Implementation of Modified Security Paradigm to Data for Cloud Computing

[1] S.Rajan (Reg No: 12338), [2] Dr.D.S.Mahendran, [3] Dr.S.John Peter
[1] Assistant Professor and Head, (Research Scholar), Dept of Computer Science [SF], Kamaraj College (Affiliated to Manonmaniam Sundaranar University, Tirunelveli), Tuticorin, Tamil Nadu, India.
[2] Principal, (Guide), Aditanar College of Arts & Science (Affiliated to Manonmaniam Sundaranar University, Tirunelveli), Tiruchendur, Tamil Nadu, India
[3] Associate Professor & Head of Research Center, (Co-Guide), Dept of Computer Science, St.Xavier College (Autonomous and Affiliated to Manonmaniam Sundaranar University, Tirunelveli), Palayamkottai, Tamil Nadu, India.

Abstract

Today cloud plays a vital role in all walks of Information Technology. Applications and data moved to Cloud can be accessed at anytime, at anywhere and in any device. So lots of business organizations from small to large are showing great interest to migrate to cloud but they revert due to some yet to solve security issues in cloud. The main problem is that they are reluctant to put their sensitive data in an unknown third party Data Center not owned by them. To address this security issue, we have already come up with an Effective and Efficient cryptographic algorithms which can be used for transmission, storage and key-exchange through cryptanalysis on different symmetric and asymmetric cryptographic algorithms. In this paper based on the study a New Security Frame work for cloud is designed and implemented in an effective and efficient manner.

Keyword: Cloud, Data, Security issues, Cryptographic algorithm, New Security Frame Work

Introduction

Cloud computing concept doesn't arise suddenly but it dates back to 1960's when time sharing technology has shown the way to the new development in the utilization of computer resources in computer system. In Mainframe computers TP Monitor is used for effectively managing all the computer resources later due to advancement in low cost involved in distributed computing and internet led to the development of client-server technology. Now the Technology is moving towards the centralized Server-based architecture and TP monitor architecture is taking the new form in the name of hypervisor. Today Cloud computing is the revolutionary technology with most of the companies are ready to move to the cloud if proper Security is provided to them.

Cloud computing can be categorized as SaaS, PaaS, IaaS, HaaS etc based on the services it provides. Again Cloud can be categorized as public cloud, private Cloud and hybrid cloud based on the location of the cloud. The best network where we can place the Sensitive data is private cloud as data center is placed inside the organization's premises but to attain protective security, the private cloud should be properly configured for security through firewall and security policies. The cost involved in private cloud is very high and suitable only for big corporations with sensitive data. So, Small and medium companies are hesitant with private cloud. As hybrid cloud interfaces with private and public infrastructure, special care should be taken for the security of the interface gateway, it also needs huge investment in infrastructure and security development. To attain the reasonably priced cloud [11] one should go for public cloud. The main concern in the case of public cloud is security as all the communications are done though shared network called internet. Security lapse may occur due to vulnerability in hypervisor, denial of service attack, dictionary

attack, viruses, man-in-the-middle attack etc. To overcome the above drawbacks we need authenticated access control over the resources in the public cloud where communication is done through the public network called internet. In this paper a security frame work is developed which gives security and privacy protection for the data and focuses mainly for public cloud.

Literature Review

We have seen that security is the main issue in cloud. This section analyses the various researches done in connection with the implementation of security in Cloud.

Ahmed Albugmi, Madini O. Alassafi and Robert Walters discusses about the various risks involved in the unprotected data in cloud further it concludes that threats caused by compromising hypervisor and Multitenant is very severe and it can be overcome by best authentication for data before de-allocation. The paper also discusses about the efficient technique for encryption in Cloud [8].

Parsi Kalpana and sudha singaraju proposes RSA algorithm for storing data in the cloud but did not discuss about the security in Transit [2].

Gawali, Wagh and Patil proposed model with presentation layer, Business Logic Layer and Data Access Layer to overcome the security lapse in Multi-tenancy [1].

Sanjoli Singla and Jasmeet Singh implemented data security on cloud through Rijndael Encryption algorithm [3].

Goikar Vandana T., Jagdale Supriya K., Parade Priya B.and Pawar Sumedha D in their paper proposed a security model in which banking data are protected by location based and Geo Encryption algorithm. The biggest drawback in this approach is the non-availability of data in other location which will hinder the anywhere banking [5].

Rimmy Chuchra and R.K Seth proposed a token based security where token acts as a digital certificate and authentication to data are possible only after verification of tokens. It did not specify how token-Id is protected from intruders [6].

K.Hajarathaiah, T.SeshuChakravarth and G. Raphi proposed security solution where Data present in failed server can be recovered through Cross-over server through distributed protocol [4].

Manisha R. Shinde and Rahul D. Taur analyzed the feasibility of the encryption algorithm for data security and privacy in cloud Storage and concluded that encryption and decryptions of data will boost consumer confidence, give peace of mind and attract more people to cloud platform if user given more control over it [7].

M. Thangapandiyan, P. M. Rubesh Anand and K. Sakthidasan proposed a Modified Elliptic Curve Cryptography (MECC) algorithm to provide privacy to sensitive data in Cloud [12].

Hongbing Cheng, Chunming Rong, Manyun Qian, and Weihong Wang proposed a privacy-preserving Mechanism based on IBE scheme [14].

Ms.Neha, Mahakalkar and Mrs.Vaishali Sahare proposes re-encryption technique to provide high security for user private data [9].

S.Rajan, Dr.D.S.Mahendran and Dr.S.John Peter proposed the scalable map reduce model for finding Aathaar number linked to the bank account [10]

In the previous paper Based on study on different symmetric, asymmetric and key exchange algorithms, we found that Blow Fish, AES, RSA and MD5 are best suited for Cloud [13].

Existing Model

In the existing model, there are many solutions for security with a Single Cryptographic algorithm for data transmission which may make intruder predict the plain text from cipher text and Security Solution for cloud is evolving.

Proposed Model

The proposed secure Cloud Model has the following players

1) Cloud Service Provider

2) Automatic Cryptographic Algorithm Selection and key distribution center (ACAS_KDC)
3) Data owner
4) User

Cloud Service Provider: Provides cloud data storage service and infrastructure needed for it.

Automatic Cryptographic Algorithm Selection and Key Distribution Center (ACAS_KDC): Selects the algorithm from the given set of best cryptographic algorithm based on file size and file type for transmitting data in the cloud.

Data Owner: owner of the organization who hosts data on the cloud. In some cases user will also be a Data Owner.

User: one who access data based on access control in the cloud.

Terms used

ACAS_KDC Server: Automatic cryptographic Algorithm Selection and Key Distribution Center in the server side.

ACAS_KDC Client: Automatic cryptographic Algorithm Selection and Key Distribution Center in the Client side.

Persistent Encryption/Decryption: Encryption/ Decryption done for permanent storage.

Transit Encryption/Decryption: Encryption/Decryption done for data transmission.

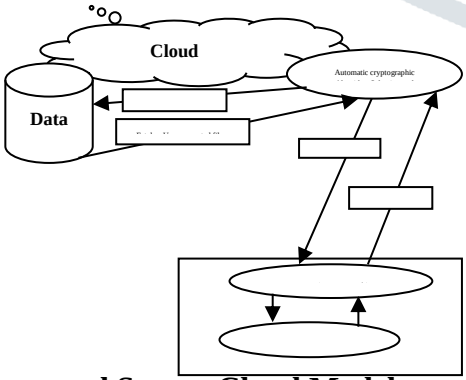


Fig 1: Proposed Secure Cloud Model - Downloading

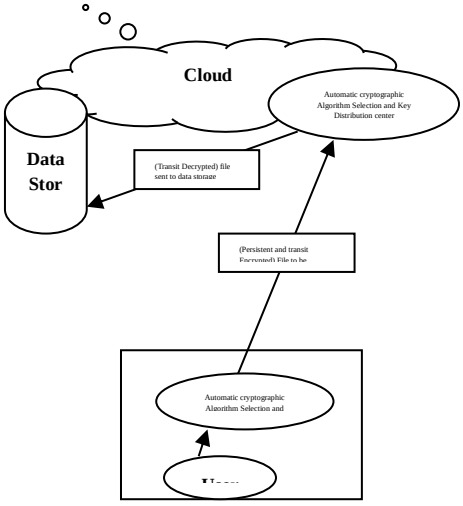


Fig 2: Proposed Secure Cloud Model – uploading

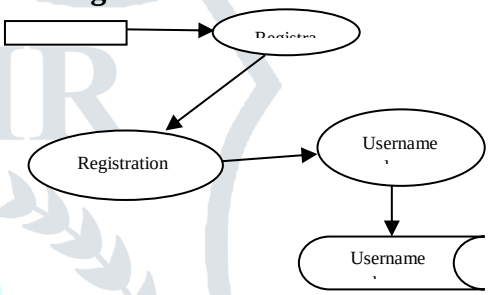


Fig 3: Registration Process

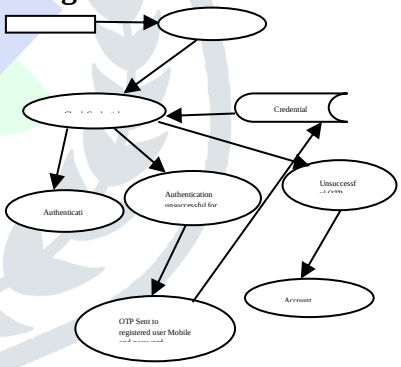


Fig 4: Login Process

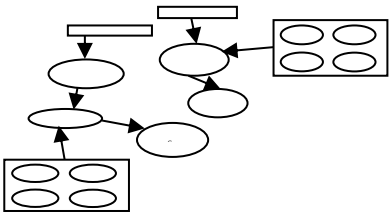


Fig 5: ACAS_KDC Server

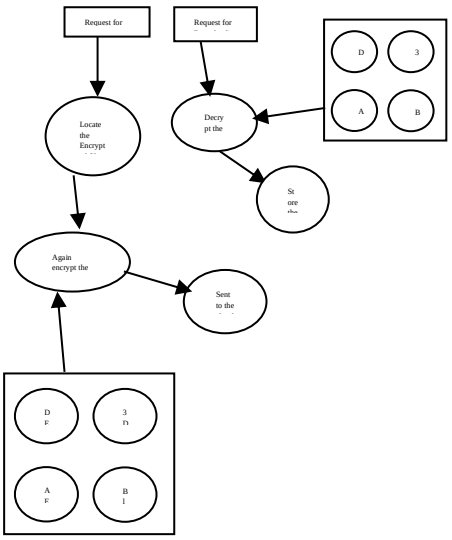


Fig 6: ACAS_KDC Client

Working Process of Proposed Model

i) Downloading File

Step 1: User requests for the file to the automatic cryptographic algorithm selection and key distribution center (ACAS_KDC Server)

Step 2: ACAS_KDC Server searches the persistent Encrypted file in the Data storage and locates the file

Step 3: The located file is again transit Encrypted by choosing the best cryptographic algorithm based on the file type and file size and sent to the requested user. This whole process is done by ACAS_KDC Server.

Step 4: The encrypted file (Persistent and transit Encrypted) is received by the ACAS_KDC Client and transit decrypted in the user system and stored in the user system.

Step 5: The stored file is again decrypted by (persistent decryption) for viewing.

ii) Uploading File

Step 1: User encrypts (persistent encryption) the file to be uploaded to the cloud.

Step 2: The file is again encrypted (Transit encrypted) by ACAS_KDC Client.

Step 4: The Encrypted (Persistent and Transit encrypted) file is sent to the cloud

Step 5: In cloud the Encrypted (Persistent and Transit encrypted) file is received by the ACAS_KDC Server.

Step 6: ACAS_KDC Server decrypts (Transit decrypted) the file and stores it in the Data storage.

iii) Registration Process

Step 1: User or Data owner should provide the e-mail id for username; password and Phone number as mandatory along with their profile for Registration.

Step 2: The details provided will be stored in the database.

iv) Login Process

Step 1: User or Admin should enter their username and password.

Step 2: The given username and password is checked for their credentials with the credential database if it matches, the authenticated process succeeds.

Step 3: If the credentials are unsuccessful for three times, OTP will be sent to the user phone number as message and password updated in the database. The Account will be locked if the user fails to give the correct OTP Password.

v) ACAS_KDC Server

Downloading File

Step 1: Requested Encrypted (persistent Encrypted) file is searched and located in the cloud

Step 2: The file is again encrypted (transit encryption) and sent to the user.

Uploading File

Encrypted (both persistent and transit) file is decrypted (transit decryption) and stored in the cloud in encrypted form (persistent Encryption)

vi) ACAS_KDC Client

Uploading File

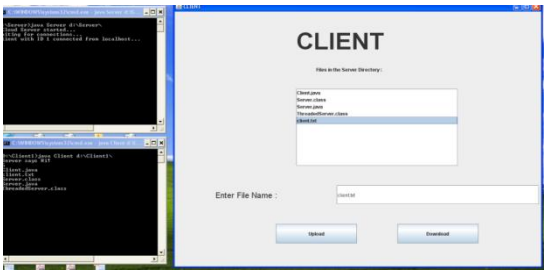
Step 1: Requested Encrypted (persistent Encrypted) file is searched and located in the user system

Step 2: The file is again encrypted (transit encryption) and sent to the Cloud.

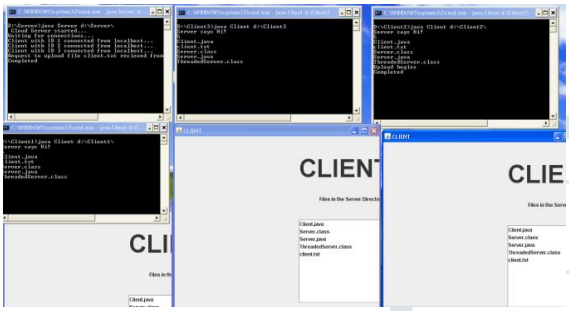
Downloading File

Encrypted (both persistent and transit) file is decrypted (transit decryption) and stored in the user system in encrypted form (persistent Encryption)

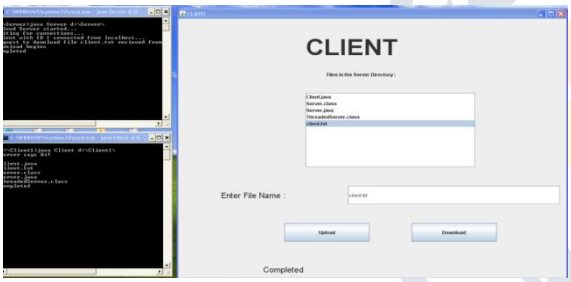
Screenshots from Cloud Prototype Developed



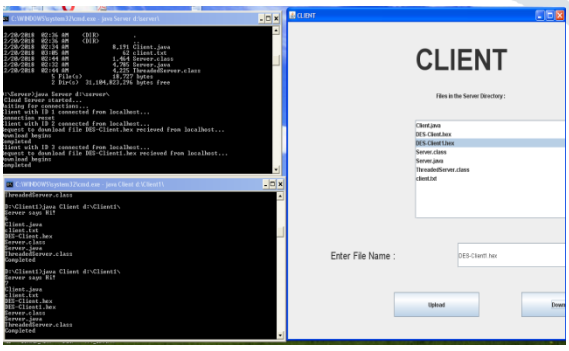
Screen shot 1: Single client connected with Cloud Server



Screen Shot 2: Multiple Clients Connected with Cloud Server.



Screen shot 3: File downloaded to Client.



Screen shot 4: File uploaded to Server

Performance of the proposed model

System Details in which testing performed.

Client Machine

Operating System used: Windows Xp with Service pack 3 Build 2600
Processor used: x86 Family 15 Model 107 Stepping 1 Authentic AMD 2109 MHz
Memory: 1 GB RAM

Prototype Cloud Server

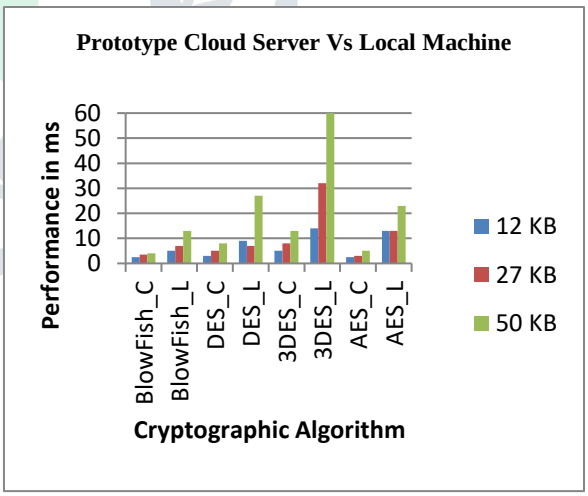
Operating System: windows 2012 server
Processor: Xeon Processor
RAM: 8 GB
HDD: 1 TB

Processing Time (ms) in Cloud				
Size (KB)	Blowfish	DES	3DES	AES
12	2.5	3	5	2.5
27	3.5	5	8	3
50	4	8	13	5

Table 1: Processing Time in prototype Cloud Server

Processing Time (ms) in Local Machine				
Size (KB)	Blowfish	DES	3DES	AES
12	5	9	14	13
27	7	7	32	13
50	13	27	60	23

Table 2: Processing Time in Local Machine



Graph 1: Processing Time Comparison -Cloud Vs Local Machine

Conclusion

The processing time for ACAS_KDC Server in Prototype server is less than ACAS_KDC Client in the local machine. This is due to the low configuration machine in the client

side. The Blowfish and DES are showing steady in performance both in server and client when compared to 3DES and AES. We also observed that the file is always in Single Encrypted form (Persistent Encryption) while in disk storage and is always in double Encryption form (Persistent and transit Encryption) while travelling in transmission Medium. So the data is more secure in the Cloud. The algorithm is chosen based on file size and type, so it is very difficult to identify the algorithm for the hackers.

References

[1] Gawali, Wagh and Patil "Enhancement For Data Security in Cloud Computing Environment," International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, ISS- 3 2012

[2] Parsi Kalpana, sudha singaraju "Data Security in Cloud Computing using RSA Algorithm," International Journal of Research in Computer and Communication technology, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[3] Sanjoli Singla and Jasmeet Singh, "Implementing Cloud Data Security by Encryption using Rijndael Algorithm," Global Journal of Computer Science and Technology Cloud and Distributed Volume 13 Issue 4 Year 2013

[4] K.Hajarathaiah, T.SeshuChakravarth and G. Raphi "Dynamic Operation Implementation in storage of Cloud Computing" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014

[5] Goikar Vandana T., Jagdale Supriya K., Parade Priya B.and Pawar Sumedha D "Improve Security Of Data Access In Cloud Computing Using Location" International Journal of Computer Science and Mobile Computing, Vol.4 Issue.2, pg. 331-340, February- 2015.

[6] Rimmy Chuchra and R.K Seth "Modeling Implementation of TBDSA-Token based Data Security Algorithm in Cloud Computing," International Journal of Computer Applications (0975 – 8887)Volume 114 – No. 7, March 2015

[7] Manisha R. Shinde and Rahul D. Taur "Encryption Algorithm for Data Security and Privacy in Cloud Storage", AJCSES[3][1][2015] 034-039, 2015

[8] Ahmed Albugmi Madini O. Alassafi Robert Walters, "Data Security in cloud Computing," Fifth International Conference on Future Generation Communication Technology 2016.

[9] Ms.Neha, Mahakalkar and Mrs.Vaishali Sahare "Implementation of Re-encryption Based Security Mechanism to Authenticate Shared Access in Cloud Computing," International Conference on Trends in Electronics and Informatics ICEI 2017

[10] S.Rajan, Dr.D.S.Mahendran and Dr.S.John Peter "Scalable Map Reduce Model for Aggregating the Data in the Cloud," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 4, Issue 12, December 2017

[11] S.Rajan, Dr.D.S Mahendran and Dr. John Peter, "Analysis on Economic Viability of Location Based Cloud," International Journal of Scientific Research in Science and Technology, ISSN: 2395-602X Vol 4, Issue 2, pp. 977 –981, Feb 2018.

[12] Thangapandiyan, P. M. Rubesh Anand and K. Sakthidasan, "Enhanced Cloud Security Implementation using Modified ECC Algorithm," International Conference on Communication and Signal Processing, April 3-5, 2018.

[13] S.Rajan, Dr.D.S.Mahendran and Dr.S.John Peter "Analysis on Cryptographic Algorithms for Effective Secure Implementation of Cryptosystem in Cloud," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018.

[14] Hongbing Cheng, Chunming Rong, Manyun Qian, And Weihong Wang "Accountable Privacy-Preserving Mechanism For Cloud Computing Based On Identity-Based Encryption," 2169-3536 (c) 2018 IEEE.