IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN EFFECTIVE AND SECURED TECHNIQUE FOR SIDE-CHANNEL ATTACKS IN CLOUD

Adi Maheswara Reddy G [1], Dr K Venkata Rao[2], Dr JVR Murthy[3]
Research Scholar, Department of CSE, JNTUK, Kakinada, AP, INDIA [1]
Department of CSE, Vignan Institute of Information Technology
Visakhapatnam, AP, INDIA [2]
Department of CSE, JNTUK College of Engineering, Kakinada, AP, INDIA [3]

DOI: 10.5281/zenodo.1049426

ABSTRACT

Nowadays in cloud based business services have risks of side channel attacks. Cache-based side channel attack, cross-VM side channel attacks are the serious threat and security pitfall under same cloud network services. In order to provide more security and less infrastructure investment leads to challenging task. In this paper, the discussions on various levels of attacks on VM ware based solution under same cloud network computing, vulnerabilities to other cloud services, security weakness and counter measures in cryptographic algorithms.

Key words: Cloud computing · Virtualization · Security · Privacy · Vulnerabilities, Side-channel assault, cross-VM side channel, store based side channel assault.

I. INTRODUCTION

The advanced virtualization technologies such as HyperV, Xen, and Virtual machine Wares are fast growing basis for the critical cloud services platforms. In these technologies major attacks such as Cache-based side channel attack, cross-VM side channel attack leads more vulnerable in cloud attacks [1].

In Cloud environment servers are generally in charge of keeping up document records of the cloud customer clients and furthermore to provide a few administrations like PaaS, IaaS and SaaS administrations. It is regularly eminent that the web correspondence is shaky against the assailant [2, 18, and 24]. In this manner, keeping up client protection, privacy, confirmation alongside client mystery are the real security issues in cloud framework. In order to avoid attacks such as Cache-based side channel attack, cross-VM side channel attack leads more vulnerable in cloud attacks researchers employ efficient cryptographic algorithms one-way hash function, elliptic curves RSA algorithm cryptosystem, and some others security methods [3,19,22]. Despite the fact that the elliptic bends and RSA calculation both cryptosystem give same level of security at cross-VM products, elliptic bends is more reasonable than RSA calculation, in light of the fact that elliptic bends utilizes just point increase operation and the key length is 160 bits, while RSA calculation utilizes exponentiation operation, which takes particularly longer calculation than elliptic bends point duplication and the key length of the RSA calculation is 1024 bits, which is bigger than ECC elliptic bends [4,20,21, 23].

II. REVIEW OF SIDE CHANNEL ATTACKS

Amittai Aviram et al. [5] proposed an approach “provider-enforced deterministic execution” for timing channel control by using resource partitioning which eliminates timing channels within a shared cloud domain. Therefore approach is removes the exploitability of *all* timing channels in the cloud. **Yinqian Zhang** et al. [6] present a novel framework for conducting cache-based side-channel attacks and explains the attacks between users the Platform-as-a-Service clouds. In their study of **RSA** cryptosystem, the private-key decryption which enables the classic Bleichen-bacher padding-oracle attack even though more secure measures are deployed for countermeasures against the cloud channels.

Yinqian Zhang et al. [7] brought up the development of an entrance driven side-channel assault by which a helpless VM separates access of VM running on the same physical PC. The creators address the setting by removing an ElGamal decoding key from a casualty utilizing the latest cryptographic library. Here the assault that was satisfactorily intense to remove ElGamal unscrambling keys from a cloud client's VM. Olivier Heen et al. [8] proposed a new “Gateway-based de-duplication” model that allows the cloud storage service provider to relate efficient de-duplication by considerably reducing the threat of information leakage. Also proposed a way for in which that cloud storage system supports I*nter-account* de-duplication by significantly reducing the information leak in which it employs de-duplication in side-channel for cloud VM data.

Thereafter Bhrugu Sevak et al. [9] also introduces how to refrain from the side channel attack in cloud computing. This is authors proposes the combination of Virtual firewall appliance and randomly encryption decryption for effective reliability, availability, and security of cloud user data. It is analyzed that it is good idea to provide security against side channel attack using virtual firewall apps and arbitrarily used encryption decryption in the cloud.

In the year 2015 and 2016 Fangfei Liu et al. [10,11] proposed the feasibility of high-bandwidth with low noise side channel attacks on the last-level cache (LLC), pointed out the countermeasure called CATalyst. CATalyst is a lightweight system mechanism for the cloud provider and cloud customers to protect vulnerable LLC-based side channel attacks. Also presents an implementation of the PRIME PROBE side-channel attack against the last level cache.

In 2012 Md. Tanzim Khorshed et al. [12] demonstrated that the cutting edge machine learning systems as the center to include as a vast database by considering the best dangers. Different VM instruments are connected to confirm the model assault conjecture capacity. The Support Vector Machine (SVM) is a notable measurable machine learning hypothesis to distinguish the best assaults with a most extreme exactness. Also Helmut Hlavacs et al. [13] presents the energy/power consumption logs of power side channels of monitored servers, which uses to recognize the exact combination of virtual machines. Taesoo Kim et al. [14] examines and showed side channel assaults through the common memory reserves to break full encryption keys of AES, DES, and RSA. Likewise introduces STEALTHMEM, a "framework level security instrument" against reserve based side divert assaults in the cloud.

In 2013 and 2014 Michael Godfrey et al. [15], are addressed the problems of sequential side-channels, and parallel side-channels. These techniques are based on the internal hypervisor of a Cloud system no including the cloud methods of operation. Also they are investigated the current state of side-channel threats of CPU cache based defenses in a Cloud environment.

III. PRELIMINARIES

3.1 Attacker model:

As the side channel is executed over the unreliable VM stations, the trespasser uses diverse preferences and capacities through the shaky channels of created convention.
In this section, the authors assumed some widely accepted valid assumptions.
a. The side-channel attack is able to extract the cloud information by monitoring the VM configuration
b. In side-channel attack, the memory leak may affect all the cloud storage entities among the cloud users.
c. In VM channels the aggressor can figure low entropy watchword and effortlessly however speculating two mystery parameters.
d. The side-channel assault can adjust, erase and resend, reroute the spy message.

3.2 Road map of the paper

The authors have displayed worthy presentation in segment "Presentation". At that point address the Yinqian Zhang et al's. Convention in segment "Brief survey of Yinqian Zhang et al. convention", whose security shortcomings shows up in segment “Security weaknesses of Yinqian Zhang et al. protocol”. After that proposed the enhanced convention in segment proposed "an enhanced preventive system for side channel assault". The familiar cryptanalysis using SAPN-AVISPA has been presented in section “Security analysis of the proposed protocol”. At last, in the paper as "Conclusion and further investigation" and future investigations of the paper with related references.

3.3 Brief review of Yinqian Zhang et al. protocol

In this segment, the audit of Yinqian Zhang et al. [3, 7] RSA based client confirmation and VM security convention for cloud framework. This convention surveyed in the following areas as VM-product instatement stage, VM-enlistment stage, VM-product login stage, VM-product verification and VM-product session key assertion stage.

3.3.1 VM-ware initialization phase

To initialize the VM-ware system, the cloud server S chooses two large prime numbers p, q and computes n, p, and q. The VM-ware server S then keeps p and q secret and publishes n as public.

3.3.2 VM-ware registration phase

In registration phase the cloud user simply registers and stores the vial information and accesses the various cloud enabled services using VM machine.

3.3.3 VM-ware login phase

During VM-ware services, user utilizes his service to the terminal or by weak identity ID_i and password pw_i. The VM-product cloud checks whether the registered ID_i is measures up to with the separate existed ID_i. On the off chance that ID_i does not holds, at that point VM-product station stops the session generally, continues to following stage.

3.3.4 VM-ware authentication and VM-ware session key agreement phase

Here VM-product confirmation by RSA should be possible by irregular extensive prime numbers p and q of practically break even with length. Figure VM-cloud registers their item n = pq. The capacity ϕ (n) is processed as $\phi(n) = (p - 1)(q - 1)$. After that it two keys a and b with the end goal that, $a.b \equiv 1 \pmod{\phi(n)}$. Presently the keys say ID_i is made open while the other key SK_i is kept a mystery. At this situation, no more require p, q and ϕ (n). In the event that the VM-product message M, encryption of M is $C = M^a \bmod n$, C is the consequence of figure key. Decoding of C is got by $M' = C^b \bmod n$.

Consider $M' = M^{ab} \bmod n = M^{k\phi(n)+1} \bmod n$ (Since $a.b \equiv 1 \pmod{\phi(n)}$)

Therefore $M' = M.\ M^{k\phi(n)} \bmod n = M \bmod n$ (It can be demonstrated that $x^{\phi}(n) \equiv 1 \pmod{n}$).

3.4 Security weaknesses of Yinqian Zhang et al. protocol

Thus the VM-product cloud key M = M'. Consequently to accomplish the proficient encryption and decoding of cloud certifications utilizing RSA. So the security examination of Yinqian Zhang et al conspire [7] will be broke down in view of the substantial suppositions specified in 3.1.

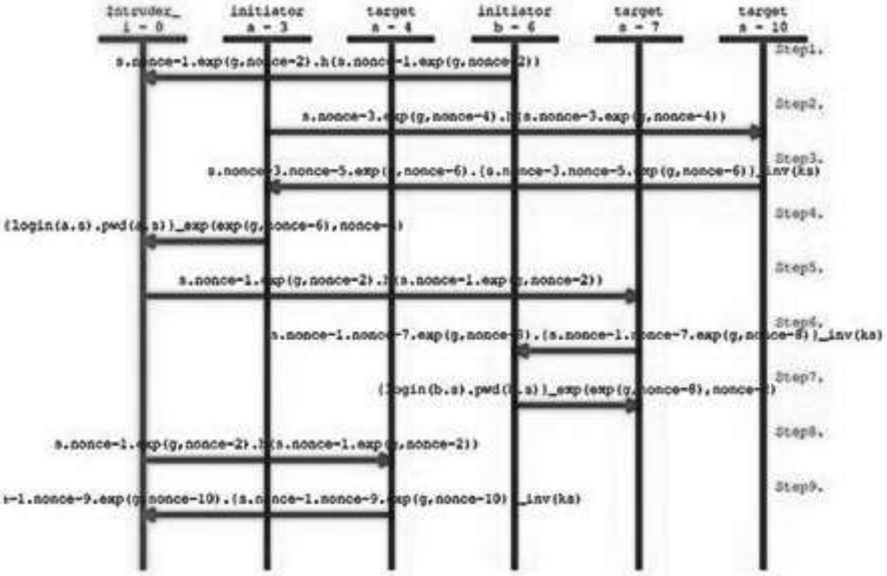

Intruder_
i = 0
initiator
a = 3
target
s = 4
initiator
b = 6
target
s = 7
target
s = 10
Step1.
s.nonce-1.exp(g,nonce-2).h(s.nonce-1.exp(g,nonce-2))
Step2.
s.nonce-3.exp(g,nonce-4).h(s.nonce-3.exp(g,nonce-4))
Step3.
s.nonce-3.nonce-5.exp(g,nonce-6).{s.nonce-3.nonce-5.exp(g,nonce-6)}_inv(ks)
Step4.
{login(a,s).pwd(a,s)}_exp(exp(g,nonce-6),nonce-5)
Step5.
s.nonce-1.exp(g,nonce-2).h(s.nonce-1.exp(g,nonce-2))
Step6.
s.nonce-1.nonce-7.exp(g,nonce-8).{s.nonce-1.nonce-7.exp(g,nonce-8)}_inv(ks)
Step7.
{login(b,s).pwd(b,s)}_exp(exp(g,nonce-8),nonce-2)
Step8.
s.nonce-1.exp(g,nonce-2).h(s.nonce-1.exp(g,nonce-2))
Step9.
s.nonce-1.nonce-9.exp(g,nonce-10).{s.nonce-1.nonce-9.exp(g,nonce-10)}_inv(ks)

Fig 1: An intruder attacker model over side-channel attack.

Here the side-channel attack model in Fig-1 may exists different forms of attacks for example, disconnected watchword speculating assault, favored cloud insider assault, and cloud client namelessness and memory expansion of secret key speculating assault on Zhang et al scheme.

IV. AN IMPROVED PREVENTIVE TECHNIQUE FOR SIDE CHANNEL ATTACK

This area proposes the change of Yinqian Zhang et al conspire. Like Yinqian Zhang et al plan's system, this convention likewise comprise a few periods of side channel assaults.

4.1 Security analysis of the preventive side channel attack

In the section "Presentation", a side-channel assault show introduced which talks about a few generally acknowledged presumptions including capacities of the side-channel assault. In this segment, the authors casually dissected the security for proposed convention in view of the side-channel assault demonstrates portrayal. And formally investigated the reproduction for formal security check utilizing AVISPA device [16]. This segment talks about in regards to the recreation of the master postured enhanced preventive system for side channel assault for the formal security confirmation utilizing the broadly acknowledged AVISPA (Automated Validation of Inter-net Security Protocols and Applications) apparatus. In the demonstration, the proposed convention is secure against aloof and dynamic assaults including the replay and man-in-the-center assaults.

4.1.1 Brief analysis of AVISPA tool

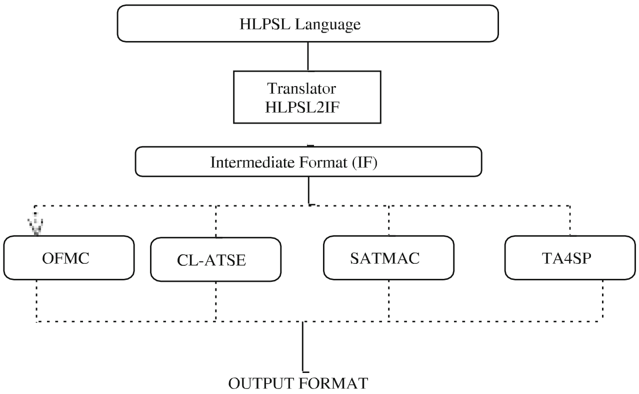


Figure- 2 Architectural hierarchy of HLPSL of the *AVISPA* tool

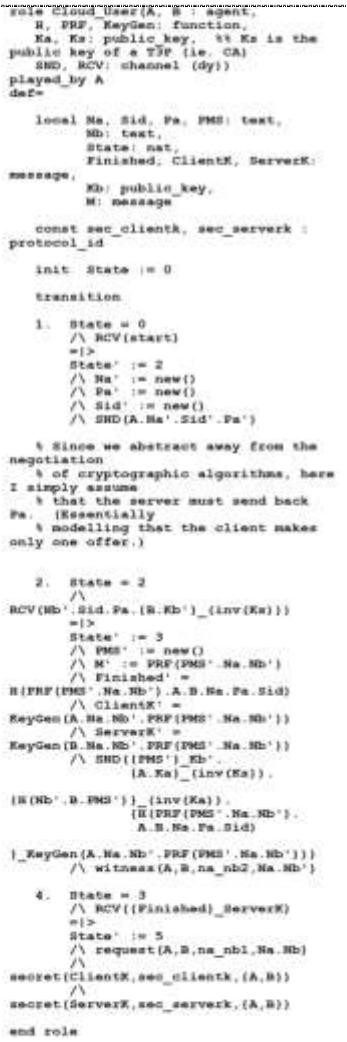
The AVISPA web based internet protocol assessment mechanism is considered as widely accepted too and which it checks the cloud based VM-ware security analysis tool for the High level protocol specification language of formal security verification. Based on the security levels of protocol it witnesses whether protocol is SAFE or UNSAFE and supports, “High Level Protocol Specification Language” called as HLPSL. The structure of the AVISPA tool is shown in Figure. 2. The AVISPA actualizes four diverse back-finishes, for example, On-the-fly Model-Checker (OFMC) which is in charge of a few emblematic systems to investigate the state space and the second back-end is known as the CL-AtSe (Constraint-Logic-based Attack Searcher), gives an interpretation from any security convention particular composed as change connection in moderate configuration document.

4.2 Specifying the proposed preventive technique for side channel attack

In this segment, discussions about quickly the determination of the proposed plot utilizing HLPSL dialect for the parts of the Cloud client, VM_ware server, session and the earth. In Fig. 3, the executed part for the Cloud client. Amid the enlistment stage, the Cloud client at first transmits ID_i, and the PWB_i to the VM_ware server Fig. 4, through secure channel.

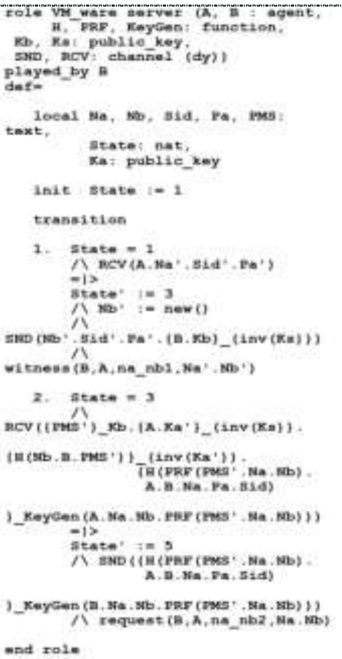
4.3 Simulation results

In this segment, to determine reenactment consequences of the proposed plot in view of the generally acknowledged two back-finishes, for example, OFMC and CL-AtSe utilizing the SPAN-AVISPA apparatus [17]. The Figures 6 and 7 affirm that the proposed convention is SAFE in two back-closes OFMC and CL-AtSe separately. In addition, the reenactment comes about utilizing AVISPA unmistakably guarantee that the proposed plot is secure against dynamic and inactive assaults incorporating replay and man-in-center assaults.



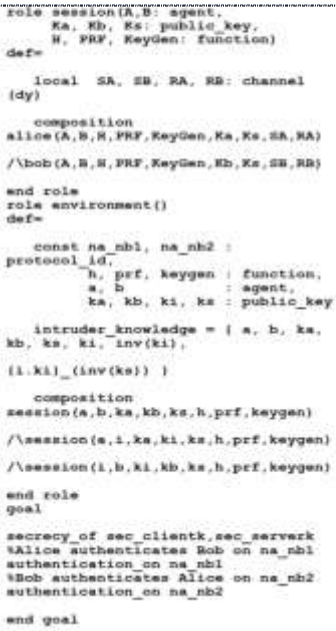
```
role Cloud_User(A, B : agent,
    H, PRF, KeyGen: function,
    Ka, Ks: public_key,  %% Ks is the
public key of a T3P (ie. CA)
    SND, RCV: channel (dy))
played_by A
def=

    local Na, Sid, Pa, PMS: text,
          Nb: text,
          State: nat,
          Finished, ClientK, ServerK:
message,
          Kb: public_key,
          M: message

    const sec_clientk, sec_serverk :
protocol_id

    init  State := 0

    transition

    1.   State = 0
         /\ RCV(start)
         =|>
         State' := 2
         /\ Na' := new()
         /\ Pa' := new()
         /\ Sid' := new()
         /\ SND(A.Na'.Sid'.Pa')

    % Since we abstract away from the
negotiation
    % of cryptographic algorithms, here
I simply assume
    % that the server must send back
Pa.  (Essentially
    % modelling that the client makes
only one offer.)


    2.   State = 2
         /\
RCV(Nb'.Sid.Pa.{B.Kb'}_(inv(Ks)))
         =|>
         State' := 3
         /\ PMS' := new()
         /\ M' := PRF(PMS'.Na.Nb')
         /\ Finished' =
H(PRF(PMS'.Na.Nb').A.B.Na.Pa.Sid)
         /\ ClientK' =
KeyGen(A.Na.Nb'.PRF(PMS'.Na.Nb'))
         /\ ServerK' =
KeyGen(B.Na.Nb'.PRF(PMS'.Na.Nb'))
         /\ SND({PMS'}_Kb'.
                {A.Ka}_(inv(Ks)).

{H(Nb'.B.PMS')}_(inv(Ka)).
                {H(PRF(PMS'.Na.Nb').
                 A.B.Na.Pa.Sid)

}_KeyGen(A.Na.Nb'.PRF(PMS'.Na.Nb')))
         /\ witness(A,B,na_nb2,Na.Nb')

    4.   State = 3
         /\ RCV({Finished}_ServerK)
         =|>
         State' := 5
         /\ request(A,B,na_nb1,Na.Nb)
         /\
secret(ClientK,sec_clientk,{A,B})
         /\
secret(ServerK,sec_serverk,{A,B})

end role
```

Figure-3:- Role specification for Cloud_User.



```
role VM_ware server (A, B : agent,
     H, PRF, KeyGen: function,
 Kb, Ks: public_key,
 SND, RCV: channel (dy))
played_by B
def=

   local Na, Nb, Sid, Pa, PMS:
text,
         State: nat,
         Ka: public_key

   init  State := 1

   transition

   1.   State = 1
        /\ RCV(A.Na'.Sid'.Pa')
        =|>
        State' := 3
        /\ Nb' := new()
        /\
SND(Nb'.Sid'.Pa'.{B.Kb}_(inv(Ks)))
        /\
witness(B,A,na_nb1,Na'.Nb')

   2.   State = 3
        /\
RCV({PMS'}_Kb.{A.Ka'}_(inv(Ks)).

{H(Nb.B.PMS')}_(inv(Ka')).
                 {H(PRF(PMS'.Na.Nb).
                  A.B.Na.Pa.Sid)

}_KeyGen(A.Na.Nb.PRF(PMS'.Na.Nb)))
        =|>
        State' := 5
        /\ SND({H(PRF(PMS'.Na.Nb).
                  A.B.Na.Pa.Sid)

}_KeyGen(B.Na.Nb.PRF(PMS'.Na.Nb)))
        /\ request(B,A,na_nb2,Na.Nb)

end role
```

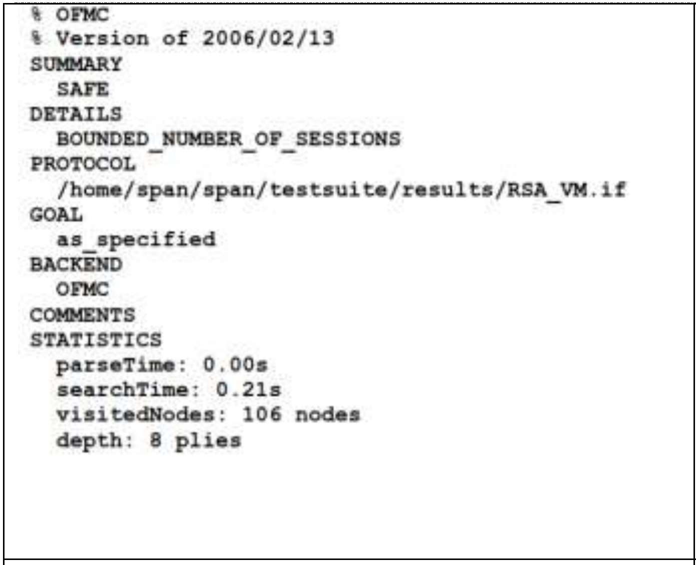
Figure-4:- Role specification for VM_ware server



```
role session(A,B: agent,
      Ka, Kb, Ks: public_key,
      H, PRF, KeyGen: function)
def=

   local  SA, SB, RA, RB: channel
(dy)

   composition
alice(A,B,H,PRF,KeyGen,Ka,Ks,SA,RA)

/\bob(A,B,H,PRF,KeyGen,Kb,Ks,SB,RB)

end role
role environment()
def=

   const na_nb1, na_nb2 :
protocol_id,
          h, prf, keygen : function,
          a, b           : agent,
          ka, kb, ki, ks : public_key

   intruder_knowledge = { a, b, ka,
kb, ks, ki, inv(ki),

{i.ki}_(inv(ks)) }

   composition
session(a,b,ka,kb,ks,h,prf,keygen)

/\session(a,i,ka,ki,ks,h,prf,keygen)

/\session(i,b,ki,kb,ks,h,prf,keygen)

end role
goal

secrecy_of sec_clientk,sec_serverk
%Alice authenticates Bob on na_nb1
authentication_on na_nb1
%Bob authenticates Alice on na_nb2
authentication_on na_nb2

end goal
```

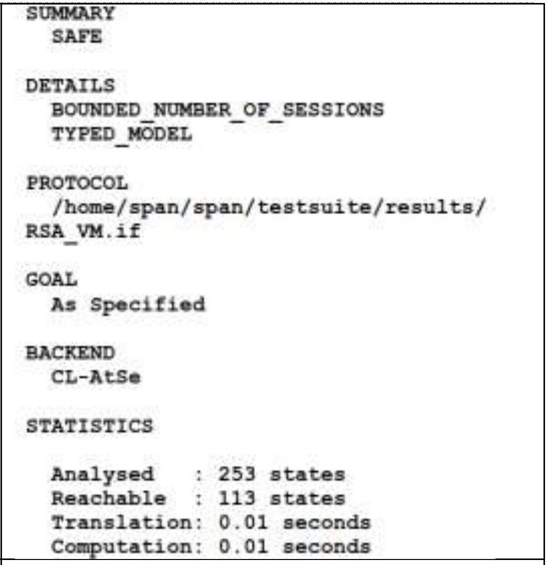
Figure-5:- Role specification for session., goal and environment of the preventive cloud side channel attack in HLPSL.

In preventive cloud side channel attack the SPAN-AVISPA used for cryptanalysis in OFMC and CL-AtSe back-end servers shown that, the proposed protocol is safe, accordingly the following security goals are verified.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/RSA_VM.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.21s
  visitedNodes: 106 nodes
  depth: 8 plies
```

Figure-6:- Simulation result of protective side channel scheme in cloud based on the OFMC back end.



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/
RSA_VM.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 253 states
  Reachable  : 113 states
  Translation: 0.01 seconds
  Computation: 0.01 seconds
```

Figure-7:- Simulation result of protective side channel scheme in cloud on the CL-AtSe back end.

V. EVALUATION OF PREVENTIVE TECHNIQUE FOR SIDE CHANNEL ATTACK

The test out a contextual analysis of the proposed protocol by utilizing the libgcrypt v.1.5.0 cryptographic library [26]. This is the latest variant of libgcrypt; the outcomes stretch out to cover prior variants too. To be solid, in additionally fixed an application that uses the library: Gnu Privacy Guard (GnuPG) v.2.0.19 [27]. GnuPG is used comprehensively to scramble and stamping email, in any case the observations in the libgcrypt use goes past just GnuPG. The physical VM assault should connect with any application using the feeble calendars from libgcrypt. ElGamal encryption. Manual code review revealed that libgcrypt uses a practically course perusing variety of the square-and-increment segregated exponentiation figuring for use with cryptosystems, for instance, RSA and ElGamal [7].

5.1 VM-ware cloud VM-ware cloud working storage processing

To execute this convention in a setting in which two VM-product cloud, each of which has two VCPUs, co-harp on a private connection quad-focus processor, specifically an Intel Core 2 Duo with a working repeat of 2.5 GHz. Both VMs ran a Ubuntu 10.04 server with a Linux parcel 2.6.32.16. The degree of the memory in the guest VMs was adequately broad to sidestep visit page swapping as was insignificant to the examinations. The loss VM ran GnuPG v.2.0.19 with libgcrypt version v.1.5.0, the latest structures as of this composed work. The setback's ElGamal private key was made with security parameter κ = 4096. Diverse parameters for the attack is showed up in Table-1.

Parameters	With VM based cloud	Without VM based cloud
a	100	50
b	50	50
c	9	15
d	15	25
x	3	3
y	50	25

Table-1: VM-ware cloud working storage processing

The examination done in Sec. 5.1, Dom0 can be stacked by, for instance, compelling it to crash a high rate of altering rules. To get different things tried with a few such situations such as shifting in the quantity of standards and parcel rates and then also other circumstances that would empower the invader and victim to share a VM cloud CPU.

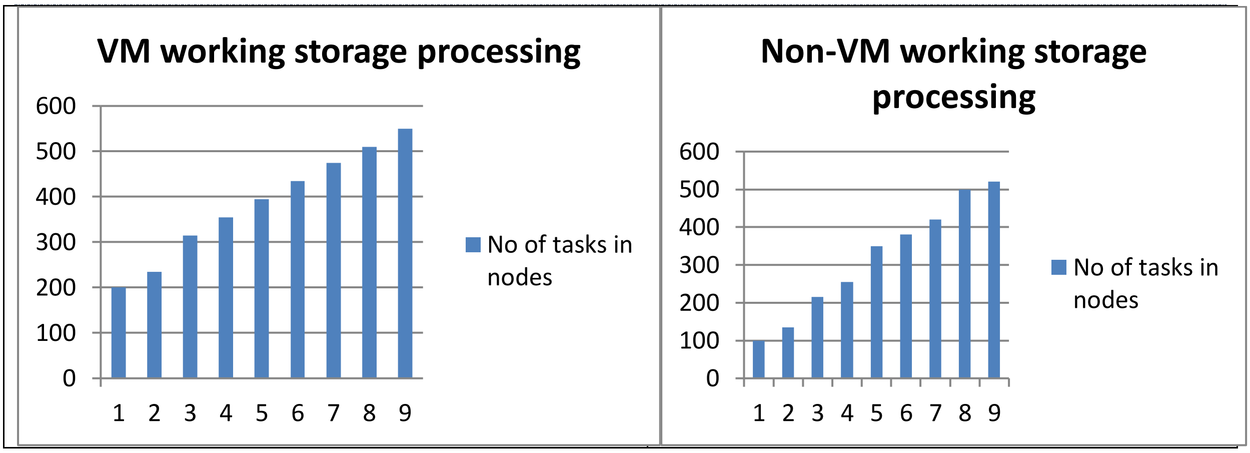


Figure 8: (a) With virtual storage processing (b) With virtual storage processing

Furthermore evaluated the assault for a non-work-safeguarding setting of the Xen scheduler which is settings as weight 256 and top 80. The incited workload in Dom0 and the setback continues as before as in the past fragment in Figure 8. At the point when this happens, the comparing prime-test result must be with virtual and non virtual work preserving, information gathering takes longer and the pieces coming about because of the Elgamal and RSA have a tendency to be shorter. These effects are shown in Figures.8 (a) and (b), which demonstrates the number of tasks executed without attach in VM storage at the same phase of handling attacks as is shown in table-1 for the VM work-moderating cases.

VI. CONCLUSION AND FUTURE SCOPE

In this approach, first checked on crafted by RSA and Elgamal in view of side channel assaults counteractive action distributed security convention by Yinqian Zhang et al. From that point forward, and demonstrated tplan is powerless against a few assaults, which prompts greater security disadvantages and furthermore can't accomplish cloud dependability property. With a specific end goal to oppose these security entanglements, this paper proposes a hearty RSA based preventive VM-product based security conspire in virtual cloud condition. Also demonstrated that the proposed plot gives enhanced security includes and propelled security level than other existing related plans, which are affirmed through casual cryptanalysis. Likewise, this approach has played out the reenactment for the formal security confirmation of the proposed plot utilizing BAN-AVISPA device. The reproduction consequences of the BAN-AVISPA and libgcrypt devices affirm that the approach is SAFE in two back-closes OFMC and CL-AtSe models, that imply the convention is secure against dynamic and inactive assaults incorporating replay and man-in-the-center assaults. The proposed avoidance conspire accomplishes cloud secrecy and in addition keeps VM-product property. In additionally studies will consolidate biometric security to give more secured cloud framework and furthermore attempt to improve troubles of the convention without trading off security angles in future.

VII. REFERENCES

1. Almutairi, Abdulrahman, et al. "A distributed access control architecture for cloud computing." IEEE software 29.2 (2012): 36-44.
2. Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 4.1 (2013): 5.
3. Zhang, Yinqian, et al. "Cross-tenant side-channel attacks in PaaS clouds." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014.
4. Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." IEEE Internet Computing 16.1 (2012): 69-73.
5. Aviram, Amittai, et al. "Determinating timing channels in compute clouds." Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010.
6. Zhang, Yinqian, et al. "Homealone: Co-residency detection in the cloud via side-channel analysis." Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, 2011.
7. Zhang, Yinqian, et al. "Cross-VM side channels and their use to extract private keys." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

8. Heen, Olivier, et al. "Improving the resistance to side-channel attacks on cloud storage services." New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on. IEEE, 2012.
9. Sevak, Bhrugu. "Security against side channel attack in cloud computing." International journal of engineering and advanced technology (IJEAT) 2.2 (2013): 183.
10. Liu, Fangfei, et al. "Catalyst: Defeating last-level cache side channel attacks in cloud computing." High Performance Computer Architecture (HPCA), 2016 IEEE International Symposium on. IEEE, 2016.
11. Liu, Fangfei, et al. "Last-level cache side-channel attacks are practical." Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.
12. Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.
13. Hlavacs, Helmut, et al. "Energy consumption side-channel attack at virtual machines in a cloud." Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. IEEE, 2011.
14. Kim, Taesoo, Marcus Peinado, and Gloria Mainar-Ruiz. "STEALTHMEM: System-Level Protection Against Cache-Based Side Channel Attacks in the Cloud." USENIX Security symposium. 2012.
15. Godfrey, Michael, and Mohammad Zulkernine. "A server-side solution to cache-based side-channel attacks in the cloud." Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on. IEEE, 2013.
16. BAN Tool, A. W. http://www.avispa-project.org/web-interface/ Febru- ary, 2015.
17. Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P., Hem, P., Kouchnarenko, O., Mantovani, J., Mdersheim, S., von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Vigan, L., Vigneron, L., The avispa tool for the automated validation of internet security protocols and applica- tions. In: Computer Aided Verification, Lecture notes in computer science. Vol. 3576, pp. 281–285, 2005.
18. Harnik, Danny, Benny Pinkas, and Alexandra Shulman-Peleg. "Side channels in cloud services: Deduplication in cloud storage." IEEE Security & Privacy 8.6 (2010): 40-47.
19. Chen, Yanpei, Vern Paxson, and Randy H. Katz. "What's new about cloud computing security." University of California, Berkeley Report No. UCB/EECS-2010-5 January 20.2010 (2010): 2010-5.
20. Singh, Ajey, and Dr Maneesh Shrivastava. "Overview of attacks on cloud computing." International Journal of Engineering and Innovative Technology (IJEIT) 1.4 (2012).
21. Hund, Ralf, Carsten Willems, and Thorsten Holz. "Practical timing side channel attacks against kernel space ASLR." Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013.
22. Mulazzani, Martin, et al. "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space." USENIX security symposium. 2011.
23. Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE, 2011.
24. Godfrey, Michael Misiu, and Mohammad Zulkernine. "Preventing cache-based side-channel attacks in a cloud environment." IEEE transactions on cloud computing 2.4 (2014): 395-408.
25. Modi, Chirag, et al. "A survey on security issues and solutions at different layers of Cloud computing." The Journal of Supercomputing 63.2 (2013): 561-592.
26. The libgcrypt v.1.5.0 cryptographic library http://www.gnu.org/programming/ libgcrypt/
27. http://www.gnupg. organization/

CITE AN ARTICLE

G, A. M., Rao, K. V., & Murthy, J. (n.d.). AN EFFECTIVE AND SECURED TECHNIQUE FOR SIDE-CHANNEL ATTACKS IN CLOUD. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(11), 226-233.