Botnet attack investigation on Geography of Things (GoT)

[1]K.UMAMAHESWARI
[2]R.SANTHI DEVI
[3]S. SUJATHA

[1,3]Department of Computer Science, Bharathi Women's College, Chennai, Tamilnadu, India.
[2]Department of Geography, Bharathi Women's College, Chennai, Tamilnadu, India.
[1]uma.tvr1981@gmail.com
[2]santhidevig@gmail.com
[3]sujaphd@gmail.com

Abstract. The breakneck speed of Internet of Things (IoT) is continually growing with 5G networks to add new connected devices. Hackers make use of this IoT explosion as a perfect chance to launch attacks especially by building botnet army. There had been lot of research over the decade in detecting and investigating the Distributed Denial of Service (DDoS) attacks. This paper was aimed at the presentation of a cloud based forensic investigation framework that can adaptively acquire attack evidences from IoT environment. The investigation model is called INSPECT that worked in cloud data storage to acquire corresponding evidences of the DDoS attack launched on IoT. The model optimally selected and exploited the forensic fields alone from the vast cloud data logs in order to find the source of attack and to report dynamic chain of custody. As a continuous effort, an experimental setup was built with IoT Geo-spatial devices to launch DDoS attack scenario and investigation performed with contextual initialization based evidence acquisition. Significant progress was observed by isolating the trustworthy evidence data to avert any deliberate modification by attackers and presenting the chain of custody. The work provided way for the law enforcement authority to explore and reconstruct the crime scene using virtual machine snapshots with corresponding timestamp data. Experimental results revealed the high level of accuracy in the investigation of IoT data secured in the multitenant cloud.

Keywords: DDoS attacks, forensic investigation, Geo-Spatial devices, botnet.

(Received May 1st, 2020/ Accepted June 11st, 2020)

1 Introduction

Today IoT is a trend that transforms the society by connecting almost "everything". The population of connected IoT devices almost passed the earth's population that is about 7.5 billion in early 2019 and it will likely to become triple by 2021 [11]. The IoT has become a growing security risk and privacy concern for the consumers. Cyber criminals are attracted by the explosion of IoT devices in people's homes and working places [16]. The real issue associated with such an enormous device growth is that those connected devices are mostly vulnerable to cyber attacks. The reality of IoT botnet army formed with innocent household equipments connected with Internet was realized on October 21, 2016 through Mirai botnet attack [10]. This kind of flooding attack committed Distributed Denial of Service (DDoS) against most significant websites to shut down. Here the question is about whether the regulations for the protection of consumers are effectively followed in IoT environments as fast as the speed of IoT threats. Those threats mostly focus on the use of hijacked resources for the launch of Denial-of-Service (DoS) attacks and to mine for virtual currencies. The increasing IoT vulnerability incidences show the significance of IoT Forensic techniques for the criminal investigation. The concept of IoT Forensics used to perform investigation on IoT based devices where the digital forensics aspects applied in the IoT parameters. Digital Forensics in IoT is termed as challenging and varied because of the data management issues associated with the large number of IoT devices [21]. IoT forensics can be applied in three classes based on the location of forensic data and the place of investigation as depicted in Figure 1. The classification is about Device or Node level, Network level of data collection and Cloud level of data storage [23]. Forensic research is primarily conducted at the first 2 levels where sensor data is collected, transferred and communicated among the elements of IoT [5]. Each level is associated with its own set of benefits and limitations. Device level investigation is preferred when data is to be directly collected from the device memory. But volatile memory acquisition is a challenging task that attracts many researches. The network of IoT devices or sensors can be the main data source of routing and tracking of lost packets for doing cyber forensics after an incident [4]. Network data is mostly volatile that are critical for the many forensic investigation scenarios. Cloud level forensics has its own challenges on multi-tenancy and multi-jurisdictional issues[17]. The present work is built on cloud level forensics as the actual IoT data is processed and stored in Cloud.

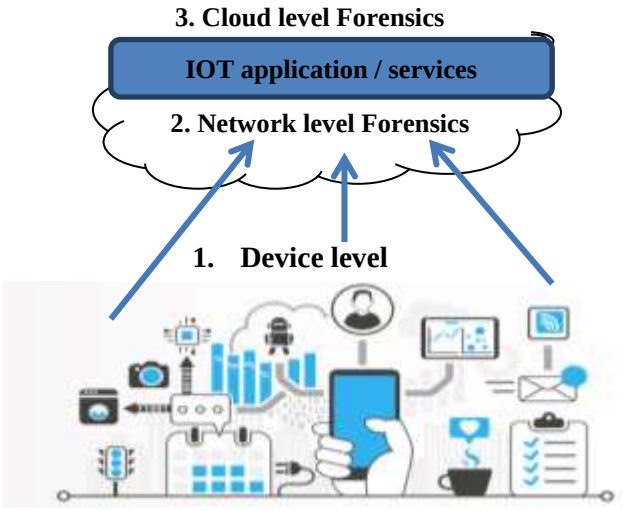

Figure 1: Digital Forensics levels on IoT

1.1 Cloud Level Investigation

Multi-tenancy and multi-jurisdiction are the challenges to be faced in cloud environment based forensic investigation. As IoT devices have limited storage and computational resources, the associated data is processed and stored in the cloud storage. Whenever data in physical storage and network is not result in useful evidence, investigations to be carried out in the cloud environment. Hence, various investigative challenges in the cloud exist when forensic investigations in IoT are to be conducted. Current research reports in IoT forensics are mostly in their early stages. There are also some successful models suggest effective investigations in the cloud environment.

1.2 INSPECT approach for IoT environment

To cope up with the constraints of IoT vulnerability this paper presents an investigation model called INSPECT [19], that applies adaptive evidence acquisition method that works in the cloud on the IoT data with adequate support for presenting dynamic Chain of Custody. The INSPECT approach utilizes the Virtual Machine (VM) log files to forensically acquire corresponding evidences from the IoT data stored in cloud based on the place of malicious activity. Here the evidence acquisition and analysis process enhanced by the optimal selection and exploitation of IoT forensic fields alone other than the entire log file. Contextual initialization method applied

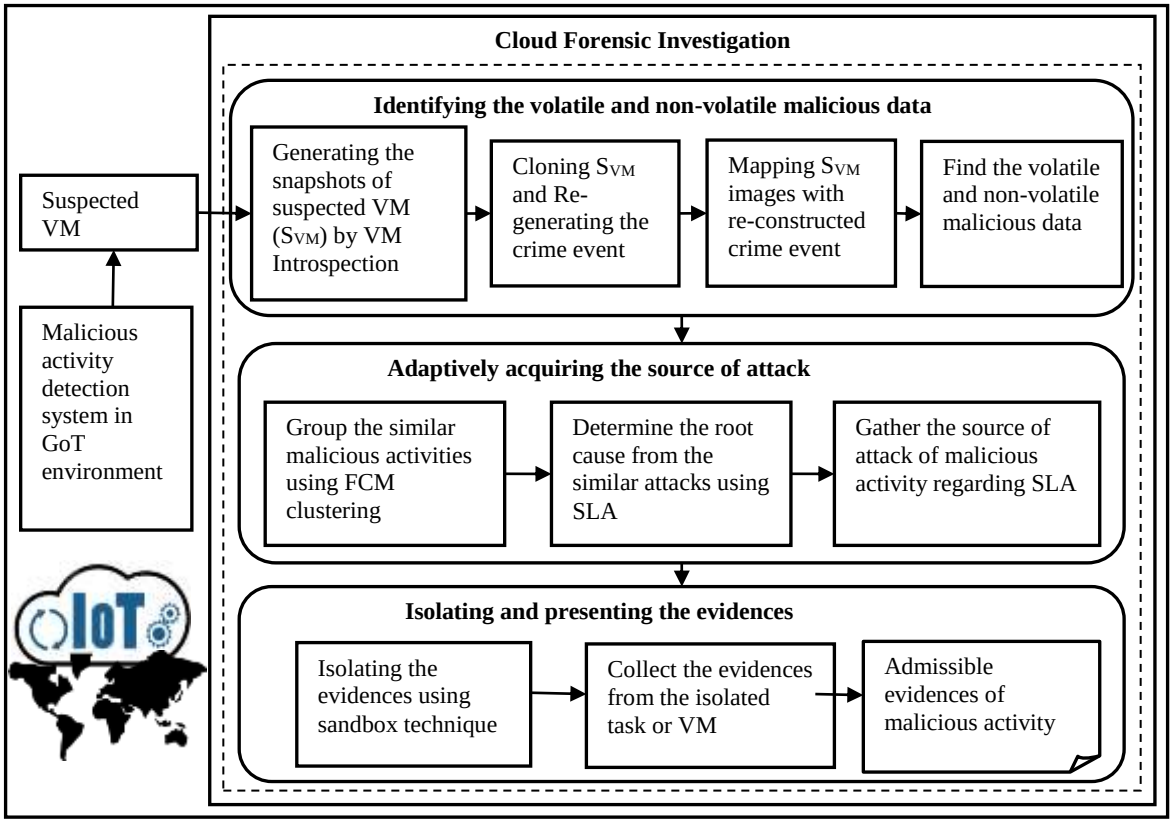

Figure 2: INSPECT forensic architecture for GoT environment in Cloud

in the INSPECT model to recognize the source of attack and to improve the evidence trustworthiness. Service Level Agreement (SLA) of the cloud users are analyzed to facilitate the identification of source of attack from the clustered IoT data stored in cloud. The method gives significance to the isolation of evidences to avert any adversary who intends to do deliberate change in the multitenant environment. The crime incident is presented by means of chain of custody information along with the evidence data to the law enforcement authority. The authority can explore the evidence information available in the chain of custody to reconstruct the crime scene with the help of VM snapshots attached with the timestamp data.

2 Related Work

Because of the mobility, distributed and decentralized characteristics of IoT environment, lot of issues associated with conventional digital forensic tools and techniques [3,9,22]. Those large counts of smart devices intend to generate vast amount of evidence. However new set of challenges to be faced by the investigators for every aspect of data management [11]. Collection of evidence from the highly distributed and decentralized infrastructures of IoT is again a breath-taking task [12]. Various formats of data followed in the variety of IoT devices raise problems in evidence analysis [23]. It is questionable to ensure the reliability as the attacker can tamper the evidence stored in those devices [18, 6].

Zawoad and Hasan [23] proposed a forensics-aware model suitable for IoT infrastructures known as FAIoT, in which the term IoT forensics was not previously defined until their proposal. Their model supports for collection of digital evidence and analysis in the IoT environment through providing easiness and forensic soundness. Cloud forensic investigation built on the base of various evidence collection methods and event reconstruction methods [15]. Frost [1] is a method of evidence collection in cloud forensic investigation where forensic tools for the OpenStack cloud platform supporting Infrastructure-as-a-service (IaaS) cloud, provides lot of chances for the investigators to acquire sound evidence from the cloud. For the precise

acquisition of evidence in the cloud infrastructure adaptive evidence collection model [13] employed. Virtual Machine Introspection is performed through the virtualization of VM interfaces in the cloud through periodical monitoring of allocated resources [21]. Two snapshots of the same virtual machine is explored in Forensic acquisition approach [7]. That model identifies the disparity among the snapshots before and after suspicious activity.

3 INSPECT methodology on Geography of Things (GoT)

The proposed system applies M-FCM clustering method in the determination of evidence data regarding malicious activities. The system gives assurance for the investigation process to be finite, as there will be continuous changes in the IoT environment and corresponding cloud scenario. The methodology involves three major phases on identification of volatile and non-volatile malicious data, adaptive acquisition of source of attack and presentation of evidence as shown in Figure 2.

3.1 Identification of volatile and non-volatile malicious data

Virtual Machine Introspection (VMI) method is exploited for the identification of volatile and non-volatile malicious data. The INSPECT approach leverages the investigator after the receipt of attack location reported by any malicious activity detection system applied on the IoT devices environment. The malicious activity detection system is any kind of Intrusion Detection System (IDS) for the determination of attack location through the concerned VM ID through the exploration of rule fluctuations of a specific process in the server. The data is of volatile and non volatile nature acquired with the help of VM snapshots. Forensic investigator performs screenshot analysis and reconstruction of crime event for finding the feasibility of locating the corresponding evidence of the crime event. The reconstruction of the crime event is based on the temporal factor associated with the sequential snapshots in which temporal information may vary to the different sources due to the presence of asynchronous instances. To tackle this inconsistency, the INSPECT approach exploits the time updating tool in which the snapshots are dynamically updated, which eliminates the existing time of the system and updates the current global time as the metadata on the snapshots. It facilitates the crime event reconstruction process in an effective manner.

With the aim of achieving more accurate and rapid process of crime event reconstruction, the INSPECT approach determines the volatile data by correlating the disparate sources of forensically relevant data. The primary objective of this work is to enable efficient and fast event recording involving storage and processing data monitoring to reconstruct the crime event quickly. The INSPECT approach employs the VMI method which monitors the VM resources through Virtual Machine Monitor (VMM) and provides the results that are to be compared with the results from IDS. It averts the feasibility of obtaining the compromised results by the attacker. After determination of the suspected VM by the IDS, the INSPECT approach utilizes the VM snapshot method which is one of the dimensions of the VMI technique where in Snapshot creates a replica of the VM at a particular time. On considering the primary objective, the INSPECT approach reduces the amount of forensically analyzing data by only accessing the VM data from live snapshots at a particular time interval rather than accessing the whole snapshots of that VM. It initiates the Live snapshot methods when the system identifies the attack location. The INSPECT approach develops a model for taking the live snapshots of the VMs to recover the volatile data involving logs and memory files of VM instances.

3.2 Adaptive acquisition of source of attack

The log files of the Virtual Machine extracted for the identification of malicious data. In order to effectively identify the source of attack, two steps are followed in the INSPECT process. In the first step M-FCM clustering is applied for the aggregation of malicious data of the similar type. Next step is the analysis of SLAs of the clusters. The second step accelerates the identification of source of attack by the presentation of set of source of attacks scored differently for each data cluster.

3.2.1 Aggregation of identical malicious data through Modified FCM Clustering

The proactive and reactive analysis for evidence collection focused by the INSPECT approach for the precise adaptive forensic investigation. The system preserves the most prominent evidence which is more beneficial to the forensic investigation to take the immediate and strong suggestion about the crime event. The approach performs the Fuzzy C-means clustering than fuzzy logic function for the adaptive determination

of fuzziness of the malicious data. The fuzzification process produces the fuzziness degree for the malicious data points. Finite set of 'n' data is segmented into the number of groups on the basis of fuzzy membership values. The initial assignment of number of clusters 'C' is based on the malicious data in the cloud collected from the IoT environment. Initial points are selected in two levels: i) random points ({P}) selection on the basis of input data and ii) finding of 'Min' and 'Max' as random points (rp1,rp2) from the initial set ({P}). For 'n' number of malicious data, the INSPECT method selects {P} random points through '$0.01*n^2/(n-1)$'. The probability of each point in Representative Point (RP) selection by the equation (1) follows:

$$Pr(rp)_{x_i}=\frac{Dist\left(x_i,rp^{(p)}\right)}{\sum_{rp_i=1}^{k} Dist\left(x_i,rp_i\right)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Here, Dist(xi,RP) is the distance from the data point (x^i) and representative point $rp^{(p)}$. The approach modifies the membership matrix (a_{ij}) through equation 2.

$$a_{ij}=\frac{\left(\left|x_i-rp_j\right|\right)^{-2/(m-1)}}{\sum_{k=1}^{c}\left(\left|x_i-rp_k\right|\right)^{-2/(m-1)}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

The approach finds out the secondary representative points and modifies the matrix of membership degree until $|A^{l+1} - A^l|$ is lower than the default value 1e-5, like the case of classical FCM clustering method. The default value means the minimum improvement over the two values. If |Al+1 - Al| is larger than default, equation (1) is employed to find the representative points and for sequential modification of membership matrix degree. Equation (3) shows the fuzzy membership function.

$$rp_j=\frac{\sum_{i=1}^{n} \mu_{ij}^{m} x_i}{\sum_{i=1}^{n} \mu_{ij}^{m}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

MFCM Algorithm is presented here as follows:

C=Number of clusters
N= Number of input points

Step 1: Create membership matrix A = (C*N)
Step 2: Select set of random points {P} for each C by $0.01*n^2/(n-1)$
Step 3: Set {rp1, rp2} as min and max random points from {P} by sorting {P}
Step 4: Select representative points based on input data
Modify membership matrix $A=\{\mu_{ij}\}_{i,j=1}^{nk}$
Step 5: If $|A^{r+1} - A^r| > 1e\text{-}5$ then do Step 6
else do Step 8.
Step 6: For every point p in {P}, calculate membership degree $\mu_k(P)$
Step 7: For every cluster ck in {C} calculate centroid. Go to step 5.
Step 8: Report C number of clusters.

3.2.2 Identification of source of attacks using SLAs

The approach analyses the SLAs negotiated among the CSP and the users where users may be involved in the range of malicious data indicated through the IDS. The INSPECT approach identifies the causal relationships among a specific type of malicious activity, attack location, and attack launcher who may be a malicious insider, cloud user, VM, or third party through SLA data. The associated SLAs are explored to find the probability of attack launchers. Sequential log matching of the components are accomplished from hypervisor.

3.2.3 Isolation and presentation of the evidence

After the determination of the evidence and the source of attacks, the INSPECT approach aims to isolate the evidence collected from IoT environment in the cloud storage for facilitating the forensic investigation. It is an integral part investigation process to prevent the evidence from tampering. Isolation intended to protect the evidence admissibility. It is possible through the cloud instances in the multi-tenant environment during forensic investigation.

3.2.4 Evidence Isolation through Sandboxing

Appropriate sandboxing applied for the isolation and preservation of the evidence in forensic investigation. Sandboxing restricts the actions of the process in a sandbox depending on the security policy that can ensure the realistic forensic investigation in an isolated environment. The images of the virtual instances are completely captured through the dynamic analysis of the sandboxing method that can help compare the actual execution from malicious execution, like the case of snapshot based evidence identification. Our approach provides the factors of the evidence ahead to a specific Sandbox for the isolation of the appropriate evidences. Hence evidence isolation is facilitated and leading to proactive measures against the future malicious attacks on the collected evidence. Hypervisor logs are exploited to potentially find the information of all tenants. Here the information comprises virtual instances creation and deletion logs.

3.2.5 Preservation and Presentation of Evidences

The evidence gathered from the acquisition phase need to be presented to the court of law in the form of a chain of custody by the forensic investigator. It is a process of submitting the organized report regarding the conducted actions of the crime investigation like evidence collection, analysis, and preservation. For the maintenance of the chain of custody log, the approach employs the Advance Forensic Format (AFF4) and Resource Description Framework (RDF) for the improvement of AFF4. AFF4 is an open, expansive and configurable format, which stores the arbitrary metadata. AFF4 with RDF descriptions can automate the interaction among the chain of custody software and the real world. Finally, the jury performs validation of the evidence from the source of attacks and the knowledge of CSP and consequently, adjudges the real suspect of the corresponding crime scene.

4 Experimental Evaluation

This section describes the evaluation of prototype implementation of the proposed INSPECT approach in IoT environment in which the evaluation is done in the OpenNebula cloud management architecture.

4.1 Experimental setup

In the context of this paper, Geography of Things (GoT) is defined in terms of physical sensors or mobile phones with sensing equipment. Physical location is considered as any location (i.e., the location of crime occurrence) tagged with geographic coordinates of latitude and longitude. The INSPECT approach for IoT environment runs its prototype model in OpenNebula which has the ability to work with the Kernel-based Virtual Machine (KVM), Xen, and VMware virtualization facilitating the accommodation of multiple hardware and software. The INSPECT approach employs daemon tool to create a forensic session, including collections and separation of evidential artifacts in the cloud by exploiting an IP address determined from the IDS employed in IoT environment. Then, the information is given to the OpenNebula and GRR to which information refers that the IP address based mapped cloud data. Google Rapid Response (GRR) is an open source tool involving client-server model, which eases the process of attaining the incident response in a large-scale server. It enables the administrators to explore the appropriate user machines and accumulate the segregated data of the corresponding user from the cloud storage. To perform the memory forensics, the INSPECT employs Libvmi API for VM introspection in the cloud.

4.2 Evaluation metrics

Investigation time, Data recovery efficiency and Investigation Accuracy are the basic evaluation metrics employed in INSPECT for IoT environment. Investigation time is the total time taken by the investigator to collect the evidential artifacts from the cloud. Data recovery efficiency is the ratio between the amount of recovered data of malicious activity and deleted data of malicious activity. Investigation Accuracy is the percentage of evidence collection accuracy of a malicious user at a specific time, which is based on the mapping of crime event with the acquired evidence.

4.3 Experimental results

To evaluate the performance of the proposed model, the INSPECT approach exemplifies the attack scenario in the Geography of Things environment with the detail demonstration of the proposed forensic investigation process.

4.3.1 Case Study

The INSPECT approach selects and analyzes the Simple Storage Service (S3) scenario from Amazon Web Service (AWS) that stores the GoT log data. AWS provide the service to the users with the entire control of user-required resources in a pay-as-you-go manner. The INSPECT runs the proposed algorithm with the main objective of forensic investigation in the OpenNebula cloud middleware. The overall process of the INSPECT approach is illustrated in the following steps.

Step 1: Initializing the INSPECT Forensic process

The malicious activity in the host is determined by Suricata IDS[2], which is packet header anomaly detector for the signature based intrusion detection. The INSPECT approach initializes the forensic method in the cloud environment, which is illustrated in Figure 3 demonstrating the sample forensic login using credentials for Gmail.

In OpenNebula, with the help of hypervisor, daemon receives the IP address or unique information of attack location from IDS and maps the received IP address with the cloud storage to take the snapshots of that particular machine. The sample suspected location in the cloud is shown in Figure 4.

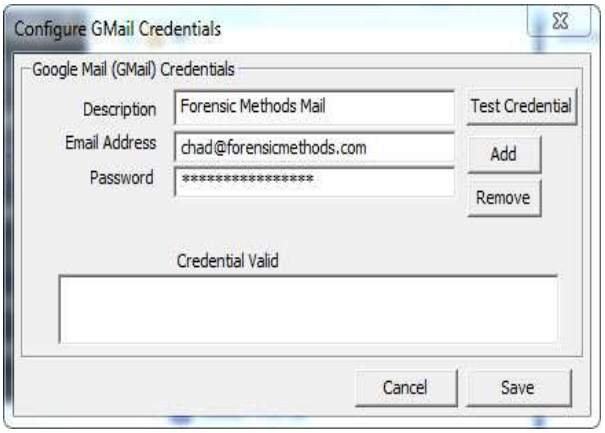

Figure 3: Forensic method initialization

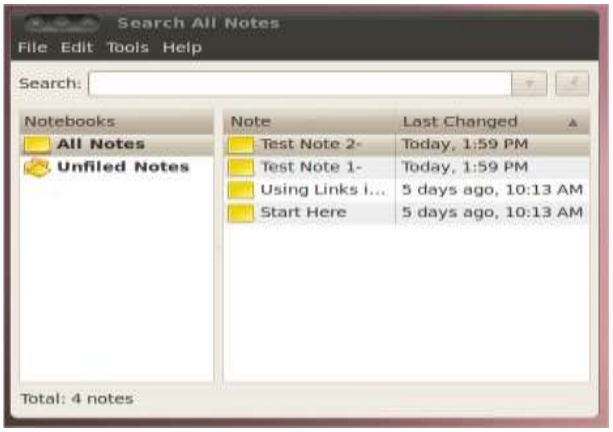

Figure 4: Location of Malicious activity

Step 2: Determining the VM residing evidence regarding malicious activity

In the cloud infrastructure, if an attack is known attack, IDS has the ability to determine the malicious activity and consequently take the snapshots. In contrast, the system utilizes the stored snapshots to recognize the malicious activity residing location and to perform the post forensic investigation after receiving the command of initiating the forensic process in a specific location. OpenNebula enables the snapshot creations and VM migrations.

The dashboard information shows the run time availability of the cloud storage, which is shown in Figure 5. The corresponding VM and data storage location with the specifications of VM ID, IP address, availability, and so on, which are illustrated in Figure 6 and 7. These information facilitates the INSPECT approach to determine the machine that having the evidential artifacts with respect to the malicious activity.

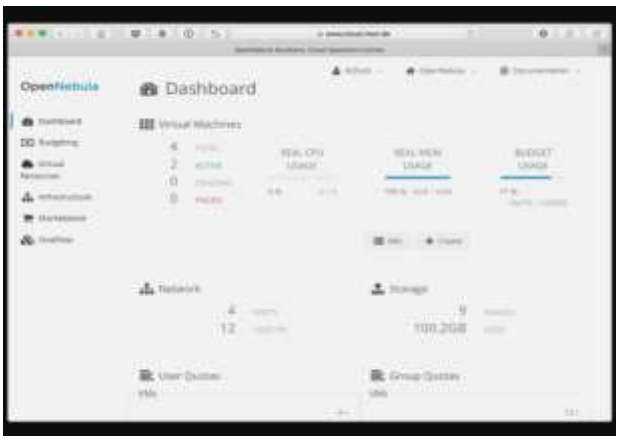

Figure 5: Dashboard

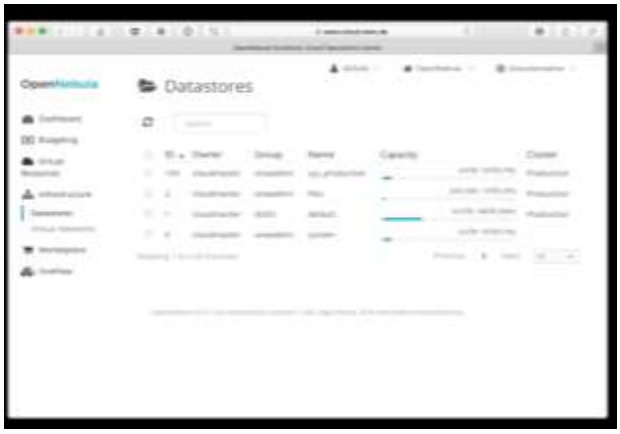

Figure 6: Data Store Locations

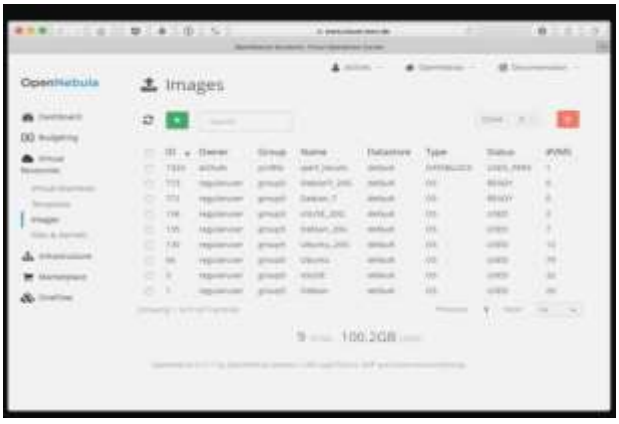

Figure 7: VM images

Step 3: Performing memory analysis on a specific VM

The INSPECT employs the time updating tool while storing the VM snapshots in the cloud, which maintains the synchronized time information. Figure 8 shows the process information regarding a specific VM execution.

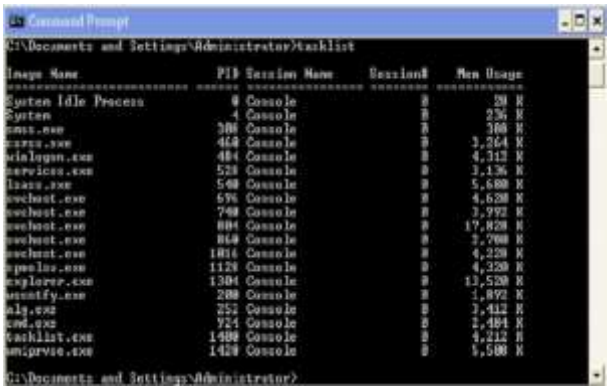

Figure 8: Processes running on VM

Figure 10: Hidden process revealed using INSPECT

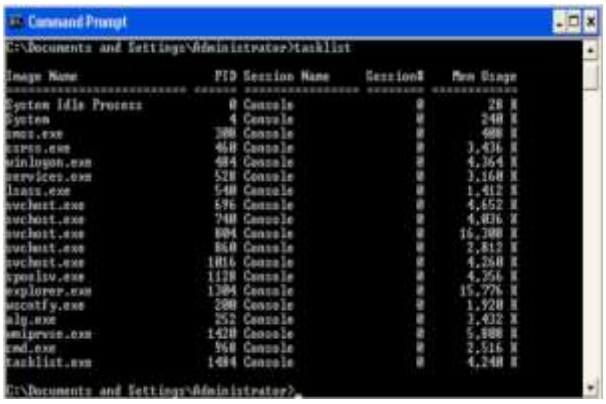

Figure 9: Processes running on VM after infection

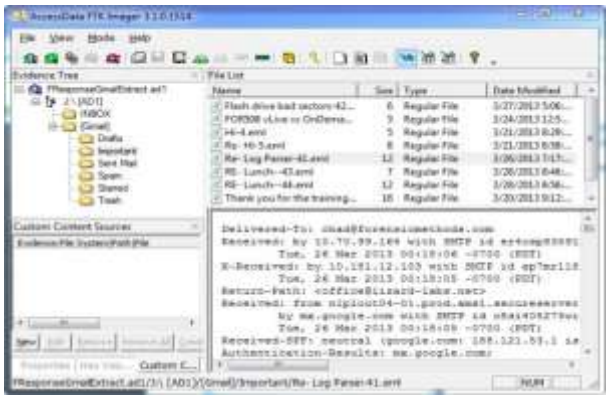

Figure 11: Forensic acquisition

Step 4: Applying VM introspection method

The information related to a specific VM running in the cloud, which is obtained by LibVMI.

Step 5: Reconstructing the crime event

The INSPECT approach reconstructs the crime event using the VM snapshots to determine the evidence even when the VM is terminated after launching the malicious activity in the cloud. The crime event reconstruction is based on the sequential VM snapshots stored in the cloud. Figure 10 illustrates the sample running state of VM after reconstruction.

Step 6: Identifying the volatile data using VM snapshots

The INSPECT approach determines the volatile and non-volatile data in the cloud using VMI method, which also averts the inaccurate evidence acquisition by analyzing the evidence with VMI method instead of utilizing the data from IDS. Figure 10 reveals the deleted volatile evidence in the cloud.

Step 7: Adaptive forensic data acquisition using MFCM

The INSPECT approach aggregates the similar malicious data in terms of numerical values by FCM clustering. The forensic data acquisition process involves source of attack identification to maintain the chain of custody and determine a real suspect of the corresponding crime scene in the cloud. By utilizing the FCM clustering and SLA information with the assistance of the CSP, the INSPECT approach performs the forensic data acquisition which is shown in Figure 11.

Step 8: Isolation and Forensic investigation analysis

To tackle with the multi-tenancy, the INSPECT approach isolates the evidences using sandboxing method and investigates the evidential artifacts by the forensic investigator. It submits the evidence with the chain of custody information with the help of AFF4 and RDF to improve the trust worthiness of the forensic investigation. Figure 12 illustrates the sample of forensic analysis process in the cloud infrastructure.

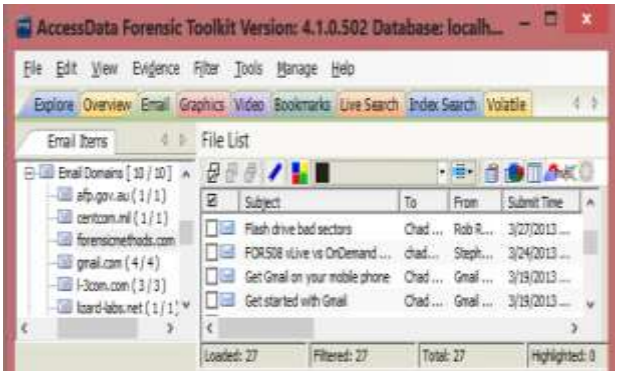

Figure 12: Forensic analysis

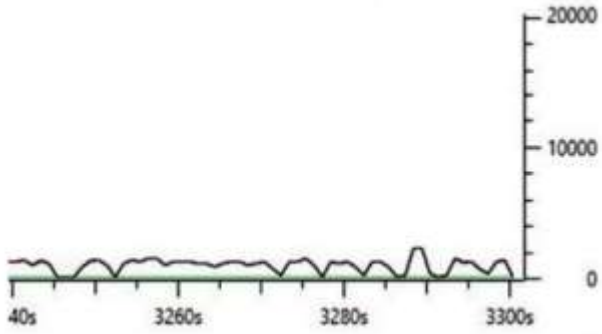

Fig. 13.a: IO graphs for normal traffic

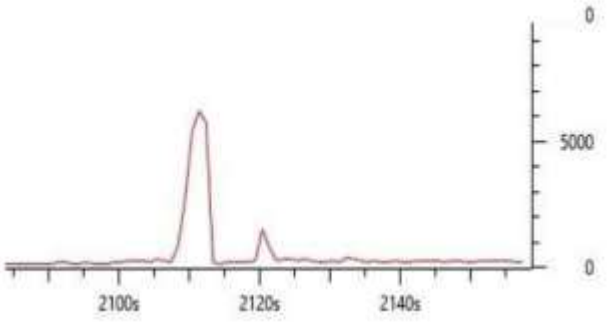

Fig. 13.b.: IO graphs for attack traffic

5 Results and Discussion

In the real IoT environment, evaluating the performance of the INSPECT approach is essential by analyzing the benefits of the cloud provider, forensic investigator, and cloud users. In order to validate the significant performance improvement in the INSPECT approach, the evaluation system discusses the investigation time, data recovery efficiency, and the investigation accuracy. The cloud service provider is AWS and the cloud user is the AWS dependent organization. The INSPECT approach improves the performance regarding the scalability due to the forensic investigation does not depend on the number of resources and requests in the remote server. It considers only the snapshots for forensic investigation rather than exploring the entire cloud storage. Hence, the INSPECT approach does not increase the burden to the cloud service provider with respect to the scalability. The proposed methodology ease the forensic investigation by exploiting the snapshots and determining the volatile data of the crime scene, which leads the investigator to complete the investigation in a reasonable time and also ensures better volatile data recovery efficiency. It improves the investigation accuracy due to the consideration of the FCM clustering and SLAs while acquiring the evidences. The attack states can be better understand through the IO traffic graphs obtained from Wireshark tool as given in Figure 13 a and b. The INSPECT approach provides the two main benefits to the IoT user. Initially, it improves the feasibility to perform the cloud forensic investigation in their services even the cloud user runs their service on a remote cloud. Secondly, the cloud user has the ability to allocate the resources to perform the forensic investigation. Thus, the INSPECT approach ensures the benefits to both the user and the provider while ensuring the data privacy.

6 Conclusion

This paper has presented a intelligent and reliable forensic investigation model for the IoT from cloud environment. The proposed model, the INSPECT approach employs the VM snapshots and MFCM clustering method to acquire the evidences from the IoT even when there is the deleted malicious data. It reconstructs the crime scene using temporal information based VM snapshots and adaptively collects the source of attacks using MFCM clustering with contextual initialization. The INSPECT approach determines the appropriate evidences and source of attacks using SLA information given by the CSP. Then, it isolates the evidences by applying sandboxing method to perform the uninterrupted and uncompromised forensic investigation in the cloud infrastructure. Finally, it preserves and presents the acquired evidences with the help of AFF4 and RDF framework comprising the information related to forensic investigation, which maintains the chain of custody and facilitates the presentation process. The experimental evaluation demonstrates that the proposed INSPECT approach yields better investigation accuracy as well as volatile data recovering accuracy with the concern of data privacy in the cloud infrastructure for the IoT environment.

References

[1] Dykstra, J., Sherman A. T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, 10, pp.S87-S95, 2013.

[2] Elrawy, M., Awad, A., Hamed, H. Intrusion detection systems for IoT based smart environments: a survey. *J Cloud Comp*, 7, 21(2018). https://doi.org/10.1186/s13677-018-0123-6

[3] Encase, Encase forensics. https://www.guidancesoftware.com/.

[4] Faraoun K.M., Boukelif A. Neural networks learning improvement using the K-means clustering algorithm to detect network intrusions. *INFOCOMP Journal of Computer Science*, 5(3):28-36, 2006.

[5] Gokila Dorai, Shiva Houshmand, Ibrahim Baggili. I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Rating You Out. In *ARES, Hamburg*. Aug 27-30, 2018.

[6] Hegarty, R., Lamb, D., Attwood, A. Digital evidence challenges in the internet of things. In *Proc. of the 10th International Network Conference*, pages:163, 2014

[7] Hirwani, M., Pan, Y., Stackpole, B., Johnson, D. Forensic acquisition and analysis of vmware virtual hard disks. In *Proceedings of the International Conference on Security and Management (SAM), The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), ew publication*, 2012.

[8] IoT Threat Landscape. https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf

[9] Khaing, M.S., Thant, Y.M., Tun, T., Htwe, C.S., Thwin, M.M.S. IoT Botnet Detection Mechanism Based on UDP Protocol. *In IEEE Conference on Computer Applications (ICCA), Yangon*, Pages: 1-7, 2020.

[10] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer*. 50 (7) : 80-84, 2017.

[11] Meffert, C., Clark, D., Baggili, I., Breitinger, F. Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition. in *ARES. ACM*, 2017.

[12] Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P. Internet of things forensics: Challenges and approaches. in *COLLABORATECOM. IEEE*, 2013.

[13] Pasquale, L., Hanvey, S., Mcgloin, M., Nuseibeh, B. Adaptive evidence collection in the cloud using attack scenarios. *Computers and Security*, 59, pp.236-254, 2016

[14] Randi Rizal, Imam Riadi,Yudi Prayudi. Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 7(4): 382-390, 2018.

[15] Ruan, K., Carthy, J., Kechadi, T. Survey on cloud forensics and critical criteria for cloud forensic capability: a preliminary analysis. In *Proceedings of the Conference on Digital Forensics, Security and Law, Association of Digital Forensics, Security and Law*, page: 55, 2011.

[16] Sapalo Sicato, J.C., Sharma, P.K., Loia, V., Park, J.H. VPN Filter Malware Analysis on Cyber Threat in Smart Home Network. *Appl. Sci.* 9, 2763, 2019.

[17] Taylor, M., Haggerty, J., Gresty, D., Lamb, D. Forensic investigation of Cloud computing systems. *Network Security*, 2011(3): 4-10, 2011.

[18] Toldinas, J., Venckauskas,A., Grigaliunas, S. Damasevicius, R., Jusas, V. Suitability of the digital forensic tools for investigation of cyber crime in the internet of things and services. in *RCITD. RCITD*, 2015.

[19] Umamaheswari, K., Sujatha, S. INSPECT- An Intelligent and Reliable Forensic Investigation through Virtual Machine Snapshots. *I.J. Modern Education and Computer Science*, 3: 17-28, 2018.

[20] Wireshark: Network packet analyzer, https://www.wireshark.org.

[21] Wook Baek, H., Srivastava, A., Van der Merwe, J. Cloudvmi: Virtual machine introspection as a cloud service. In *IEEE International Conference on Cloud Engineering (IC2E)*, pp.153-158, 2014

[22] Zawoad, S., Hasan A1R. Cloud forensics: a meta-study of challenges, approaches and open problems. *A17 in arXiv preprint arXiv:* 1302.6312, 2013.

[23] Zawoad, S., Hasan, R. Faiot: Towards building a forensics aware eco system for the internet of things. In *IEEE International Conference on Services Computing (SCC)*, pages: 279-284, 2015.