© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 08 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Enhancement Of Multimedia Security In Cloud Computing

[1]Chanky Swami , Research Scholar, Department of CSE, CBS Group of Institutions, Jhajjar
[2]Nishant Anand, H.O.D, Department of CSE, CBS Group of Institutions, Jhajjar

ABSTRACT: Information is most vital piece of cloud services so gigantic concern ought to be given to its security. A few malicious persons can utilize Cloud computing for unlawful and criminal and active use of cloud for illicit intentions is called cloud ill-use. The biggest need is to maintain, manage information resources in digital format and made resource sharable for multiple access. Every organization is building its resources either by digitizing documents or by entering new data in digital form. Digital resources available are maintained and are being shared frequently over Cloud Network. Cloud Server is giving importance to its digital collections of multimedia data. Multimedia data are becoming main source of information in a library and preferred mode of acquisition for collection development. digital materials are not secure on network by its nature. There is risk of unauthorized use of these materials. Maximum efforts are made to create digital contents whereas less attention is given to its security and security threats are in many forms.

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

[1]Introduction

Security issues in Cloud

Security is a standout amongst most concerning issue of Information engineering Issue. To keep authoritative or client information is essential concern. In event that association's information is not protected on cloud then there is no utilization of moving from old discovery to cloud engineering. There are parcel of Non-Profit Organization which are helping & making mindfulness about security problem of Cloud computing. One of such association is Cloud Security Alliance that distribute a report in each year in regards to most famous security issues in Cloud computing. In 2013 CSA reports they are well know eight famous security dangers to cloud which could mischief client's individual information without knowing them.

Video as Multimedia

Video format consists of different technology concept: one is containers & another is codec. Containers are sometimes called as wrappers. Container basically describes structure of file: where various pieces are stored, how they are interleaved & which codec are used by which pieces. It may specify an audio codec as well as video. It is used to package video & its components & is identified by a file extension such as .AVI, .MP4 etc. A codec is a way of encoding audio or video into a stream of bytes such as MPEG1, H.264 etc. It is method used to encode video & is chief determiner of quality. A multimedia video file comes in various formats, each of them possess a level of popularity based on several specifications. Based on availability & usage, most popular types of multimedia video formats are Joint Photographic Expert Group (JPEG), Audio Video Interleave (AVI) & Moving Pictures Expert Group (MPEG). Mobile devices & online streaming services often use Flash video (FLV), Windows Media Video (WMV), & 3rd Generation Partnership Project (3GP). Other common multimedia video formats include QuickTime Movie (MOV), Matroska (MKV), & RealMedia® (RM). DivX® & OGG are also popular among users.

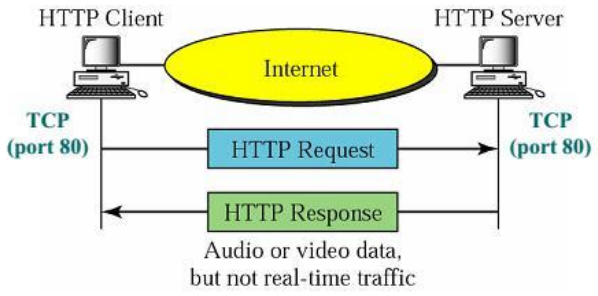

Figure 1. Non-Real Time Video Streaming (Video- on Demand)

[2] Literature review

***Rahat Afreen and S.C. Mehrotra* (2011)**

This paper deals with cryptography that makes use of

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 08 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

the public key also called as the PKC systems in short. In systems pertaining to PKC , two keys that are entirely different are utilized for encoding and decoding the data. The strength and security depends on large key size as among the two keys one is distributed and kept open to the public in PKC systems . Previously in PKC systems the mathematical problems of prime factorization and discrete logarithm are used. The security with a almost euql to the above with relatively small sizes of the key has been promised by ECC and it has been proved. The ECC implementation on application specific systems is the main point focused in the field of research. The requirement of separate crypto coprocessor can be reduced by doing a research in the category of ECC mainly related to present various combinations of speed optimized algorithms. Various mathematical techniques are considered to enhance the speed and security of ECC. [116]

***Paul Kocher, Ruby Lee, Gary McGraw , Anand Raghunathan and Srivaths Ravi* (2004)**

In this paper the security aspect of embedded has been discussed in detail. A case study that takes into account the efforts that is needed for securing the electronic systems has been created with the increasing cases where the data from systems concerned with embedded are being hacked and destroyed leading to huge loss in the last few year. Systems in the embedded world that are dedicatedly and specifically utilized to capture the data and then storing it and accessing it when required keeping its security sensitivity do possess a large security and other challenges in providing the full security to the data.

[3] 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 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.

.

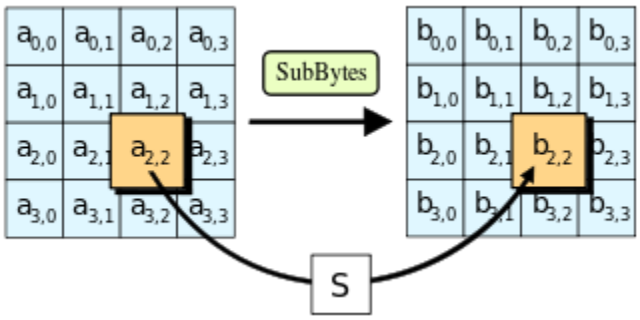

Fig 2 In SubBytes step, each byte in state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

The ShiftRows step

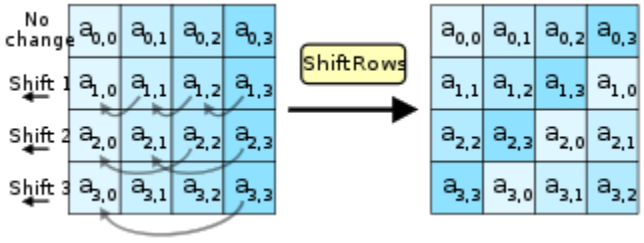

Fig 3 In ShiftRows step, bytes in each row of state are shifted cyclically to left. number of places each byte is shifted differs for each row.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 08 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

The MixColumns step

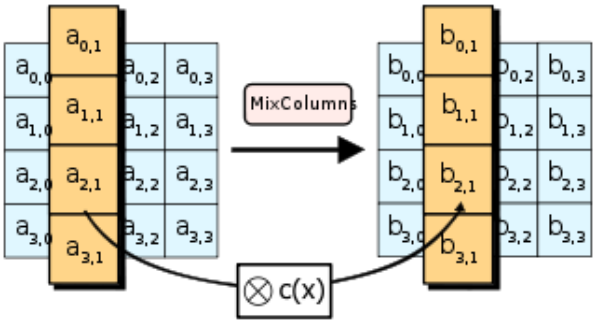

Fig 4 In MixColumns step, each column of state is multiplied with a fixed polynomial *c(x)*.

[4] Proposed Implementation

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.

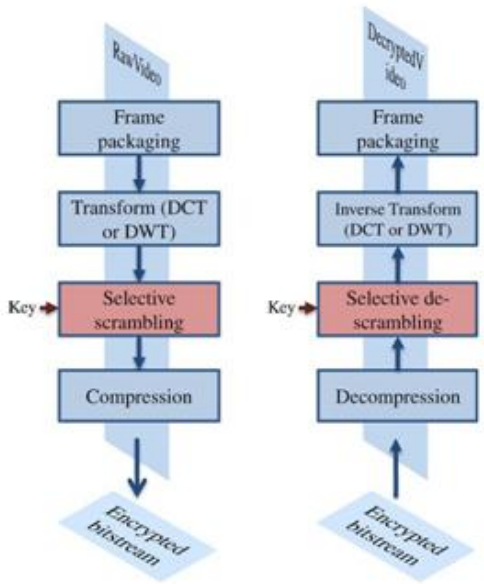

Fig 5 Joint scrambling **&** compression framework

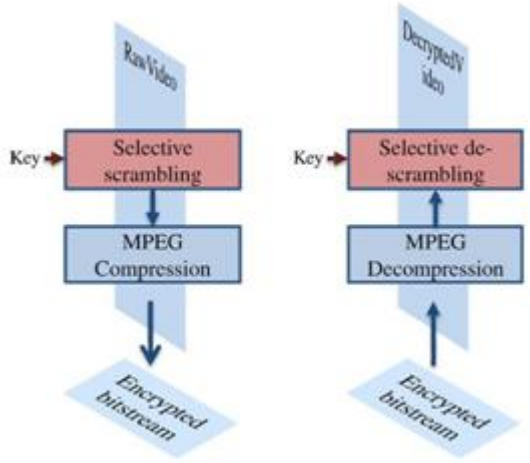

Fig 6 Pre-compression encryption scheme proposed by Pazarci & Diplin. scrambler allows unauthorized user to have an arbitrarily degraded view of program, yet is totally transparent to MPEG-2 compres

[5] Implementation

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

Hardware Requirements

- CPU (1GHZ or above)
- RAM(1 GB OR MORE)
- 5GB FREE SPACE IN HARDDISK
- HIGH RESOLUTION MONITOR

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

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 08 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

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

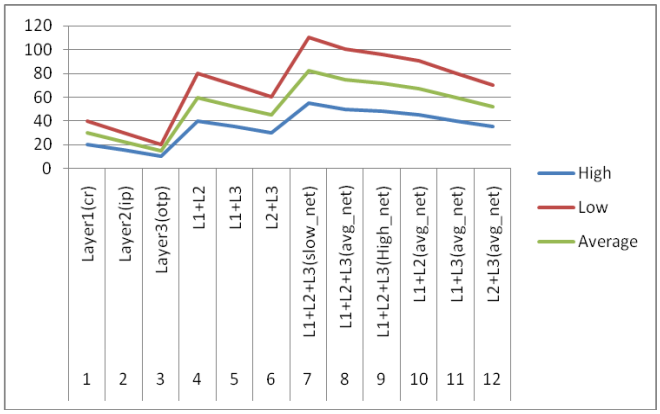

Fig 7 Analysis of transmission speed of packet in case of Fiber optics

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

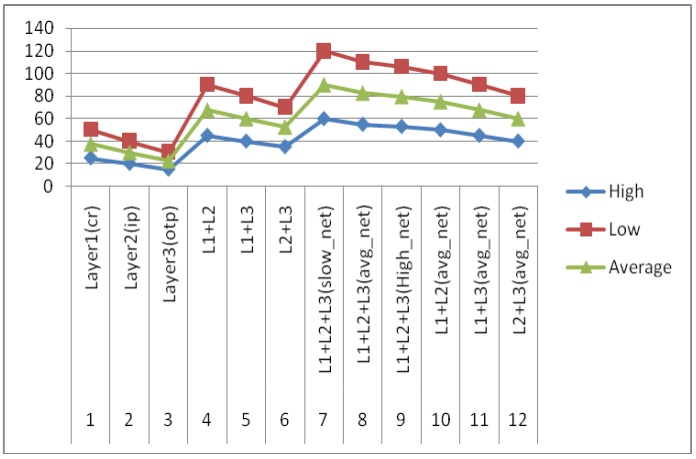

Fig 8 Analysis of transmission speed of packet in

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

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 08 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

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

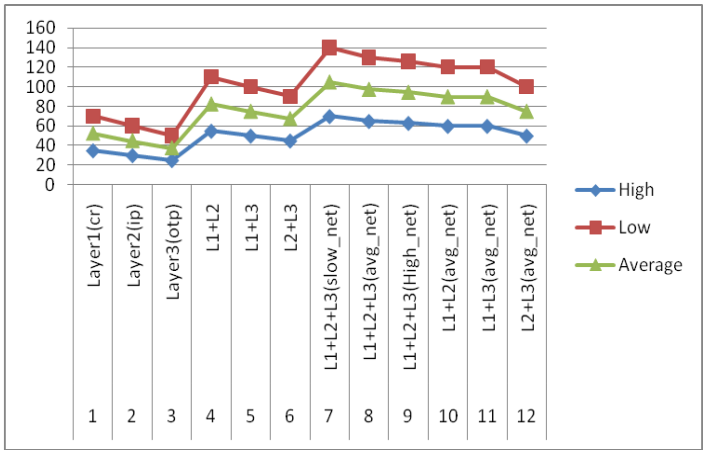

Fig 9 Analysis of transmission speed of packet in case of Wireless network

[6] Conclusion

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.

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