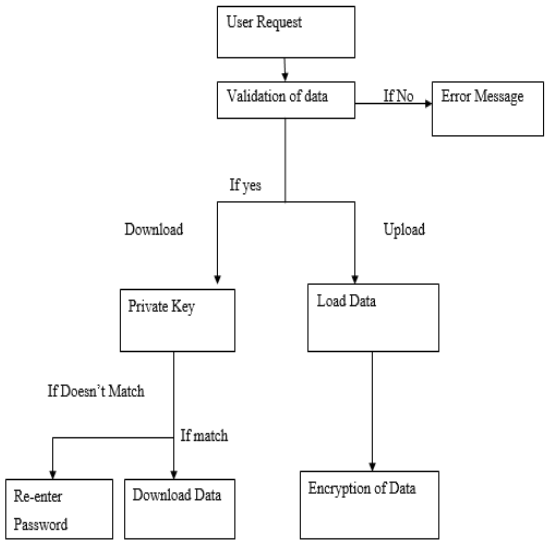


Figure 2: Flow of work

3. Results

Any text file is selected and after choosing that text file it is uploaded as shown in Fig. 3. After that the user can encrypt that text file into Cypher text which is shown in Fig 4, after that user can decrypt that file by pressing the decrypt button as shown in Fig. 5.

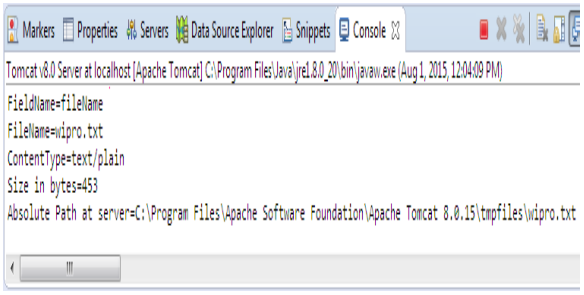


Figure 3: uploading of file

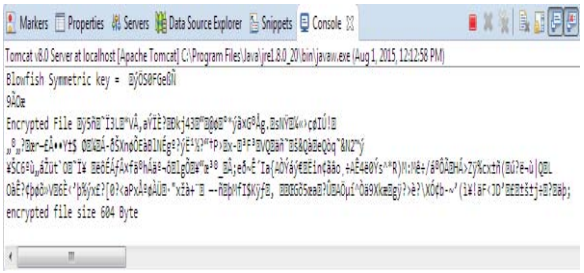


Figure 4: Appling blow fish encryption

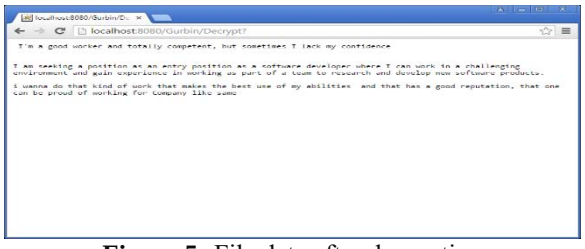


Figure 5: File data after decryption

Table 1: Computation time for encryption of data of different sizes

Sr. No.	Files	Proposed	AES Encryption	Percentage improvement
		Time (in ms)		
1	2.2 KB	95	101	6.3 %
2	1.35 KB	79	86	8.8 %
3	3.54 KB	110	121	10 %
4	3 KB	102	111	8.9 %
5	2.4 KB	97	105	8.2 %
6	1 MB	415	488	17.59 %
7	2 MB	559	605	8.3 %

Table 1 represents computation time for encryption of different sizes. In this the values calculated of previous and proposed work for the files of different sizes are represented.

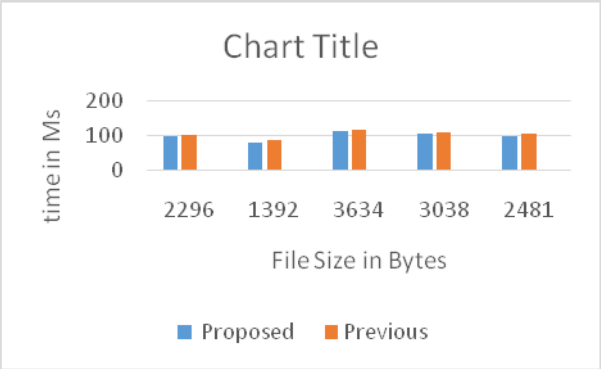


Figure 6: Graph representation of computation time

Fig. 6 represents the graph showing the comparison of computation time for the file for the previous work and present work.

Sr. No.	Files (in bytes)	Proposed	AES Encryption	Percentage improvement
		File Size In bytes		
1	2296	3586	3965	10 %
2	1392	2015	2386	18 %
3	3634	5028	5569	10.76 %
4	3038	3865	4215	9 %
5	2481	3658	4008	9.5 %
6	108456	132544	158008	19.2 %
7	189456	220120	235608	7 %

This table represents the file size of different file have been changed after the process of encryption. The encryption process adds the padding bits to the data that increase the size of the files. In this table the size represents that in the proposed work the file size increases but less than that of the previous AES encryption.

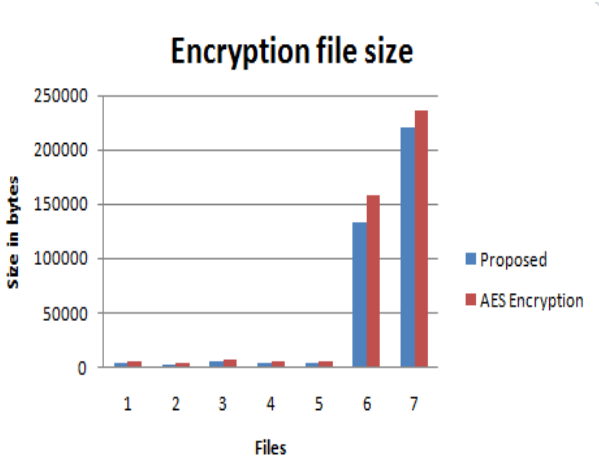


Figure 7: graph representation for file sizes after encryption

This figure represents the graphical representation between different files for encryption using proposed approach and AES encryption standard.

4. Conclusion

Cloud computing is the environment that has been used in various approaches in recent applications. In the concept of cloud computing different virtual machines have been used for allocation of data to different machines. In this process the space has been allocated to different users on private cloud. In the cloud computing environment different users get access for cloud environment. In the cloud space different users provide their secret information on cloud environment of secure the information. In the proposed work different approaches have been used for the security of the data. In this firstly the validation of the user has been done. In this the user want to access the data then firstly himself have to be provide username and secret key that has been transmitted via email on authorized mail address. The user cans upload and download data after the validation process get complete. In this user uploads its data and contents of the file has been extracted for encryption process. In the proposed approach RSA and BLOWFISH algorithm has been used for encryption of the data. A key generator generates a private key and the RSA approach use the modules function to convert cipher text into plain text. After RSA on the cipher text the blowfish algorithm has been implemented that that reconvert the cipher text into the blowfish cipher text. After this the data can be stored on cloud and can be downloaded by authorized user. If any authorized user can be able to get secret data then due to encryption user will not be able to extract the information without decryption key. The proposed work has been providing better security to the secret information of the user than the previous approaches. The user can access the data after only validation process. The validation of the proposed work has been done by using various parameters. These parameters are computation time and encryption file size. In this work the comparative study has been done with AES encryption approach. The proposed work provides 15 % better results than that of AES encryption approach.

References

[1] Ahmed DheyaaBasha, Irfan Naufal Umar, and Merza Abbas, Member, IACSIT "Mobile Applications as Cloud Computing: Implementation and Challenge",7865-7564,IEEE,2013.
[2] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
[3] RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing
[4] RuWei Huang, Si Yu, Wei Zhuang and XiaoLinGui, "Research on Privacy-Preserving Cloud Storage Framework Supporting Cipher text Retrieval" 2011 Ninth International Conference on Grid and Cloud Computing.
[5] FarzadSabahi, "Cloud Computing Security Threats and Responses," IEEE Trans. on Cloud Computing., vol. 11, no. 6, pp. 670 { 684, 2002.}
[6] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.
[7] Mehmet Yildiz, JemalAbawajy, TuncayErcan and Andrew Bernoth "A Layered Security Approach for Cloud Computing Infrastructure" 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. © 2009 IEEE.
[8] Jianfeng Yang, Zhibin Chen "Cloud Computing Research and Security Issues" Vol 978-1-4244-5392-4/10/$26.00 ©2010 IEEE
[9] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh "Personal Cloud Computing Security Framework" 2010 IEEE Asia-Pacific Services Computing Conference.
[10] Mohammed Achemlal, Sa¨ıdGharoutandChrystel Gaber "Trusted Platform Module as an Enabler for Security in Cloud Computing" Vol. 978-1-4577-0737-7/11/$26.00 ©2011, IEEE.
[11] Ranjita Mishra, Sanjit Kumar Dash "A Privacy Preserving Repository for Securing Data across the Cloud" Vol. 978-1-4244-8679-3/11/$26.00 ©2011 IEEE
[12] Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee "From System-centric to Data-centric Logging – Accountability, Trust & Security in Cloud Computing" IEEE Computer Society, 2011.
[13] Shucheng Yu, CongWang, Kui Ren and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" at IEEE INFOCOM 2010.