Light Weight Forensic Investigation System using VM snapshot Approach

[1] Miss. Aishwarya Patil, [2] Prof. M. U. Inamdar

[1]Student, [2]Proffesor

[1] P.G. Student, Department of E&TC, SCOE, Pune, Maharashtra, India,

[2] Assistant Professor, Department of E&TC, SCOE, Pune, Maharashtra, India.

Abstract : Cloud computing has as of late developed as an innovation to enable clients to get to software, deployment, storage, and foundation condition dependent on a compensation for-what-they-utilize model. Customary digital forensics can't deal with the dynamic and multi-occupant nature of the cloud condition as it needs to address different specialized, lawful, and authoritative provokes common to the cloud frameworks. The dynamic idea of cloud computing enables inexhaustible chances to empower digital examinations in the cloud condition. In this tends to the difficulties of digital forensics in the cloud environmentand existing answers for facilitate a portion of the difficulties. We propose an effective way to deal with scientific examination in cloud utilizing Virtual Machine (VM) previews.

IndexTerms **- Cloud computing, Virtual Machine, Intrusion Detection system, Forensic Investigation, VM Snapshots, Attacks.**

I. INTRODUCTION

Cloud is a developing innovation and cloud based storage is the recently embraced thought that encourages clients not exclusively to transfer information to the web yet additionally enables moment openness to accessible assets and offer information with anybody anytime of time. Yet, Cloud is an innovation that makes a test for the individual who is examining and discovering the measurable confirmations that may help in the scientific investigation as information put away on cloud can be gotten to from anyplace and from any framework and almost no measure of follows are abandoned.

The 21st century is known to be the time of digital world. There has been the reception of PCs all things considered. Today without PCs and Internet one can't get by as we are subject to these machines for practically the entirety of our work. Mulling over beginning from home to instruction till banking and even corporate working everything has now been mechanized to PCs. PCs contain all our significant information in the digital arrangement. With this the need to store the digital information has expanded and virtual condition has swapped the physical storage for putting away the entirety of our qualifications as appeared in Fig. 1. The most crushing test of cloud is to anticipate the unapproved cancellation of the put away information on cloud since one can undoubtedly erase the stuff with no legitimate approval. The information cancellation is absolutely reliant on erasure of hubs that are indicating some data in Virtual Machine.

VMs are quickly picking up fame because of their capacity to imitate computing situations, seclude clients and bolster remote introduction. Avoidance of unapproved or noxious exercises in cloud is a noteworthy test. So there is need of performing Digital Investigation on the cloud stage which prompts propose a strategy that will most likely anticipate the unapproved exercises on VM. We propose a way to deal with measurable examination, utilizing Log Information and VM Snapshots of the pernicious exercises in the cloud condition. To guarantee the security of Log documents we expect to apply Encryption calculations to Log data, which will be useful for further examination.

II. LITERATURE SURVEY

Wireless sensor networks (WSN) throughout the years have turned out to be one of the most encouraging systems administration arrangements with energizing new applications for the not so distant future. Its deployment has been improved by its little, reasonable and savvy sensor hubs, which are effectively conveyed, contingent upon its application and inclusion territory. Basic applications incorporate its utilization for military activities, observing ecological conditions, (for example, well of lava discovery, agribusiness and the board), dispersed control frameworks, human services and recognition of radioactive sources. Despite its promising qualities, security in WSN is a major test and remains a progressing examination pattern. Sent sensor hubs are defenseless against different security attacks because of its design, threatening deployment area and shaky directing convention. In this work, we present a survey of DoS attacks that influence asset accessibility in WSN and their countermeasure by exhibiting a scientific categorization. [1]

Intrusion of psychological militants and trespassers are antagonistically influencing the harmony and agreement in the country. The fatalities and unsettling influences brought about by the most recent Uri assault in Indian Army Camp demonstrate the need of a proficient fringe observation and gatecrasher recognition framework for the successful checking and identifying the unapproved development of interlopers over the national outskirts. Customary outskirt watching comes up short on an incorporated multi-detecting framework that directions different advances for observation and location of human gatecrasher development in the diverse fringe situations: level surface development, waterway/lake intersection and dry leaves development. This paper portrays the present Wireless Sensor Network (WSN) procedures identified with gatecrasher location and outskirt reconnaissance. Our future work centers around conveying an improved multi-detecting framework for distinguishing intrusion exercises to verify the national borders.[2]

Asset restriction is primary worry of sensor hubs in wireless sensor networks. There are numerous security dangers which are influencing the, usefulness, security and system life time of and wireless sensor networks. In this paper security dangers, security objectives, different attacks, order of these attacks are introduced alongside the examination of various intrusion recognition frameworks in wireless sensor networks. Point by point data about intrusion identification frameworks is given at that point,

intrusion recognition techniques are thought about dependent on various plans. Intrusion location plans are arranged dependent on systems utilized in the plan: Specification based plan, computational insight and information mining based plan, game hypothesis approach based intrusion discovery conspire, likelihood circulation based identification scheme.[3]

Wireless Sensor Network (WSN) is a system with enormous number of modest sensor gadgets which are of ease, and least utilization of intensity called as sensor hubs. These sort of hubs have extraordinary detecting innovation which are explicitly intended for applications, for example, military, brilliant homes and other security related territories. Due its wireless nature, system can be sent anyplace in the earth, which turns out to be progressively defenseless for assailants to decimate the system. Above all, WSN ought to be shielded from malevolent exercises to happen and in this way security turns into a noteworthy issue. In any case, such security can be given by applying instruments to both intrusion location and counteractive action. In our examination, design coordinating is one of the system that can be utilized for security of WSN. We likewise talk about a portion of the preventive estimates that can be considered for securing the sensor network.[4]

In this strategy the conduct of hubs is watched and checked whether it is ordinary or not. We select some Intrusion Detection System(IDS) specialists based on inside blockage inside the hub. IDS operator are prepared to examine the conduct of the hubs and can check the deviation in the conduct of the hubs. We give a framework to IDS operator, which is put away in their support. This framework comprise of parameters which are identified with the conduct of the hub. Info estimation of the network is 0 or 1, on the off chance that the lattice result is 1, at that point the conduct of the hub is abnormal(deviation from typical). The IDS operators send the one of a kind identifier of the bargained hub to the Base Station. Base Station will at long last check what number of messages a hub can send to Base Station. On the off chance that the number is more prominent than the greatest message limit, at that point the hub is viewed as bargained hub. The calculation which is proposed in this paper can be effective for the little networks.[5]

III. Problem Statement

This work focuses the challenges of digital forensics in the cloud. In recent times the cloud environment is misused by many clients for storing and distributing illegal information. There is need of dedicated digital forensic framework for cloud environment. System proposes an efficient approach to forensic investigation in cloud using Virtual Machine (VM) snapshots. This will be capture VM snapshot whose integrity cannot be compromised. This approach will be executed for multiple VM's.

IV. Objectives

The objectives of this research work include the following:

- Explore the challenges and requirements of forensics in the virtualized environment of cloud computing
- Design a digital forensic framework for the cloud computing systems from the view point of investigator and/or cloud architecture
- Address the issues of dead/live forensic analysis within/outside the virtual machine that runs in a cloud environment
- Using digital forensic triage in the examination and partial analysis phase of cloud forensics

V. Proposed System

There are too many systems which are used for attack detection and forensic IDS in cloud environment. The traditional digital forensic process undergoes the following steps which can be incorporated in cloud forensics considering its different service and deployment models.

- Identification of malicious activity
- Collection of Evidences
- Examination
- Analysis
- Reporting & presentation

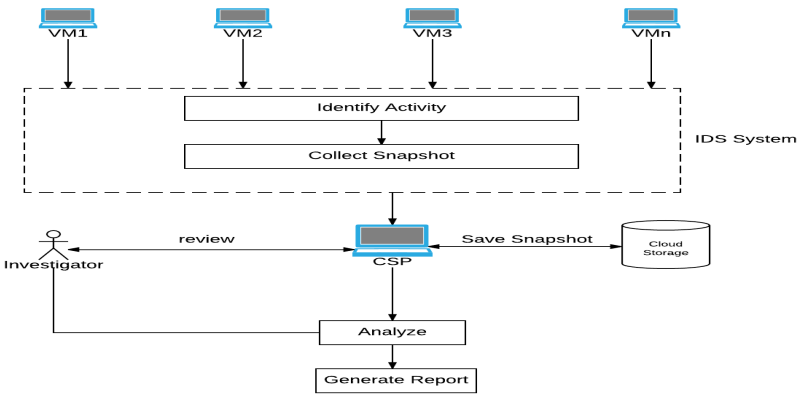

Fig.1. Proposed System Architecture

We have implemented the system which can be divided into three modules.

1. Attacker
2. Receiver
3. Investigator

1. Attacker:

In attacker module we have implemented SQL injection attack, DOS attacks, R2L attack. These attacks are performed on Virtual machines of amazon ec2 cloud. SQL injection attack is implemented using cosine algorithm as described below. During search file of user module we can search keyword for that file. If keyword matches with file data then it will show file name. Also

we have performed cosine similarity for keyword with SQL signature pattern to check and detect SQL Injection Attack. We have created matrix to define 16 pattern signature attacks that are stored in database Using Cosine similarity formula SQL injection attack is detected.

2. Receiver

We have implemented Intrusion detection system that is continuously running on VM. IDS is created in such a way that as soon as malicious activity is observed it takes snapshots of attacker. For e.g. if user enters SQL injection signature like 1==1 or?? , this activity is observed by IDS. We have stored worldwide accepted 16 types of signature for SQL injection attack so if text entered by user matches one of these signatures then user is suspected as malicious user.

VI. ALGORITHMS

1. AES design flow:

It consists of plaintext, sub keys and that is given to add round key which is then given to rounds.

- Bytes in AES: Bytes this is the Hexadecimal representation of bit patterns. The basic unit for processing in the AES algorithm is a byte.
- Array of bytes: Arrays of bytes will be represented in the following form: a0a1a2a15. The bytes and The bit ordering within bytes are derived from the 128 bit input se-quence input0input1input2input126input127 A0= input0, input1,...input7 A1= input8, input9,.input15 . . . A15= input120, input121,input127. The pattern can be extended to longer sequences (i.e. for 192 and 256 bit keys) so that in general, An= input8n, in-put8n+1,.input 8n+7
- subbytes step:
  In the subbytes step, each byte in the state is replaced with its entry in a fixed 8 bit lookup table,S; bij=S(aij)
- The mix column step:
  In the mixcolumns step, each column of the state is multiplied with a fixed polynomial c(x).
- The addround key step:
  In the addround key step, each byte of the state is combined with a byte of the round sub key using the xor operation.

2. Cosine Similarity Algorithm for Word Matching

```
CosineScore(q)
1   Initialize(Scores[d ∈ D])
2   Initialize(Magnitude[d ∈ D])
3   for     each term(t ∈ q)
4   do      p ← FetchPostingsList(t)
5   dft ← GetCorpusWideStats(p)
6    α t,q ← WeightInQuery(t, q, dft)
7   for     each {d, tft,d} ∈ p
8   do      Scores[d] + =    αt,q • WeightInDocument(t, q, dft)
9   for     d ∈ Scores
10  do      Normalize(Scores[d], Magnitude[d])
11  return  top K ∈ Scores
```

3. Pattern Matching Algorithm for sub attack classification

Input : Attack type which found in test dataset T
Output: Master attack type with sub attack type
Step 1: Initialize all master attacks in DB.
Step 2: Set all sub attacks to master attacks.
Step 3: for each instance I where (T !=Null)
Step 4: attackName= matchAttackName(I)
Step 5: Return attack type with count
Step 6: repeat this up to step 3.

STEP 7: END FOR

VII. RESULTS AND DISCUSSIONS

We have implemented system to perform forensic investigation using VM snapshots as evidences along with log information about attacks. As shown in figure 13 attacker module enters the malicious query, this activity is identified by intrusion detection system. We have performed SQL injection, DOS attacks, Remote to local attacks, wrong OTP attack on VM, and we have got the following results during attack.

When user enters SQL injection signature like 1==1, snapshot of attacker VM is captured by IDS as shown in figure 10.

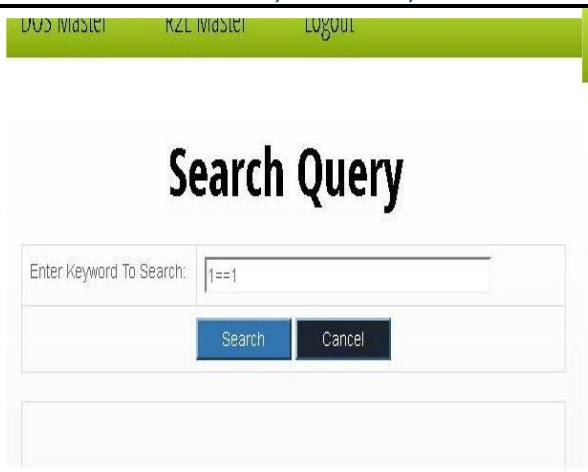

Fig. 2 Snapshot of SQL injection attacker

Fig. 3 Snapshot of Crash server attack

We have performed Remote to local attack, by crashing server on VM .Figure 12 shows snapshot captured by IDS during crash server attack.

We have also implemented OTP attack, in which users with no right cannot modify the contents of file. Only manager can read and write to file. In spite of that if malicious user tries to modify the contents of file then OTP is generated and this OTP is sent to manager's email id.As this user have no access to get the OTP he might enter wrong OTP which leads to malicious activity. IDS identify this as wrong OTP attack and capture the snapshot of attacker VM. Figure 13 shows snapshot of attacker VM.

Fig. 4 Snapshot of OTP attack

Fig. 5 Log Information

Along with the VM snapshots, log information of the attacks is maintained. This log information consists of date and time of attack, IP address and MAC address of attacker VM.Figure 14 shows the snapshot of Log information.

All the existing approaches have implemented forensic investigation on single VM, whereas we have used multiple (four) VMs for testing different types of attacks.

VIII. CONCLUSION

The proposed methodology takes previews of suspected VM and set away in steady accumulating, subsequently improves the execution of cloud. What's more, here is another module which is agent module who can counteract the assault VM to make another assault by blocking them (assaulting VMs). We demonstrate the better methodology which can have most elevated exactness pace of assault recognition.

In the area of Cloud there consistently remains a space for improvement in the current framework. At present the work was effective in incorporating the proposed framework with the order line interface. Hence, in future, endeavors for joining of a validation instrument with the graphical UI of cloud would be attempted.

REFERENCES

[1] Opeyemi Osanaiye, Attahiru S. Alfa, Gerhard P. Hancke, "Denial of Service (DoS) Defence for Resource Availability in Wireless Sensor Networks", DOI 10.1109/ACCESS.2018.2793841, IEEE Access

[2] Arjun D, Indukala P K and K A Unnikrishna Menon, "Border Surveillance and Intruder Detection Using Wireless Sensor Networks: A Brief Survey", International Conference on Communication and Signal Processing, April 6-8, 2017, India

[3] Sonu Duhan, Padmavati khandnor, "I ntrusion Detection System in Wireless Sensor Networks: A Comprehensive Review", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 978-1-4673-9939-5/16/$31.00 ©2016 IEEE

[4] Gauri Kalnoor, Jayashree Agarkhed, "Pattern Matching Intrusion Detection Technique for Wireless Sensor Networks", nternational Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16)

[5] Sushant Kumar Pandey, Prabhat Kumar, Jyoti Prakash Singh and M.P. Singh, "Intrusion detection system using Anomaly technique in Wireless Sensor Network", International Conference on Computing, Communication and Automation (ICCCA2016)

[6] Z. Qi; C. Xiang; R. Ma; J. Li; h. Guan; D. Wei, ―ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics,‖ in IEEE Transactions on Cloud Computing , vol.PP, no.99, pp.1-1 doi: 10.1109/TCC.2016.2535295

[7] V. Varadharajan; U. Tupakula, ―Securing Services in Networked Cloud Infrastructures, ‖ in IEEETransactions on Cloud Computing ,vol.PP, no.99 ,pp.1-1 .doi: 10.1109/TCC.2016.2570752

[8] S. Zawoad and R. Hasan, ―Trustworthy Digital Forensics in the Cloud,‖ inComputer, vol. 49, no. 3, pp. 78-81,Mar.2016.doi: 10.1109/MC.2016.89

[9] S. Alqahtany, N. Clarke, S. Furnell and C. Reich, ―Cloud Forensics: A Review of Challenges, Solutions and Open Problems, ‖2015 International Conference on Cloud Computing (ICCC), Riyadh, 2015,pp.1-9.doi: 10.1109/ CLOUDCOMP. 2015.7 149635

[10] E. Morioka and M. S. Sharbaf, ―Digital forensics research on cloud computing: An investigation of cloud forensics solutions,‖2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham,MA,2016,pp.1-6.doi: 10.1109/ THS.2016. 75 68909

[11] D. R. Rani and G. Geethakumari, ―An efficient approach to forensic investigation in cloud using VM snapshots,‖2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-5.doi: 10.1109/PERVASIVE.2015.7087206

[12] M. Irfan, H. Abbas and W. Iqbal, ―Feasibility analysis for incorporating/deploying SIEM for forensics evidence collection in cloud environment, ‖2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, 2015, pp. 15-21. doi: 10.1109/ICIS.2015.7166563