

INTEGRATION OF MULTILAYER SECURITY ON CLOUD SERVER

¹Preeti, ²Mr. Mahesh Kumar

¹ M.Tech Student, Ganga Institute of Technology and Management, kablana (Jhajjar)

ps25194@gmail.com

² Assistant Professor, Ganga Institute of Technology and Management, kablana (Jhajjar)

maheshmalkani@gmail.com

Abstract

There are several services that are making cloud computing more feasible & easily accessible to users. Cloud computing is providing number of advantages but there are several risks associated with in this technology. Cloud has provided flexible & scalable services. But there would issue of security due to data transfer from one cloud server storage to another cloud. This research would reduce risk to confidentiality & availability of data prior to selecting a cloud vender or choosing own cloud.

Keywords: Cloud Computing, Organizations, Service Model, Infrastructure, Encryption.

1. Introduction

Cloud Computing

Cloud might be network or internet & it is something that is available at remote place. It provides services over network that are public & private. They are used in wide area network, local area network or virtual private network.



Figure 1: Cloud Computing

Advantages

Cloud computing provides several benefits & they are listed below

1. User on internet could access remote applications in form of utilities.

2. User at any time could change & configure application online.
3. Online development tools are offered by cloud computing.

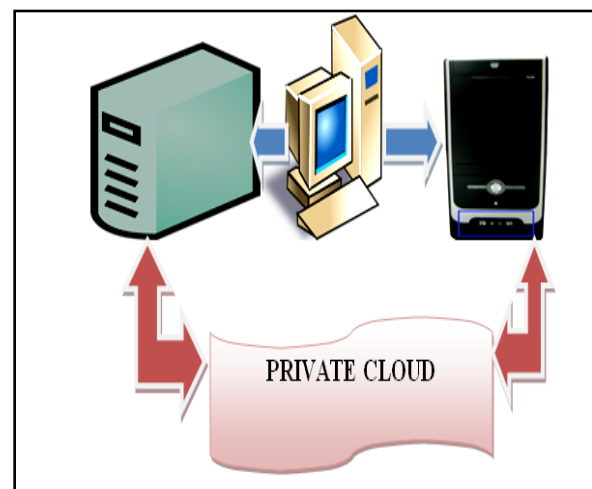


Figure 2: Private Clouds

Cloud Computing Security

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form.

Hybrid cloud

Hybrid cloud is a piece of music of two or extra clouds private, community or public that remain individual entities but are bound together.

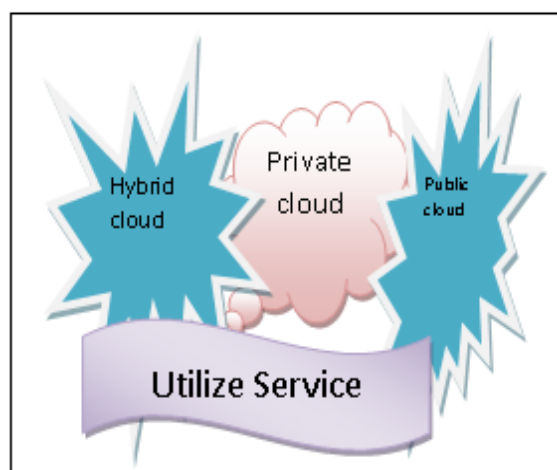


Figure 3: Public cloud vs. Private cloud

2. LITRATURE REVIEW

Mladen A. Vouk (2014) **Cloud Computing – Issues, Research & Implementations**

Cloud computing more or less recent term, built on decagon of scanner in virtualization, scattered computing, utility computing, & more recently networking, web & software services.

Raj Kumar (2015) **Research on Cloud Computing Security Threats using Data Transmission**

Computer Science & Software Engineering Cloud computing is set of resources & services offered through Internet. Cloud duty are delivered from folder centres located throughout world. Cloud computing simplify its consumers by providing virtual resources via internet.

Meiko Jensen (2009) **On Technical Security Issues in Cloud Computing 2009**

The Cloud Computing concept offers dynamically scalable resources provisioned as a service over Internet. Economic benefits are main driver for Cloud, since it promises reduction of capital expenditure (CapEx) & operational expenditure (OpEx).

3. TOOLS AND TECHNOLOGY

CLIENT SERVER MODEL

It is possible for two network applications to begin simultaneously, but it is impractical to require it.

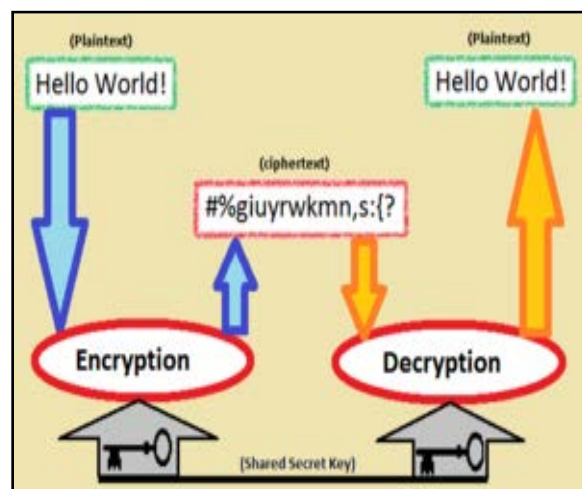
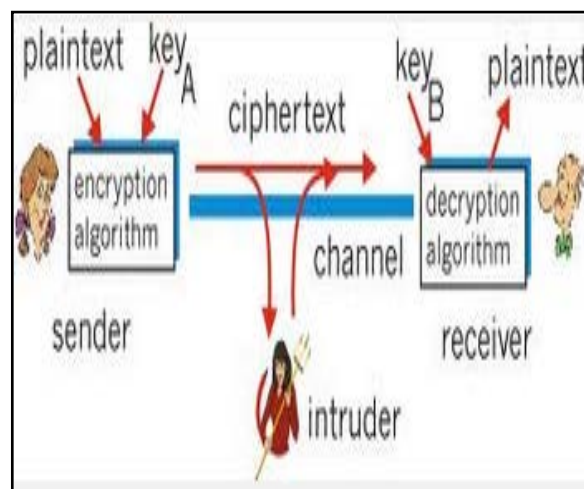


Figure 4: Encryption & Decryption of text

Cryptography

Modern cryptography is heavily based on mathematical theory & computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.



giFureyhpargotpyrC :5

MATLAB

Mat lab As a Simulation Tool

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, & programming in an easy-to-use environment where problems & solutions are expressed in familiar mathematical notation. Typical uses include: Math & computation.

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment & fourth-generation programming language. Developed by

Math Works, MATLAB allows matrix manipulations, plotting of functions & data, implementation of algorithms, creation of user interfaces, & interfacing within programs written in other languages, including C, C++, Java, Fortran & Python.

4. PROPOSED WORK

Due to limitation of existing security mechanisms there was need to develop a new security system. Chance for decryption without authentication should get reduced. We need to implement IP filter based security in order to prevent attacker from different network. Here we would also reduce size of packet during transmission using replacement policy. We would enhance Advanced Encryption standard by introducing multilayer security.

5. IMPLEMENTATION

In implementation, we encrypted data of word file from plain text to cipher text. Here we have developed an encryption module and run the command at java prompt. The name of java file is File Encrypt or that reads the data from file and encrypts the data.

Step 1: Encryption

```
C:\Java\jdk\bin>javac FileEncryptor.java
C:\Java\jdk\bin>java FileEncryptor VISUALBASIC6.DOC
C:\Java\jdk\bin>
```

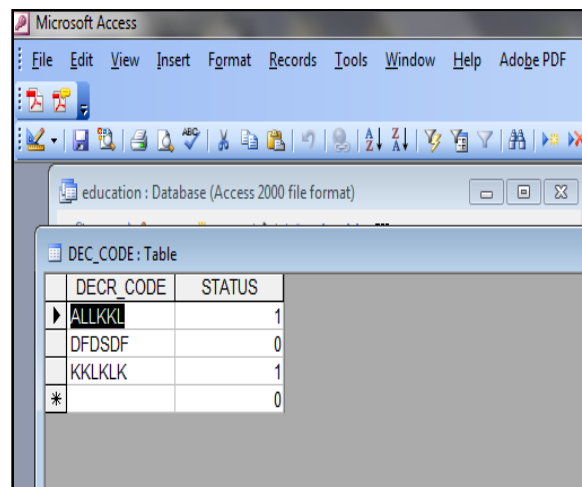
Figure 6: Encryption Process

Step 2: Here in second step we create a database to store the decryption code. Here we have stored valid codes for decryption purpose.

DEC_CODE: Table		
	Field Name	Data Type
	DECR_CODE	Text
	STATUS	Number

Figure 7: DEC_CODE schemas

Step 3: Here we have to make some entries in dec_code so that we could decrypt the data. MAKE SOME ENTRY IN DEC_CODE. And specify the status 1 if code is active and 0 if code is not active.



DEC_CODE: Table		
	DECR_CODE	STATUS
	ALLKKL	1
	DFDSDF	0
	KKLKLL	1
	*	0

Figure 8: Entry in DEC_CODE Table

Step 4: In order to connect database with table we have to create dsn from odbc in administrator tool of control panel. Make DSN OF "EDUCATION TABLE" CONTROL PANEL-> ADMINISTRATION TOOLS-> ODBC->

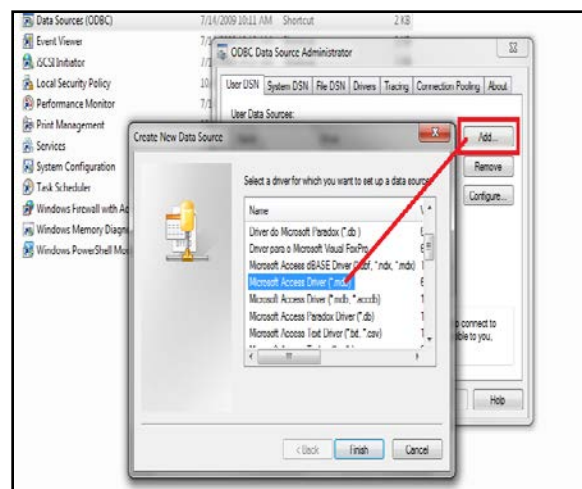


Figure 9: Adding MS Access Driver

Step 5: Here we have to specify the driver according to database used. We have used Microsoft Access so we select Microsoft access Driver & finish.

Step 6: When we browse that we are asked name of database. After choosing database from particular drive & directory we select Database & set DSN name to "edu".

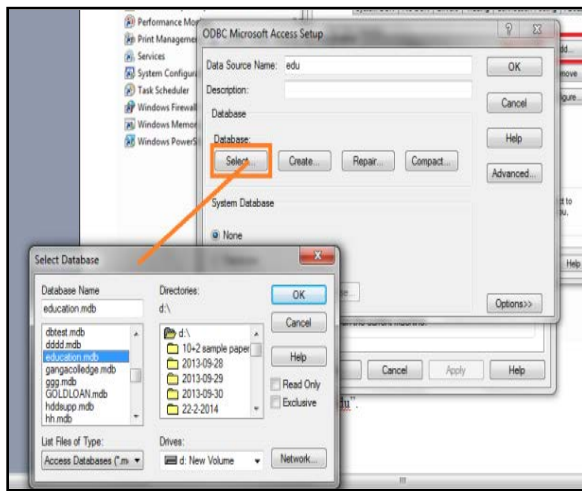


Figure 10: Selection of database

Step 7: Decryption: during this process, we convert cipher text to plain text using FileDecryptor.java module. But user has to pass valid Decr_code to decrypt data. If Decr_code is not available in table or status is 0 the user fails to decrypt the file. If Decr_code is available and status is 1 then the user successfully decrypts the file.

	DECR_CODE	STATUS
▶	ALLKKL	1
	DFDSDF	0
	KKLKLK	1
*		0

Figure 11: Entry in DEC_CODE

When we give command to decrypt data on command prompt then a new file is created with DEC extension.



Figure 12: Decryption process

Following is the decryption file that has been generated after decryption.

Step 8: In order to use the file remove .enc.dec extension of file & use it.

IP FILTER TABLE

This is the second layer security. Here we have given a IP TABLE that will authenticate the IP

address of client. This table assures the list of valid IP address of client who are eligible to decrypt data.

Table 1.1: IP Filter Table

iptable		
IP	STATUS	Add New Field
1.0.0.1	1	
126.0.0.1	0	
127.0.0.1	0	
128.0.0.1	1	
*		

OTP FUNCTIONALITY

In the third layer of security, we generated one time password of the system. One time password enhances the security of system. It is most commonly used in banking system the password one used should be deactivated after one time use.

DATA ANALYSIS WORK

We have make reading of packet transmission time in different cases such as fibre optic, coaxial, twisted pair cable.

Table 1.2: Data in case of Fibre optics

Sno	Security_Level	H	L	Avg
1	Layer1(cr)	20	40	30
2	Layer2(ip)	15	30	22.5
3	Layer3(otp)	10	20	15
4	L1+L2	40	80	60
5	L1+L3	35	70	52.5
6	L2+L3	30	60	45
7	L1+L2+L3(slow_net)	55	110	82.5
8	L1+L2+L3(avg_net)	50	100	75
9	L1+L2+L3(High_net)	48	96	72
10	L1+L2(avg_net)	45	90	67.5
11	L1+L3(avg_net)	40	80	60
12	L2+L3(avg_net)	35	70	52.5

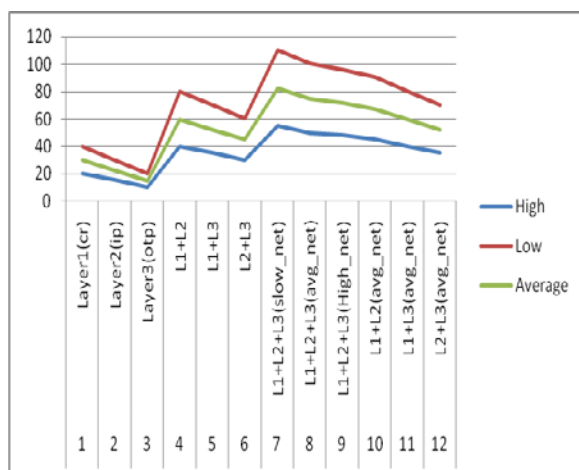


Figure 13: Analysis of transmission speed of packet in case of Fiber optics

Table 1.2: Data in case of Coaxial Cable

Sn.	Security_Level	H	L	Avg
1	Layer1(cr)	25	50	37.5
2	Layer2(ip)	20	40	30
3	Layer3(otp)	15	30	22.5
4	L1+L2	45	90	67.5
5	L1+L3	40	80	60
6	L2+L3	35	70	52.5
7	L1+L2+L3(slow_net)	60	120	90
8	L1+L2+L3(avg_net)	55	110	82.5
9	L1+L2+L3(High_net)	53	106	79.5
10	L1+L2(avg_net)	50	100	75
11	L1+L3(avg_net)	45	90	67.5
12	L2+L3(avg_net)	40	80	60

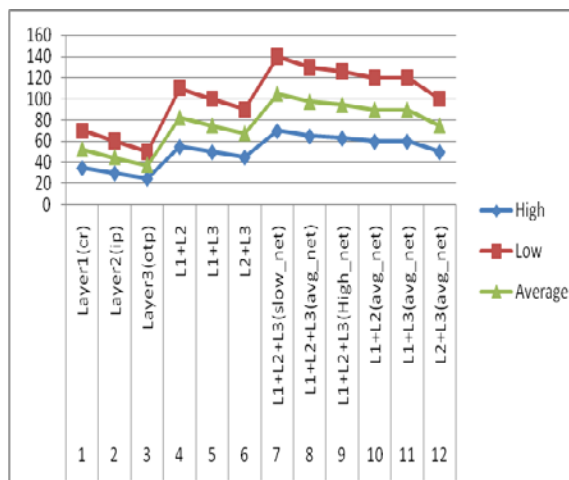


Figure 14: Analysis of transmission speed of packet in case of Wireless network

Table 1.3 Data in case of Twisted Cable

Sno	Security_Level	H	L	Avg
1	Layer1(cr)	30	60	45
2	Layer2(ip)	25	50	37.5
3	Layer3(otp)	20	40	30
4	L1+L2	50	100	75
5	L1+L3	45	90	67.5
6	L2+L3	40	80	60
7	L1+L2+L3(slow_net)	65	130	97.5
8	L1+L2+L3(avg_net)	60	120	90
9	L1+L2+L3(High_net)	58	116	87
10	L1+L2(avg_net)	55	110	82.5
11	L1+L3(avg_net)	50	100	75
12	L2+L3(avg_net)	45	90	67.5

6. FUTURE WORK

In previous researches, there were lot of challenges regarding security cloud computing. New challenges set new demands on cloud computing. In our research, we have provided security to data as well as we have saved data from being destroyed by attacker. In some research, the security key to encrypt data was not much strong and delay was increased in data transmission due to security reasons. Here we have reduced the transmission delay by reducing size of packet and made the security key stronger. Battle btw ethical or white hat hackers & malicious or black hat hackers has been long war, that has no end. While ethical hacker helps to understand companies' their security needs, malicious hackers intrudes illegally & harm network for their personal benefits. Ethical & creative hacking has been significant in network security, in order to ensure that company's data has been well protected & secure. At same time this allows company to identify, & in turn, to take remedial measures to rectify loopholes that exists in security system, that might allow malicious hacker to breach their security system.

7. CONCLUSION

Cloud has provided flexible & scalable services. But there would issue of security due to data transfer from one cloud server storage to another cloud. This research would reduce risk to confidentiality &

availability of data prior to selecting a cloud vendor or choosing own cloud. In previous researches, there were lot of challenges regarding security cloud computing. New challenges set new demands on cloud computing. In our research, we have provided security to data as well as we have saved data from being destroyed by attacker.

REFERENCES

1. Malden A. Vouk (2014) Cloud Computing – Issues, Research & Implementations International Conference on Cloud Computing.
2. Abhinay B.Angadi,(2013) Security Issues within Possible Solutions in Cloud Computing-A Survey International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013
3. Raj Kumar(2015) Research on Cloud Computing Security Threats using Data Transmission Volume 5, Issue 1, January 2015 International Journal of Advanced Research in.
4. Meiko Jensen(2009) On Technical Security Issues in Cloud Computing2009 IEEE International Conference on Cloud Computing.
5. Saju Mathew(2012) Implementation of Cloud Computing in Education – A Revolution International Journal of Computer Theory & Engineering, Vol. 4, No. 3, June 2012
6. Flavio Lobardi(2010) Secure virtualization for cloud computing Journal of Network & Computer Applications
7. Sean Marson(2010) Cloud computing – business perspective journal homepage: www.elsevier.com
8. Monjur Ahmed(2014) cloud computing & security issues in cloud International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
9. Santosh Kuar(2012) cloud computing – research issues, challenges, architecture, platforms & applications: a survey international journal of future computer & communication, vol. 1, no. 4, december 2012.
10. Mladen A. Vouk(2008) Cloud Computing – Issues, Research & Implementations Journal of Computing & Information Technology - CIT 16, 2008
11. Amol C. Adamuthe (2015) Cloud Computing – A market Perspective & Research DirectionsI.J. Information Technology & Computer Science, 2015, 10, 42-53