© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

INVESTIGATION INTO SECURITY LOOP HOLES OF CLOUD SERVER AND SOLUTION USING MULTI LAYER SECURITY MECHANISM

[1]Preeti Lohan, Research Scholar, Department of CSE, IITB College, Sonipat, preeti.lohan30@gmail.com
[2]Ritika Saroha, Assistant Prof. Department – CSE, Department of CSE, IITB College, Sonipat, saroharitika@gmail.com

ABSTRACT: Inspired by the cloud computing characteristics like pay per use, rapid elasticity, scalable, on demand self service, secure and economical. The motivation for cloud computing was initially driven by large scale resource intensive government application, that require more computational, network and storage resources then a single computer, cloud provides in a single administrative domain. Cloud Server is giving importance to its digital collections of multimedia data. The multimedia data are becoming main source of information in a library and the preferred mode of acquisition for collection development. Research studies reveal that any authentication mechanism related to web applications and cloud should provide high security, easy to use interface and support user mobility. Customers prefer to access their applications from different locations and different devices such as desktop, laptop, PDA, smart phones, cell phones etc.

Keyword: Server, Technology, Multimedia, Organization, Rick, Partnership, Network, Resource

[1] Introduction

Cloud Based Government Information System

Cloud computing system has various advantages over traditional client server architecture of the government information system. Governments around the world have started using cloud computing models instead of traditional client server architecture due to advantages of cloud computing. In many cases government is the leader in deployment of cloud computing model across the wide economy [1]. The government contains general data and information for citizens but it also contains critical data which needs high security.

Fig 1 Cloud computing

Information System and Security:

Information System: – The system which processes the data to produce some result in human understandable form is called the information system. Information system connects the computer and user by producing information in some meaningful form. Information system processes data as per the requirement of user and produces required result in the form of information. Information systems are used to capture, create, store, process or distribute classified information with the help of information and communication technology (ICT).

[2] Tools & Technology

Authentication Attacks In Cloud

Research studies reveal that any authentication mechanism related to web applications & cloud should provide high security, easy to use interface & support user mobility. Customers prefer to access their applications from different locations & different devices such as desktop, laptop, PDA, smart phones, cell phones etc. Those needs pose significant requirements to security of applications. broad range of user requirements introduces wide range of attack vectors in cloud that makes security of cloud applications a thought provoking

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

matter. Cloud service providers want to ensure that only legitimate user are accessing their services & this points out to requirement of a strong user authentication mechanism. But there exists numerous attacks that could create loop holes in authentication mechanism & hence identifying most secure authentication mechanism within high user acceptability is a big challenge in cloud environment. Thus an in-depth idea of attacks on authenticity & corresponding prevention techniques are required to draft a fool proof authentication mechanism for cloud environment.

.

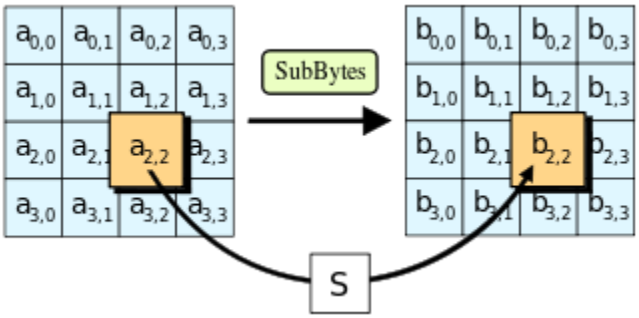

Fig 2 In SubBytes step, each byte in state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

The ShiftRows step

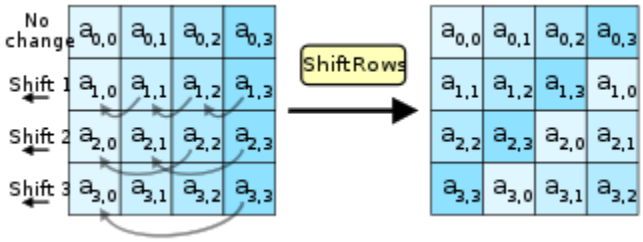

Fig 3 In ShiftRows step, bytes in each row of state are shifted cyclically to left. number of places each byte is shifted differs for each row.

The MixColumns step

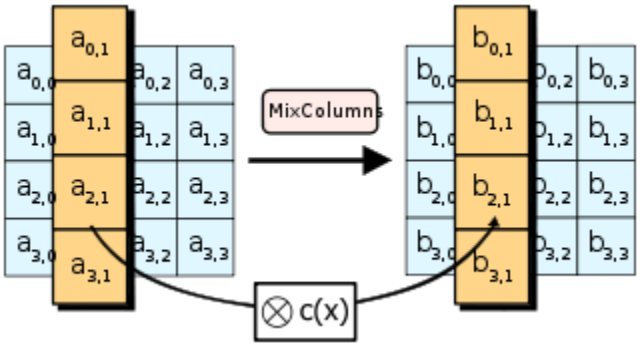

Fig 4 In MixColumns step, each column of state is multiplied with a fixed polynomial $c(x)$.

[3] Proposed Work

Security is becoming an escalating concern in an increasingly multimedia defined world. recent emergence of embedded multimedia applications such as mobile-TV, video messaging, & telemedicine have increased impact of multimedia & its security on our personal lives. For example, a significant increase in application of distributed video surveillance technology to monitor traffic & public places has raised concerns regarding privacy & security of targeted subjects.

Multimedia content encryption has attracted more & more researchers & engineers owing to challenging nature of problem & its interdisciplinary nature in light of challenges faced with requirements of multimedia communications, multimedia retrieval, multimedia compression & hardware resource usage.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

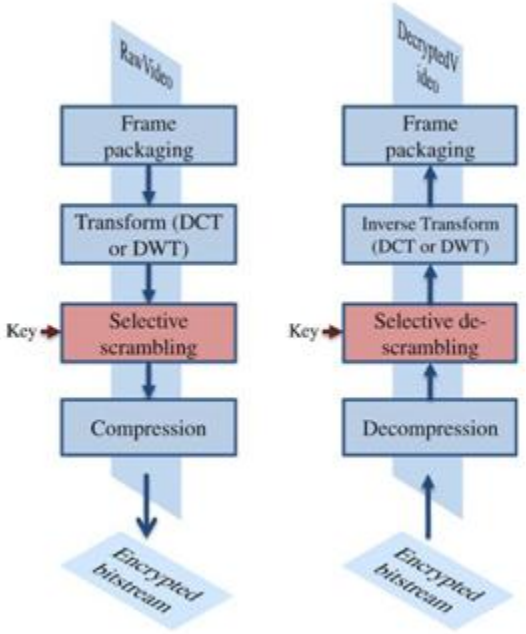

Fig 5 Joint scrambling **&** compression framework

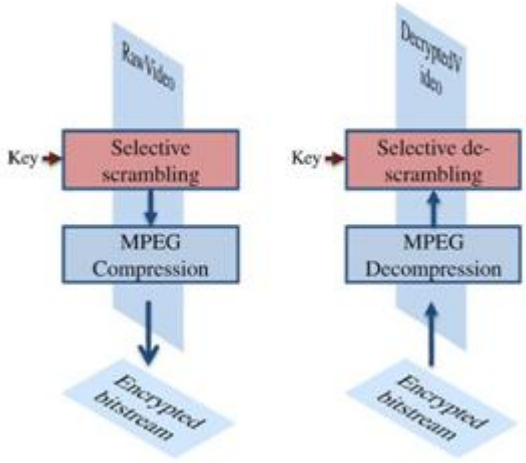

Fig 6 Pre-compression encryption scheme proposed by Pazarci & Diplin. scrambler allows unauthorized user to have an arbitrarily degraded view of program, yet is totally transparent to MPEG-2 compres

[4] Implementation

In order to simulate encryption & decryption of multimedia file we need following:

Data Analysis work

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

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

Table 1 Data in case of Fiber optics

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

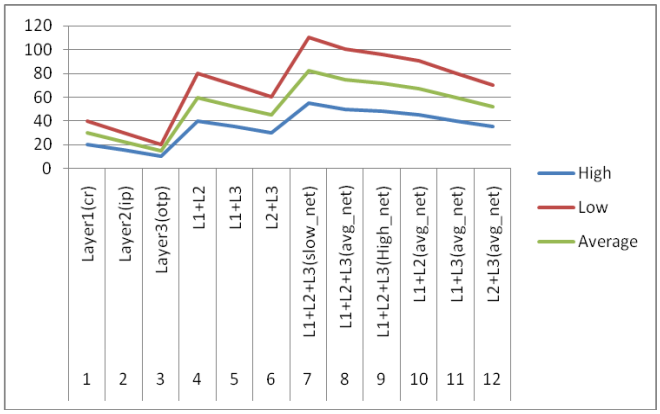

Fig 7 Analysis of transmission speed of packet in case of Fiber optics

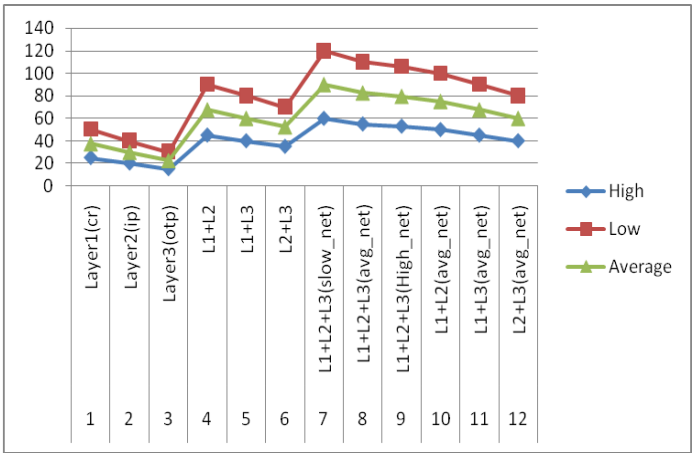

Fig 8 Analysis of transmission speed of packet in

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

Table 2 Data in case of Coaxial 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

Table 3 Data in case of Twisted Cable

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

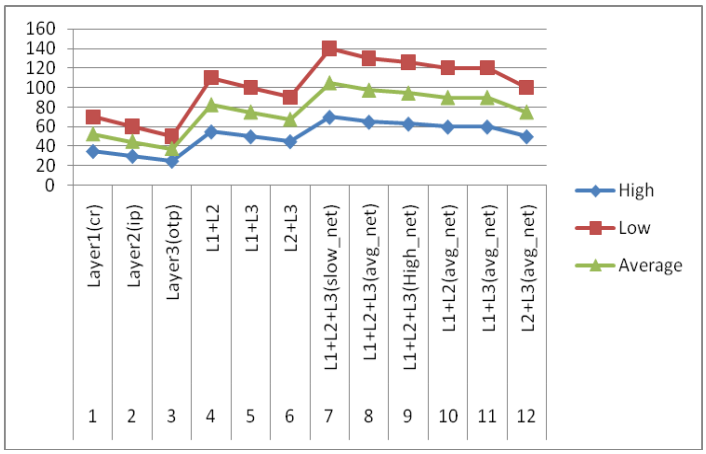

Fig 9 Analysis of transmission speed of packet in case of Wireless network

[5] Future Scope

The main idea behind research is to integrate encryption into compression operation by parameterization of compression blocks, & (in general) not modifying compressed bits. Two main compression blocks where these techniques had been applied are Wavelet Transform & Entropy Coding.

Encryption into a single operation makes it feasible for cloud servers, mobile & embedded devices to ensure multimedia security within their low power budgets. By integrating compression & encryption operations into one these approaches reduce latency of encryption operation which is useful for real-time video delivery. Our research typically do not change compressed bit streams themselves but change way compressed bitstream is obtained. This integration allows exploiting hierarchical signal representation in a transform domain, as used by most image & video compression techniques, in order to provide advanced functionalities required by many modern applications.

[6] Conclusion

Providing security for many Multimedia applications like Video on-Demand service, broadcasting a video, video-conferencing and multimedia mails is must. A secured video transmission ensures the user such that no unapproved eavesdroppers can get the information from the video while it's being sent to receiver i.e. the users those who paid for these services can only watch the videos and movies. If the video is more redundant it helps the attacker to easily rebuild the original video file. Data such as text and program code has less redundancy when compared to videos in its structure. All these factors make providing security for a MPEG video more challenging. Providing security for these MPEG video transmission involves in encrypting parts of the MPEG bit stream or the entire bit stream.

[7] References

1. Agi, I., Gong, L.: An empirical study of secure mpeg video transmissions. In: Proceedings of the Symposium on Network and Distributed System Security, pp. 137–144. IEEE Press, New York (1996)

2. Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K.: The secure real-time trans-port protocol (SRTP) (2004)

3. Bergeron, C., Lamy-Bergot, C.: Complaint selective encryption for h.264/avc video streams. In: IEEE 7th Workshop on Multimedia Signal Processing, pp. 1–4 (2005). doi: 10.1109/ MMSP.2005.248641

4. Cheng, H., Li, X.: Partial encryption of compressed images and videos. IEEE Trans. Signal Process. **48**(8), 2439–2451 (2000). doi: 10.1109/78.852023

5. Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., Reginelli, M.: A new chaotic algorithm for video encryption. IEEE Trans. Consum. Electron. **48**(4), 838–844 (2002)

6. Li, S., Zheng, X., Mou, X., Cai, Y.: Chaotic encryption scheme for real-time digital video. In: Real-Time Imaging VI. Proceedings of SPIE, vol. 4666, pp. 149–

160 (2002)

7. Lian, S., Liu, Z., Ren, Z., Wang, H.: Secure advanced video coding based on selective encryp-tion algorithms. IEEE Trans. Consum. Electron. **52**(2), 621–629 (2006)

8. Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. **17**(6), 774–778 (2007)
9. Logik Bomb: Hacker's Encyclopedia (1997)
10. Hafner, Katie; Markoff, John (1991). Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster. ISBN 0-671-68322-5.
11. Sterling, Bruce (1992). The Hacker Crackdown. Bantam. ISBN 0-553-08058-X.
12. Slatalla, Michelle; Joshua Quittner (1995). Masters of Deception: The Gang That Ruled Cyberspace. HarperCollins. ISBN 0-06-017030-1.
13. Dreyfus, Suelette (1997). Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier. Mandarin. ISBN 1-86330-595-5.
14. Verton, Dan (2002). The Hacker Diaries : Confessions of Teenage Hackers. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.
15. Thomas, Douglas (2002). Hacker Culture. University of Minnesota Press. ISBN 0-8166-3345-2.

16. Taylor, Paul A. (1999). Hackers: Crime in the Digital Sublime. Routledge. ISBN 978-0-415-18072-

17. Levy, Steven (2002). Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin. ISBN 0-14-024432-8.

18. Ventre, Daniel (2009). Information Warfare. Wiley - ISTE. ISBN 978-1-84821-094-3.

19. Bhushan Lal Sahu,Rajesh Tiwari, Journal of Advanced Research in Computer Science and Software Engineering 2(9) (2012) 33-37.

20. Peter Mell, Tim Grance (2011). The NIST Definition of Cloud Computing, the National Institute of Standards and Technology Report. 2011.

21. Sultan Ullah, Zheng Xuefeng (2013). Cloud Computing Research Challenges. IEEE 5th International Conference on Biomedical Engineering and Informatics, pp 1397-1401.

22. Tripathi A., Mishra A. (2011). Cloud Computing Security Considerations. Signal Processing, Communications and Computing (ICSPCC), IEEE International Conference.

23. Mohammad Reza Modarres Zadeh, International Letters of Social and Humanistic Sciences 3 (2013) 21