© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Implementation On Cloud Server Security Using Password Authenticated Key Exchange

[1]Payal Rani, Research Scholar, Department of CSA, CDLU Sirsa
[2]Monika Bansal, Assistant Professor, Deptt. Of CSA ,CDLU ,Sirsa

ABSTRACT: Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These new innovative, technical and pricing opportunities bring changes in the way business operated. Cloud computing is the matchless computing technology. Cloud computing is a new label to an old idea. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing makes possible for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. General example of cloud services are Google Engine, Oracle Cloud, Office 365. As the cloud computing is growing rapidly this also leads to severe security concerns. Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users and providers.

[1] INRODUCTION

NETWORK SECURITY THREATS

Categories of attack could consist of passive monitoring of data communications exploitation by insiders, close-in attacks, harmful attacks through service provider & active network attacks. Information systems & networks usually offer targets & must be resistant with in order to attack from full range of threat agents, from hackers to nation-states. system must be capable to restrict damage & recovery from occurrence of attacks.

TYPES OF ATTACK

Five types of attacks are as follow:

1. **Passive Attack**
2. **Active Attack**
3. **Distributed Attack**
4. **Insider Attack**
5. **Close in Attack**

Passive Attack

A **passive attack generally** checks data which has been not converted traffic & would checks for sensitive information & clear-text passwords which could be used with in different types of attacks.

Active Attack

In **active attack** attacker generally attempts to crack or breakdown into secured systems. This could be performed through worms/viruses/stealth/Trojan horses.

Distributed Attack

A **distributed attack** would require opposition introduced code, such as back-door program or Trojan horse attacks, to trusted component or software which are later be distributed to several other client companies & users.

Insider Attack

An **insider attack** includes somebody from inside, such as discontented operative, attacking on network that generate Insider harmful attacks may be spiteful or not spiteful. Malicious insiders intentionally steal, eavesdrop or damage confidential or valuable data;

Close-in Attack

The **close-in attack** includes somebody attempting to get physically/connected close to network data, components & systems within order to learn more about network Close-in harmful attacks consist of regular checking of individuals attaining close physical proximity to networks, systems, or

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

facilities for purpose of altering, denying access to information or gathering.

HACKING

A **hacker** has been somebody who exploits & seek weaknesses within computer network or computer system. hacker can be motivated by multitude of reasons, such as profit, challenge or protest. grouping that has evolved everywhere hackers has been often referred to as computer underground & these days they are well known community.

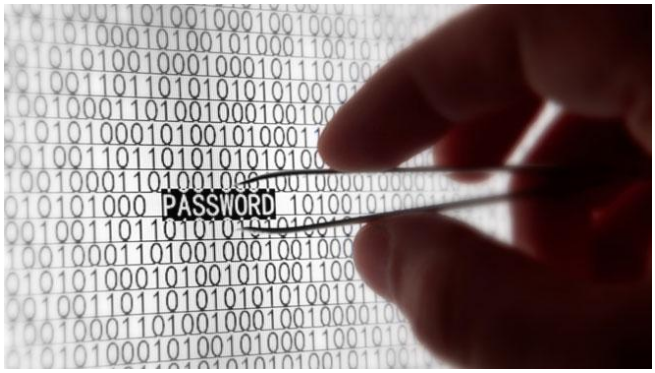

Fig 1 Password cracker

Fig 2 Threats to Data Security

[2] **LITERATURE REVIEW**

Research Titled "**ENHANCEMENT OF SECURITY USING CRYPTOGRAPHIC TECHNIQUES**" published by Natasha Saini, Nitin Pandey & Ajeet Pal Singh focus on various types of security issues which include confidentiality, integrity & availability of data.There exists various threats to security issues traffic analysis, snooping, spoofing, denial of service attack etc. asymmetric key encryption techniques may provide higher level of security but compared to symmetric key encryption Although they have existing techniques symmetric & assymetric key cryptography methods but there exists security concerns.

Raghav Mathur, Vishnu Sharma ans Shruti Agarwal published their research titled "**Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey**" in which they talk about advancements in wireless networking have been initiated idea of mobile computing, where user does not have to be bound to fixed physical location in order to exchange any data benefits of on-the-move connectivity are several but there exist serious networking & security issues that need to be solved before realizing full benefits of mobile computing

"**A Modified RSA Algorithm to Enhance Security for Digital Signature**" was research paper published by "Sangita A. Jaju, & Santosh S. Chowhan in which they talk about digital signature been providing security services to secure electronic transaction over internet. Rivest, Shamir & Adlemen (RSA) algorithm was most widely used to provide security technique. Here they have modified RSA algorithm to enhance its level of security.

"**Wireless Network Security Using Dynamic Rule Generation of Firewall**" published by Bhushan Chaudhari, Prathmesh Gothankar, Abhishek Iyer & D. D. Ambawade describe wireless computing has evolved tremendously & is being used almost everywhere these days. With the obvious advantage of mobility & easy installation, it also provides service comparable to its wired counterpart.

[3] TOOLS & TECHNOLOGY

In United States, AES was announced by NIST as U.S. FIPS PUB 197 on November 26, 2001. Announcement followed five-year standardization process in which fifteen competing designs were presented & evaluated, before Rijndael cipher was selected as most suitable.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

AES became effective as federal government standard on May 26, 2002 after approval by Secretary of Commerce. AES has been included in ISO/IEC 18033-3 standard. AES has been available in several different encryption packages, & has been first publicly accessible cipher approved by National Security Agency for top secret data when used in NSA approved cryptographic module.

AES has been based on design principle considered as substitution-permutation network, combination of both substitution & permutation, & has been fast in both software & hardware. Unlike its predecessor DES, AES does not use Feistel network. AES has been variant of Rijndael which has fixed block size of 128 bits, & key size of 128, 192, or 256 bits. By contrast, Rijndael specification *per se* has been specified with block & key sizes that may be any multiple of 32 bits, both with minimum of 128 & maximum of 256 bits.

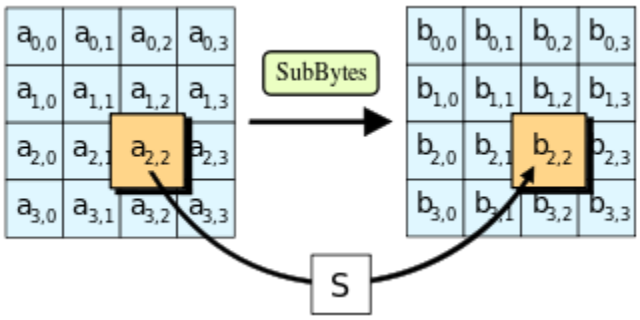

Fig 3 In SubBytes step, each byte in state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

The ShiftRows step

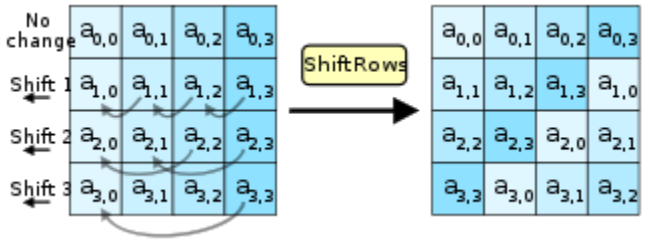

Fig 4 In ShiftRows step, bytes in each row of state are shifted cyclically to left. number of places each byte is shifted differs for each row.

The MixColumns step

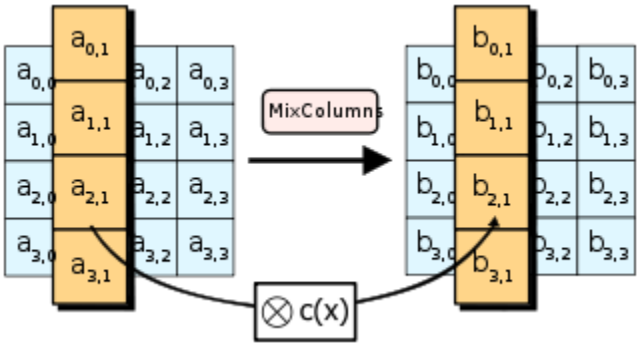

Fig 5 In MixColumns step, each column of state is multiplied with a fixed polynomial $c(x)$.

[4] PROPOSED IMPLEMENTATION

CHALLENGES TO EXISTING NETWORK SECURITY

Much of theoretical work within cryptography is to cryptographic primitive algorithms with basic cryptographic properties & their relationship to other cryptographic problems. More complex cryptographic tools are then built from these basic primitives. Such primitives provide fundamental properties which are used in development of more complex tools called cryptosystems or cryptographic protocols that guarantee high-level security properties. Note however, that distinction between cryptographic primitives & cryptosystems, has been quite arbitrary; for example, RSA algorithm has been sometimes considered cryptosystem, & sometimes primitive. Eg. of cryptographic primitives consists pseudorandom functions, one-way functions, etc.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

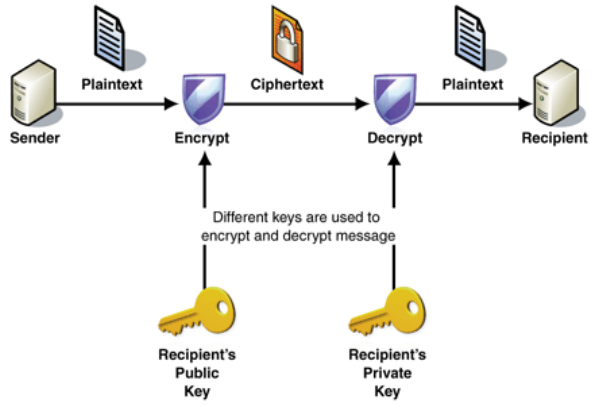

Fig 6 Encryption & decryption

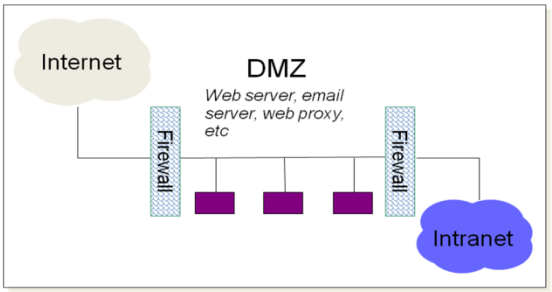

Fig 7 Firewall within internet & Intranet

[5] **Result and Discussion**

Simulation Environment

The following environment was taken to simulate the proposed protocol.

Hardware used:

- Processor : Intel(R) Core (TM) above 1 Ghz
- RAM : 1.00 GB or above
- System Type : 32/64 bit operating System
- Harddisk : 1 GB free space

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

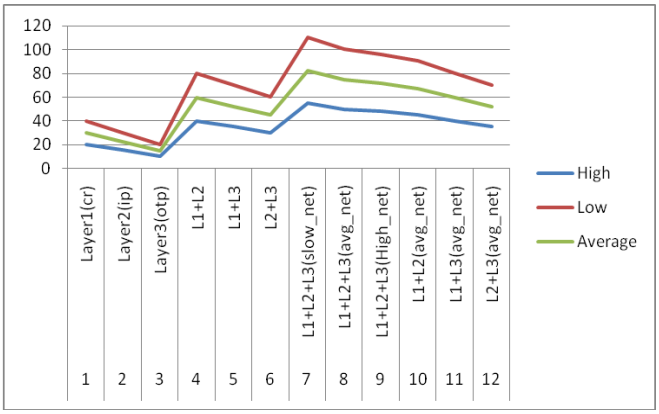

Fig 8 Analysis of transmission speed of packet in case of Fiber optics

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.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

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

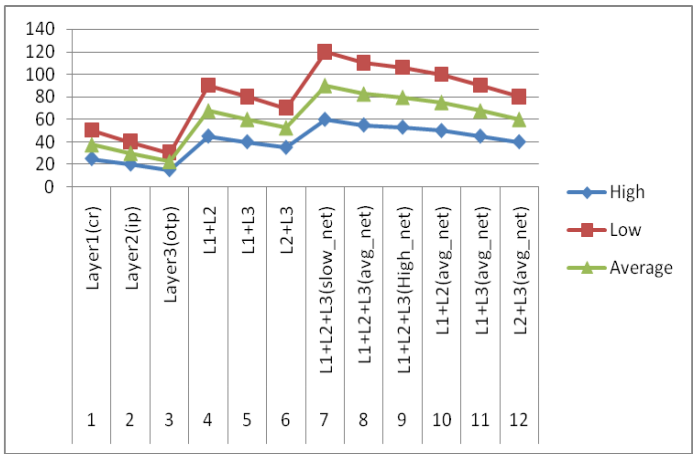

Fig 9 Analysis of transmission speed of packet in

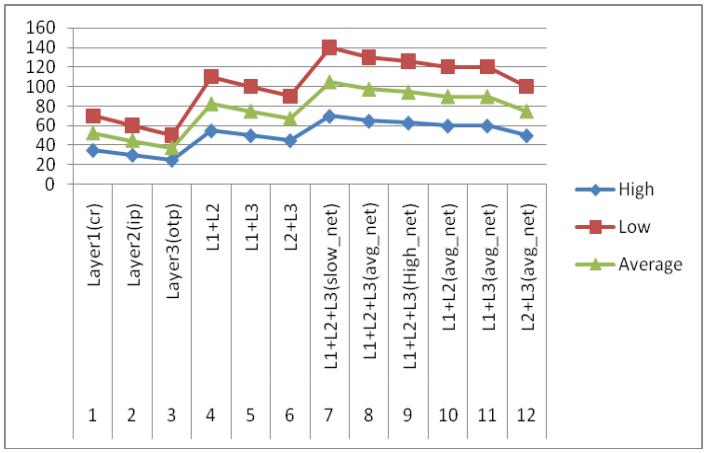

Fig 10 Analysis of transmission speed of packet in case of Wireless network

Sno	Security_Level	H	L	Avg

[6] CONCLUSION

AD HOC Networking has been still evolving but its benefits are enormous. AD HOC Networking provides excellent support for amazing infrastructures, applications & services such as shared resource pool, broad network base, reduced this cost or rapid elasticity of network to handle varying customers demands as well as AD Hoc network computing various service & deployment models that has been part of main reason for adopting this computing system. Thus this makes network computing open shared system volatile to security breaches & other challenges.

So there has been need to focus on solutions of various challenges to maintain dependence level of organization for deploying AD HOC networking without any hesitation & also need of technical support for elastic scalability to serve ever pressing demand of customer.

REFERENCES

[1] David Pointcheval, Olivier Blazy, New Smooth Projective Hash Functions & One-Round Authenticated Key Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice & Theory within Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, Password-based Authenticated Key Exchange. (21-23 may 2012, Darmstadt, Gerseveral)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, Strong Cryptography from Weak Secrets, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, Distributed Public-Key Cryptography from Weak Secrets, (18_20 march 2009, Irvine, CA, USA), S. Jarecki & G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

[8] David Pointcheval, Michel Abdalla, Password-Authenticated Group Key Agreement with Adaptive Security & Contributiveness, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, Analysis & design of secure key exchange scheme, Information Sciences 179 (2009) , Elsevier

[10] Research Titled "**ENHANCEMENT OF SECURITY USING CRYPTOGRAPHIC TECHNIQUES**" published by Natasha Saini, Nitin Pandey & Ajeet Pal Singh

[11] Raghav Mathur, Vishnu Sharma ans Shruti Agarwal published their research titled "**Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey**"

[12] "**A Modified RSA Algorithm to Enhance Security for Digital Signature**" was research paper published by "Sangita A. Jaju, & Santosh S. Chowhan

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in