Journal of Theoretical and Applied Information Technology
30th September 2019. Vol.97. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY OF DIGITAL FORENSIC METHODS UNDER ADVANCED PERSISTENT THREAT IN FOG COMPUTING ENVIRONMENT

AHMAD K. Al HWAITAT[1], SAHER MANASEER[2], RIZIK M. H. Al-SAYYED[3]

[12] King Abdullah the II IT School, The University of Jordan , Department of Computer Science, Jordan,

[3] King Abdullah the II IT School, The University of Jordan ,Department of Information Technology, Jordan,

E-mail: [1]*Ahmad.Hwaitat1@gmail.com* , [2]*Sahr@ju.edu.jo* ,[3] *rizikalsayyed@ju.edu.jo*

A B S T R A C T

DA Digital forensics has been recently become a significant approach to investigate cybercrimes. Several questions exist about the future of this domain. Many researchers have been done in this field for development, they analyzed the challenges within the domain of cloud computing and an advanced persistent threat (APT) attack. These challenges are rapidly increasing as the volume of data increase, and the technology that the attacker used is continually developed. However, the lack of valid evidence data that is due to the diversity of technology, the deployment platforms, and the less effective models for processing huge volume of data as seen in FOG computing whereas there is a limitation in the analysis tools that are using for investigation of cybercrime. The work in this paper represented in two folds the first is a survey and the second is a proposed method.

The survey review the current forensic Methods under Advanced Persistent Threat (APT) attack and concentrates on the challenge that faces cybercrime in Fog Environment. The other part surveys Meta-heuristic approach such as particle swarm optimization (PSO) and Frequencies particle swarm optimization (FPSO).Then we propose a unique method, which deals with ambient environment and other ways of dealing at the network level.
The proposed method deals with APT attacks in a two-sided manner. The first side identifies the detection and the second side analyzes the behavior of the spread process. The proposed method is based on optimizing the solution using Investigator Digital forensics particle swarm optimization (IDF-PSO) that will be enhanced to detect APT attack that is considered an optimal solution for collecting digital evidence, through to detection and classification APT attack and Study of propagation behavior.

Keywords : *Digital Forensics , Investigation Cyber of Crimes , Security , APT Attacks, Fog computing , Cyber security , cloud computing.*

1. INTRODUCTION

Unknown cyber threat attacks have recently increased so rapidly due to the recent security systems which are unable to detect the attacks. However, there has been more of the leaking of the personal detailed cyber attacked attacking cloud computing [1]. These bouts have been altered from the destruction of the service rather the information leaking to attack the enormous data systems. However, large or small the organizations are, they all use a technology called cloud computing, which helps protect their data. Moreover, they use cloud resources whenever they are true of them [2]. Despite all, Cloud computing technology is also used by the end-user and even big enterprises although it is a resource which is shareable it has also problematic in latency in that the services and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the applications with a new breed as well as their high effectiveness amid the cloud and the fog have as well been developed more so when data management and analytics are considered [3]

Consequently, fog computing has been taken to be a technology tool which helps in preventing the cloud environment. This type of computing model is located for a period of big analytics, which assists the distributed time collection points so closely, which has been used for other application as well as personal computing. Fog computing and cloud computing is the main concept clearly seen in these concepts since cloud does form a centralized system while fog computing constitutes more of decentralized distributed infrastructure. Moreover, cloud computing became a trending technology which consisted of parallel and distributed system, and if the cloud environment shares resources, then it can be actively provisioned and also reconfigured. Since the objective aim of the cloud is to focus on the storage and the computation of the date which by using high bandwidth connections connect high-performance machines. Cloud also concentrates more on centralization while the fog does enlarge the cloud to the borderline network. Fog computing also is elaborated more as a primary part consisting of cloud interaction, features and its linked work in the following subset.
Fog computing should not be seen as a substitute for cloud computing. This platform is being given at computer stores and traditional cloud computing centers for a number of reasons. The highly virtualized platform is the future of technology. Several characteristics of fog computing listed [7]:

1. Edge location
2. location-awareness
3. Low latency.

The main feature of Fog computing is that it extends the borderline network, which combines with well-off services at the network nodes, that enable low latency. Fog computing layer includes computing, network, and storage services benefit nearer to the end-hubs in the IoT. Contrasted with cloud computing, this registering layer is profoundly conveyed and acquaints extra administrations with end-gadgets situated in the discernment layer [8]. This crossing over-layer is eluded distinctively, however, with comparable or little varieties in reason. For instance, edge registering, miniaturized scale cloud or cloudlet is a portion of the related terms. Despite the name, the idea of presenting a middle of the road figuring layer in IoT is spurred by the comparable arrangement of difficulties [9]. Additionally, the conceivable arrangements of administrations that can be possibly coordinated in the fog figuring layer are immense [10]. A portion of these administrations is a scaled adaptation of the ones given by distributed computing while a large portion of these administrations rose as of late in light of IoT challenges.

The current technology of the cloud environment has many challenges with respect to encryption, authentication, authorization, and privacy of personal data [11]. For this, many researchers started to search for solutions to these problems that affect different fields. These problems cause the loss of millions of dollars annually by cyber-attacks. This is particularly caused by Advanced Persistent Threat (APT) attacks that are specialized in hacking and cyber-espionage of military, government, financial, industrial and other installations [12]. The issue is that the danger has changed. However, organizations way to deal with security has not changed. While traditional dangers are as yet worry and can't be disregarded. However, organizations currently have another Advanced Persistent Threat known as the APT.

1.1 The issue of APT Attack

The APT is attacks that is information centered, directed and healthy and not the same as customary viruses as well as the worms. They are as well efficient elements which focus on organizations, therefore, accumulating specific snippet data which helps the APT attack to extract and to reach data as well as concealing tracks at any period of time. Consequently, an organization gets targeted with the use of the APT, and despite this, there are also some steps which assist in limiting the effect since many organizations focus entirely about settling vulnerabilities.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

For example, fixing as a way of dealing with the security for many governments focuses on the fixing random vulnerabilities, for instance, mending as their approach to safety for, they are not defensive against intimidations which got the peak compromise likelihood. Therefore, this explains why many companies to spend millions of dollars every year safety up to date they do get a concession. It gets hard for the individuals at times to accept the fact, but however, in this decade, this day, an organization needs recognition of going to be attacked with an expectation of being compromised highly. It sounds frustrating but it is better to be accepted than to deny life, for if an individual claims not to be sick for the rest of his or her life, I am sure that you would shake your head saying it is not realistic, but a nice claim and also that your organization will never be compromised is being so naïve by uttering that you will never be sick.

When an individual gets sick, its goal to minimize its impact and not to die. Therefore we take lots of vitamins and eat very healthy to reduce times we get sick. However, when we fall sick, the achievement is to get to the doctor to help us to overcome the illness when the disease is still small. For the philosophy that is followed is that detection is a must while prevention is ideal. Therefore, an organization should do a lot of things which help minimalize compromise chance by making sure that the appropriate measures are taken to deal and to detect with an attack in a timely way. With this, the enemy will be in a position to discover a route to the target at APT. They will also be in a position to determine one of the susceptibilities to make the attack. However, this attack needs an effort of discovering each susceptibility since many organizations do not perceive that if the crime more much than the blockade that will get attacked for the attacked is very determined. Therefore, they will go on attempting to a point where they will be very successful, and its major reason for being successful is that it is of another risk where the many organizations are not able to deal with it. APT is a complex assailant that plays out a share of the attack with the human mediation.

This paper aims to propose a method of investigation and collection of evidence dealing with APT attacks in the ambient environment away from the primitive or traditional methods in order to study the mechanism of its work and the stages of its development in spying on the data and the motivation that the work of APT Attack mechanism of its work is linked to the artificial intelligence of the difficult detection, identification and analysis of the propagation behavior of those attacks Return to APT.

Ways to achieve the goal is first to work on a survey of many research that uses different methods in the investigation and collection of digital evidence and work on the study of those methods use. Second, the study of the algorithm (IDF-PSO) to be developed and knowledge of its positivity and usefulness in verifying the collection of digital evidence of APT attacks in the ambient environment.

This paper is dived into the section. Section 2 classifies more of APTs attacks; section 3 gives a report of the investigation of occurrence response of APT attack reports in the Middle East. Section 4 analyses the Shamoon Industrial Espionage as well as the industrial Espionage. Section 5 as well tells more of the cloud forensics. Section 6 analyses the Fog Forensics and its comparison amid them is highlighted in section 7 while section 8 gives the surveys structure, section 9 gives a presentation of the related work and the last, but not least the whole summary is described in the last section which is section 10.

1.2 APTs attacks classification

According to [19-20], the APTs are classified differently from other targeted attacks in the following ways:-

- Customized attacks— In APTs regularly utilize much redone devices and interruption systems, grew particularly for the campaign. These apparatuses incorporate zero-day vulnerability exploits, viruses, worms, and rootkits. APTs regularly dispatch different dangers or "kill chains" all the while to rupture their target.
- Low and slow—APT attacks happen over extensive

stretches of time amid which the attacker to move gradually and unobtrusively to keep away from identification. Rather than the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"crush and snatch" strategies of many focused on assaults propelled by more normal cybercriminals, the aim of the APT is to remain undetected by moving "low and moderate" with consistent checking and connection until the point that the attacker accomplishes their targets.

• Higher aspirations— The goal of an APT may incorporate military, political, or financial data gathering, private information or prized formula danger, disturbance of activities, or even decimation of hardware.

• Specific targets— while about any organization having protected innovation or profitable client data is defenseless to targeted attacks, APTs are used for a lot of targets. APTs may attack merchant or accomplice organizations that work with their primary targets. It may, government-related organizations and makers are by all account, not the only targets.

1.3 Analyzing the incident response of APT attack reports in the Middle East

We have analyzed the incident response of APT attack reports in the Middle East and summarized the results in table 1 that describes the APT attack group, threat intelligence source, and the targeted victims. It can be noticed that Jordan has been one of the countries that had been attacked by APT Espionage.

Table1: A sample of Targeted APT Attacks over the Middle East

Group Common Name	Targeted Objects	Targeted Counties	Malware Name	source Name	date
DarkHydrus	Middle East Government	Middle East	NA	paloaltonetworks	7/27/2018
Leafminer	Gov-Fi-Petro-Shipping	SA-EY-UAE-PL	NA	Symantic	25 JUL, 2018
OilRig	Technology Service Provider and Government	Middle East	QUADAGENT	paloaltonetworks	7/25/2018
Gaza cybergang	Government , NGO	Palestine, State of	NA	checkpoint	7/8/2018
NA	NA	Middle East	Gzipde	AlienVualt	6/20/2018
MuddyWater	Government	Middle East , SA	NA	trendmicro	gence/another
TEMP.Reaper	NA	Middle East	NA	NA	6/14/2018
NA	jobs sites	Qatar	NA	icebrg	6/7/2018
NA	Mikrotik routers	Sudan , Libya , Jordan , Iraq , Yemen	NA	kaspersky	6.March.2018
OilRig	financial institution	Middle East	NA	paloaltonetworks	2/23/2018
NA	Dar El-Jaleel	jordan	Jenxcus	talosintelligence	2/7/2018
DustySky	Third-Party Services	Palestine, State of	DustySky Core	paloaltonetworks	1/26/2018
OilRig	Middle Eastern government organizations	Middle East	RGDoor backdoc	paloaltonetworks	1/25/2018
FrozenCell	mobile	jordan - Palestine,	android	RESEARCHERS	10/5/2017

Figure 1 shows the global attacks that happened on June 2018. The figure there is four reasons that motivate attackers such as Cyber Crimes that constitutes 84.4% of attacks while Cyber Espionage constitutes 12.5% of attacks [21].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

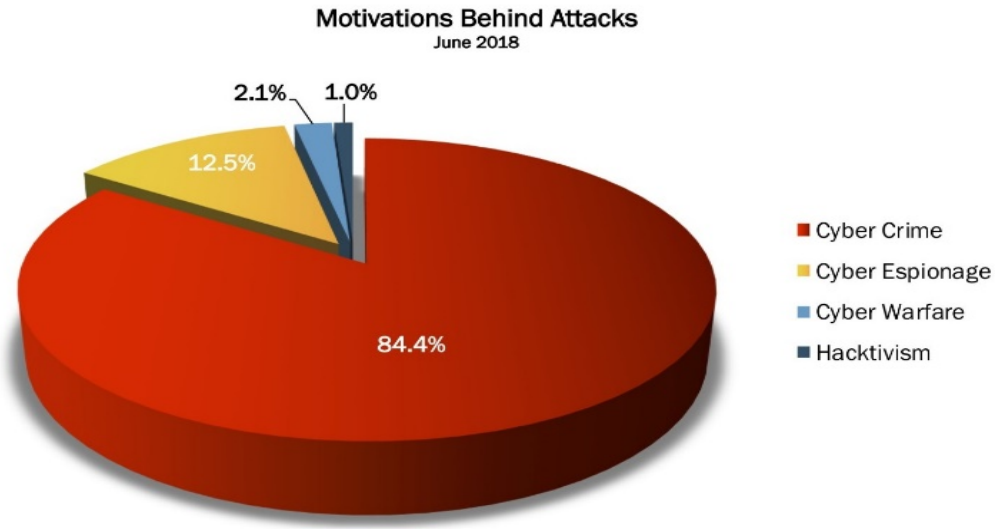

Figure 1: Global attacks that happened on June 2018

1.4 Industrial Espionage

Espionage is the preparation of collecting information that is confidential and not approving approval for its proprietor. It moreover, featured by the demonstration of imparting, transmitting, conveying rather accepting the data based on the national barrier with an aim or the motivation to trust in which the data may be utilized to any country's damage [22]. Contrasting with various types of data assembling happening remotely and which are identified by getting to the bodily site area in which coveted data is kept as well as the overall users handling the explicit data. Spies in other cases attempt to differentiate data from the individuals approved to have known it [23]

1.5 Shamoon Industrial Espionage

Shamoon is also referred to as W32.distract is a specific PC infection that is found by a succulent back in the year 2012, and it focuses on the continuing 32-bit NT portion of the Microsoft window. Its infection has been known to have varying conduct from other malware assaults for they are hazardous to the nature of the assault. The Shamoon further can be spread from a device that is infected to PCs that is varies from the system. For instance, when a framework gets infected, the infection will keep on ordering documents that are random from the specific framework areas, eradicating them as well as transferring them to the aggressor. The infection will finally overwrite boot ace file of the PC that is contaminated and hence making it unusable. This type of infection has been utilized for a numerical fight in contradiction of the national oil company of Qatar's Ras Gas as well as Saudi Arabia's Aramco [25]. This was reported 16 August the year 2012 by Seculert, Kaspersky and Symantec. Moreover, more similarities have been featured by Seculert as well as Kaspersky amid Flame malware and Shamoon.[24]

1.6 Cloud forensics

The most trending model that is efficient in computing model is Cloud computing. Its significant is more affected by the safety issues within the cloud environment. We are going to explain more of cloud forensics in this section.

1.6.1 Definition of cloud forensics

Cloud forensics is distinct as [26] as a cross-discipline that is amid digital forensics and cloud computing. Basing on Cloud computing definition by NIST, it is a procedure that used to attain cloud paradigm as well as reconstructing cloud computing past for giving the numerical evidence [27]. Its technical measures involve more of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

procedure sets. The company measurement as well does involve interactions within cloud actors involving cloud client and the CSPs which assist accelerating investigating whereas Multi-tenancy, Multi -jurisdiction and SLA are implied by legal measurement [28].

1.6.2 Challenges of cloud forensics

Cloud computing has many characteristics. Among them are cloud environment and multi-tenancy which are taken as the encounters of cloud forensics, and these challenges [29] are in the three dimensions as:

1.6.3 The technical dimension of cloud

Any error occurring while obtaining data will bring an impact on the entire investigation. Lack of trust in CSPs, as well as physical access, will bring an impossibility of obtaining data and also the records from the clouds. Another one is the trust problems, and volatile data will determine the extrapolation and the integrity of the records and the data obtained due to accessibility and decentralization. Third is that bandwidth limits the costs and the speed for the absence of information that is important can never be guaranteed at all. For one to preserve the privacy tenants, renting multiples will make it more difficult in obtaining evidence for Forensic tools have not developed for research but rather a virtual environment.

1.6.4 Organizational Dimension

Lack of relevant legal experience and forensic experience is the major problem in the regulatory measurement of forensic medicine due to the evidence that is obtained from the CSPs as well dependence of CSPs which may be questionable for any kind of interruption in the dependency chain can result to several problems.

1.6.5 Legal dimension

SLA has not been taken as an important term for forensic investigations due to international regulations, CSP'S transparency and customer awareness. Cross border law, as well as the Multi-jurisdictional, affect the trials of the legal dimension in the cloud environment

1.7. Discussions in Fog Computing Forensics

Numerical forensics has been identified as science applied to the examination, identification, collection and data description during the conserving strict chain data storage and retaining the data integrity. Cloud forensic is defined [30] as cross-discipline amid digital forensics and cloud computing meaning that cloud forensics can be viewed as digital forensics request in the cloud environment in other words we could give the definition of fog forensics as numerical forensics application in a particular fog environment [10].

1.8 Comparison between Fog forensics and Cloud forensics

Here we are going to discuss more of fog forensics and cloud forensics as well as IoT and fog forensics and before stating that, we give a comparison of cloud amid fog forensics and to find the similarities and the differences among the challenges [31]. For we have known that fog computing means cloud computing, which is the extensions to the device's network. Nevertheless, digital forensics application in the environment has been given the meaning by cloud forensics and fog forensics and that the differences between the two are that the solutions in fog forensics are based on the differences amid fog and cloud computing. For the large bandwidth trial in a cloud environment will be solved in the Fog environment due to the big numbers of nodes and sensors, which makes fog computing free the bandwidth limitation [31]. Consequently, fog computing gives localization, which might help alleviate cloud legal challenges for examples, cross border issue among others.

1.9 Original Particle Swarm Optimization (PSO)

This algorithm initializes a group of entities with random locations, calculates their individual location-based fitness values and then searches for the entity with optimal fitness value of the group, which can be called the global best value. Another optimal fitness value that each entity keeps track of is the best fitness value the node has had so far, which can be called the local best value [7]. After the two optimal values are calculated

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for all entities, their positions are updated with the following equations [2]:

$$\begin{cases} \vec{v}_i^{(t)} = \vec{v}_i^{(t-1)} + \varphi_1(p_l - \vec{x}_i^{(t-1)}) + \varphi_2(p_g - \vec{x}_i^{(t-1)}) \\ x_i^{(t)} = x_i^{(t-1)} + \vec{v}_i^{(t)} \end{cases}$$

..... (1)

.....(2)

Where X is the position of the current entity being analyzed, Pl is the position of the entity with the local best fitness value, Pg is the position of the entity with the global best fitness value, I is the current dimension being analyzed, t is the current iteration and phi1 and phi2 are learning factors (usually 0 to 1) and user-defined) [73]. Depending on the situation the algorithm is applied to, the user can either define the number of iterations to run the algorithm for or the required optimal value to attain.

2. Literature of Surveys

With the comparison and summarization of the twelve surveys based on digital forensics as well as the comparisons include: Result visualization, the pros and cons, challenges, cloud forensics, collecting evidence solutions, tools and methods of digital APT, analysis techniques, future advanced, detection, digital forensic, Yara rules using digital forensics, PSO algorithms, and cyber-crime investigation. The comparison results is presented as a relation between the research and the methods used in the research with a check mark as shown in table 2. Every cloud forensic step has various challenges with solutions that can mitigate the challenges. As well as providing the solution to the problems by Rani D. et al. in 2016 as well as the solutions for collecting the snapshots in the Eucalyptus cloud and effective proposed framework for cloud forensics [32]. Ambreen R et al. in 2016 Proposes on the new model that is based on the large data analysis, which might take out the data from a source variety detecting future attacks. Divided in to four sections; live triage, post-mortem Triage, mobile device triage, and triage tools, the survey shows a number of findings [33] , and also by juices V. et al. in 2107 shows that the developers will still find it complex during the creation of methods for digital triage to keep pace with the development of new technologies [34].

In addition, Published literature has been reviewed widely by joseph et al. in 2016 to analyze the challenges that exist within the domain of digital forensics starting from the increasing data volumes to the changing technology platforms and systems. It is understandable that lack of effective evidence data acquisition approach having gone through several kinds of literature, due to technology diversity, their deployment platforms and lack of effective models to process huge data volume to analyze are limiting key factors in this domain. Also, the current forensic models identify cyber-crime and focus on domain challenges [35]. Rana et al. in 2017 Investigated various cybercrimes have followed by different digital forensics processes included in the cybercrime investigation. Further several tools with detailed explanation are discussed with their pros, cons, challenges, and drawbacks. Among all the selected tools, a comparison also presented. Lastly, the paper suggested the training programs needs for the first respondent and signature judgment based on the image authentication [36].

Table 2: literature survey analysis

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Methods / Survey Researches	Challenges	cloud forensics	solutions	Collecting evidence	analysis techniques	future Advanced	APT	methods and tools of digital	Result visualization	pros and cons	detection	digital forensic	Yara rules using in digital forensic	PSO algorithms Using in digital forensic	Cyber-crime Investigation
Rani D. et al,(2016)	√	√		√								√			
Ambreen R. et al. ,(2016)					√	√	√				√	√			
Jusas V. et al.,(2017)	√		√			√		√				√			
JOSEPH A. et al. ,(2016)	√				√			√				√			√
Rana N. et al. ,(2016)	√		√	√		√		√		√		√			√
Lanh T. et al. , (2007)								√			√	√			
Jetunmobi A. et al. ,(2016)						√		√		√		√			
Dezfoli F. et al. ,(2013)						√						√			
Jayamagarajothi M et al. ,(2017)								√				√			
Sun J. et al. ,(2015)			√	√	√							√			√
Naresh S. et al. , (2017)		√	√									√			

However, Lanh T. et al. in 2007 researchers have helped introduce major processing stages inside a digital camera and then review for the source of digital camera identification and forgery detection. During forgery detections, the method is to check the change in image color or appearance which may help gather important evidence, source identification of current approaches scout the many processing stages to originate the thread for distinguishing the cameras tampering sourcing. [37].

Jetunmobi A. et al. in 2016 reviewed certain various digital forensic paradigm - the Digital Forensic Research Workshop (DFRWS) paradigm, Reith's

Digital Forensic Model, Thus, they explored the forensic investigative model's evolutions, their pros, and cons, when being considered by highlighting new paradigms and approaches [38]. Furthermore, the Dezefholi F. et al. in 2013 review served as a foundation to develop a viable and working digital forensic investigative paradigm that will integrate the Chain of Custody role (CoC) [39].

Furthermore, Jayamagarajothi M. and Murugeswar P. in 2017, having an analysis of the current trends of digital forensics apps and security helps to understand and provide a rough estimate of future outlooks in the area [40]. On the other hand, Sun J. et al. in 2015 reviewed the different data mining approaches and digital forensics approaches and methods for Intrusion Detection and Protection System (IDPs). This effective cause detection of both normal and malicious events in the network, to develop a secure information system [41]. However, Naresh S., and Singh H. in 2017 they collected the researches of investigation procedure of cybercrime, and they explored every procedure features by introducing the research investigation procedure. Furthermore, they compared it through the traditional investigative procedures compatibility, cybercrime behavior analysis, testimony forensic procedures, case analysis and verification, the approach of evidence analysis and collection. Lastly, proposed the cybercrime investigation viewpoints and procedures of forensic. In addition, [42] discussed the fundamental of cloud computing, the emerging area of cloud forensics, features and highlights its opportunities and challenges.

In table 2 the checkmark describes a process in digital forensic tool used in researches and as shown in figure 2 we can notice that several types of research have discussed the challenges, cloud forensics, solutions, evidence, the analysis techniques, future advance, APT, methods and tools, Pros,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Detection, Digital forensics, and Cybercrime investigation. With digital forensics and method and tools were the most discussed topics. But no one of the researchers has discussed the use of PSO algorithm in digital forensics or Yara rules or result visualization in digital forensics.

Through the study of research related to digital evidence and the study of methods used in the investigation and collection of digital evidence and where the proposed method was not mentioned previously or used in the investigation and collection of digital evidence.

The proposed method is considered unique because it deals with ambient environment and other ways of dealing at the network level.

The proposed method deals with APT attack attacks in a two-sided manner. The first side identifies the detection and the second side analyzes the behavior of the spread, while the other methods focus on the less dangerous attack than the APT attack and one side in the investigation. .

As well as through the number of researches published for this type of investigation and collection of digital evidence, while the other methods contain many and many researches that mimic the methods used (traditional).

Which I am looking for is by finding an algorithm in which to develop an algorithm called (IDF-PSO) is able to deal with APT attacks in the ambient environment in identifying and detecting these attacks and collecting digital evidence to investigate and study the behavior of the spread of these attacks to places of data damage within the environment.

"APT only attacks an industrial data such as a missile organization or reactors or things very sensitive and is only important to spy on it and stole information artificial intelligence" even to be detected from the protection systems.

(IDF-PSO) is able to deal with APT attacks in the ambient environment in identifying and detecting these attacks and collecting digital evidence to investigate and study the behavior of the spread of these attacks to places of data damage within the environment.

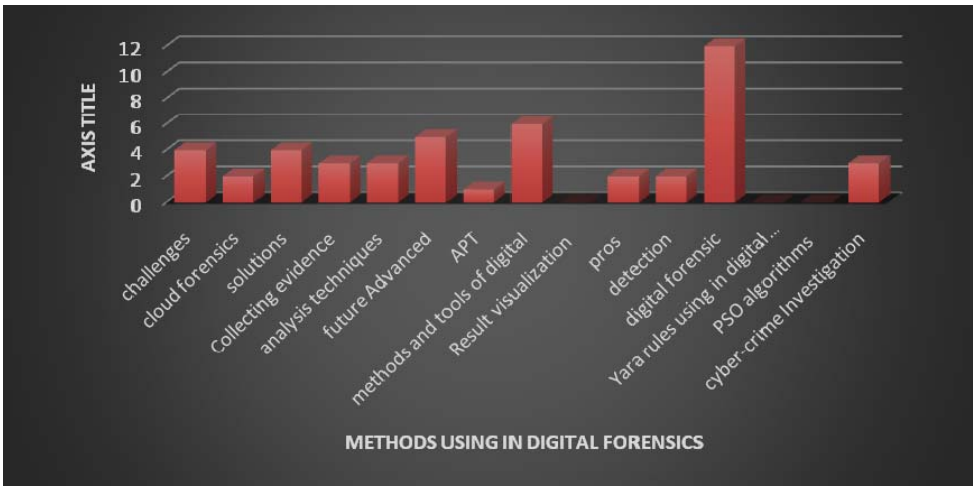

Figure 2: visualization chart of the analysis of the survey

3. Investigation of Digital forensics methods

Many methods have been used by researchers in digital forensics a review of the most common techniques will be discussed in this section; UdayakumarN N.et al in 2015 proposed routes for machine learning-based malware classification and detection. They performed a regular investigation that is useful as a base for any examination inside the field of malware examination with machine learning procedures [43]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Alkhateeb E. in 2017 proposed a productive, unique malware-location method dependent on API similarity. The proposed strategy outperforms the conventional signature-based detection technique. The investigation was assessed 197 malware tests. The results indicated promising after-effects of effectively-recognized malware. The researcher performed an experiment of 100 malware and 100 amiable programs. That was gathered from various sources and used to break down under various adaptations of Windows machines. The results tests outcomes had shown that it is relatively difficult to identify malware by just utilizing one apparatus. However, utilizing static and dynamic analysis tools together expanded exactness and the identification rate. The test outcomes also demonstrated that dynamic malware investigation tools outperformed static examination devices [44]. Further More, ASLAN Ö et al., in 2017 described an automatic system that can arrange a file as contaminated dependent on the dynamic conduct of the document saw inside a controlled, checked condition. The researchers had trained a support vector machine classifier that can be additionally used to recognize malicious documents [45]. Moreover, Cab˘au G., et al, in 2016 analyzed the classifier performance dependent on the heuristics of the crude runtime data created by master frameworks and gives rules of the choice process during information managing . The researchers proposed a classifier that picks up proactively, and it can recognize inconspicuous malware, regardless of the various malware families [46]. On the other hand, Choi J. And Choi C. in 2015 proposed a strategy that can identified method that use the malicious code in order to distinguish APT attack depending on its behavior ontology that happens. It utilizes insightful APT attack rather than characterizing the derivation tenets that can be gathered about the malicious attack [47].

Malware depends on the greatest part on the mark-based system. Darshan S. et al in 2018 while proposing a procedure which can distinguish malware depending on pre featured signature which gives a compliment on poor execution when trying to instruct concealed malware with the capacity to avoid recognition utilizing dissimilar code muddling methods. The sandbox environment helps in breaking down malware progressive as well as stopping its development for it gives disengaged situation in investigating malware conduct towards the final point of malware. During its execution the researchers will be able to use cuckoo sandbox framework which assists in stopping its spread in the system and therefore it gets protected from the destruction through varieties of calls and this gathered calls are organized by NGrams which assist in constructing classifier by the utilization of Information Gain (IG) which is a component choice method [48]. However, study that was performed by Firdausi L. et al., in 2010Sparse vector for machine learning is another study which was performed by the illustrator where the classifiers utilized in his work such as Naïve Bayes, J48 Decision tree, K nearest neighbors, support vector machine (SVM) and also Multi-layer perception (MLP). Consequently the explanatory and the tests of the five classifiers was accomplished by j48 having a review of 95.9% with a 2.4% false-positive rate, the precision rate stood ar 96.8% and the exactness outcome was 96.8 % [49].

Therefore depending on conduct based malware utilization and the investigation of the machine the learning system could be able to distinguish the malware proficiently and successfully for malware tests in a virtual machine sandbox Fowler J. in 2016 built a scheme which was meant for lossless of the memory dumps and therefore packing dump memory independently. Fowler benefited from memory dump which came benchmark virtual machine condition as well as the code for the pattern memory [50]. Gandotra E. et al. 2017 The model that is proposed as well is approved on demonstrable corpus of malicious since its outcome demonstrates the dynamic and the static which is considered as given high precision which recognizes the malware that is parallel from element applicable determination as well as the clean ones and thus enhancing model building period and getting rid of bargaining malware exact identification framework. Fluffy c-implies and memory investigation research depend on the advanced introductory group and without its impact of the virtual machine in the cloud, the classifier will be in a position to determine if malware or not [51]. However, in 2016, Ge L. et al. proposed the technique can defeat the deficiency of highlight

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

checking innovation which couldn't perceive obscure Trojans altogether for enhancing the discovery speed since it doesn't have to unload, decode, and other complex activities. The experimental results demonstrated that the location strategy has great precision [52].

On the other hand, Guri M.; et al in 2014 proposed another strategy to detect and arrange anti-forensic to measurable behavior, by contrasting the logs of the presume program between various conditions. The introduced technique is basically noninvasive (does not meddle with unique program stream). They independently follow the stream of directions (Opcode) and the stream of Input-Output activities (IO). The two measurements (Opcode and IO) supplement each other to give a solid arrangement. The technique can recognize part conduct of suspected programs without earlier information with a particular enemy of forensic technique; moreover, it calms the malware examiner from dreary well-ordered review [53]. Furthermore, Hu W. and Tan Y. , in 2017 analyzed the power of four surely understood machine learning-based malware location approaches, such as the DLL and API, including the string highlight, PE-Miner and the byte level N-Gram. They proposed two falsification approaches under which malware that can bypass the detection algorithm. Experimental results demonstrated that the exhibitions of these recognition calculations decay incredibly under the falsification approaches. Although the absence of power makes these calculations unfit to be utilized in true applications [54].

In 2016 Imran M. et al. proposed a malware arrangement plot dependent on Hidden Markov Models utilizing framework calls as watched images. This methodology joins the incredible statistical pattern analysis ability of Hidden Markov Models with the demonstrated limit of framework calls as segregating dynamic highlights for countering malware muddling. Further, testing the proposed procedure on framework call logs of genuine malware demonstrates that it has the capability of viably ordering obscure malware into known classes [55], another research performed by Jain A. And Singh A. in 2018 proposed a solution where they removed chosen features from the static and dynamic analysis techniques. A coordinated methodology has been produced with the goal that the arrangement and detection rate may enhance static and dynamic methodology. They broke down malware outfitted with hostile to get better arrangement and recognition result. The outcome demonstrates an exactness of 73.47% utilizing the coordinated methodology, 69.72% utilizing static and 63.30% utilizing dynamic investigation. Looking at the static and dynamic methodology, the incorporated methodology gives better precision [56]. In the other side of using the support vector machine (SVM) by Kruczkowski M., and Szynkiewicz E. In 2014, assessed the aftereffects of the utilization of SVM to risk information analysis to expand the effectiveness of malware location. Their outcome recommends that SVM is a strong and productive strategy that can be effectively used to heterogeneous web datasets order [57]. Furthermore, Li J. et al., 2014 proposed a framework that is used in the identification of Android malware. The framework comprises of four segments: movement observing, activity irregularity acknowledgment, reaction handling, and distributed storage. The framework parses the convention of information parcels and concentrates the component information; at that point, it utilizes the SVM classification algorithm for information arrangement [58].

However, Lu J. et al., in 2017, proposed a period approach for recognizing APT assaults depend on the perception in that the malicious payload should be exchanged [18]as well the utilized machine should recognize the APT attacks in a large data for it will distinguish the malicious payloads. Static as well as the dynamic will be able to gather the information Mangialardo R. And Duarte J. in 2015, for they utilize C 5.0 whereas the Random Forest Machine will execute inside FAMA to play I the features and the ID into numerous and classes classifications. It demonstrates in examination 95.75% for double grouping issue and 93.02% for the numerous [59]. However, Morioka E. and Sharbaf S., in 2016, the investigations that are created with all the experience is of preferred outcomes that are acquired by dynamics and statics separated dissects. Forensics issues in cloud computing do give conceivable arrangements as well as the rules which includes eliminating contextual investigations

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[60]

Also, Mthunzi S., in 2017 proposed a methodology that uses current procedures which concentrates on growing computational capabilities. It is a propelled cloudlet-based digital forensics (DF) that deals with supplementing existing distributed computing frameworks to fulfill this.

In view of their approach to end-devices and remote DF investigation teams, the suggested method successfully handles low dormancy issues with the cloud elective. Furthermore, I proposed a cloudlet-based DF asset system to deal with the ascending and descending scale of assets to adjust to a variety of information, numerous gadgets, and simultaneous diverse cases [61].

Otherwise, Nakagawa N. et al. in 2016 used an Open Flow technology for virtual networks; they developed a system of identifying infected terminals by detecting communication events of malware communications in APT attacks. In addition, they prevent information fraud by using Open Flow, which works as real-time path control. To evaluate their system, they executed malware infection experiments with a simulation tool for APT attacks and malware sample [62]. However, Narayanan B. et al. 2017, executed a Principal Component Analysis (PCA) strategy for the extraction. They considered the execution of different Artificial Neural Network (ANN) calculations alongside K-Nearest Neighbors (KNN) and Support Vector Machine (SVM) characterization procedures for distinguishing proof of malware information into their individual classes. They utilized k-fold validation to check the adequacy of methodology [63]. Furthermore, Pascariu C. And Barbu I. In 2017 aimed to create patterns of ordinary PC behavior and malicious PC conduct; which will be utilized to prepare a counterfeit neural network to alarm recently made procedures and consequently set up in the event that they are protected or can make hurt the PC and its information [64].

Pektaş A et al. in 2016, proposed another malware classification technique depending on the behavior of the malware. Its document, organize, exercises the malware tests that. It applies the machine-learning algorithm [65]; they used online machine learning calculations that can give immediate refresh about the new malware test by following the first experience with the grouping plan. To approve the adequacy and adaptability of the strategy, they assessed technique by utilizing 18,000 later malignant files. R. Pirscoveanu et al. in 2015 they built up a disseminated malware testing condition by expanding CuckooSandbox that was utilized to test a broad number of malware tests and follow their conduct information. The separated data was utilized for the advancement of a novel kind grouping approach dependent on managed machine learning. The proposed classification approach utilizes a novel mix of highlights that accomplishes a high characterization rate with a weighted normal AUC estimation of 0.98 utilizing random forests classifier. The methodology has been widely tried on a sum of 42,000 malware tests. In view of the above outcomes, it is trusted that the created framework can be utilized to the pre-channel novel from known malware in a future malware analysis system [66].

Qbeitah M., and Aldwairi M., 2018 managed dynamic malware analysis, on how the malware will carry on after execution, what changes to the working framework, what library and system correspondence happen. Whereas, Dynamic analysis opens up the entryways for programmed age of peculiarity and dynamic signatures depending on the new malware's conduct. The examination incorporated a plan of nectar pot to catch new malware and a total powerful investigation lab setting. They proposed a standard examination approach by setting up the examination instruments, at that point, running the pernicious examples in a controlled domain to research their conduct. They investigated 173 late Phishing messages and 45 SPIM messages in look for conceivably new malware, they displayed two malware tests and their powerful exhaustive examination [67]. In 2017 Qiao Y.et al.studied behaviors are characterized by programming propensities and extricated from the parallel examples by static analysis. In view of the API call practices, the homologous level of various malware is l kg utilizing Jaccard similitude coefficient. At that point, the homology is recognized by contrasting the homologous degree and a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

limit. Exploratory assessments on certifiable examples demonstrate that this technique accomplishes high exactness rate and adequate review rate [68].

ZHAO G., and XU K. in 2015 Suggested a novel framework to discover APT malware viruses that depend on destructive DNS activities. The framework uses harmful DNS analysis systems to discover dubious APT malware and C&C areas. Hence, after it studies the movement of the suspicious IP using the signature-based and peculiarity-based identification methods. The framework depends on huge information that explains the different properties of malware-related DNS. It favored system activity that can identify the traffic of traded off customers which have been remotely controlled. The framework experiment included 400 million DNS queries [69]. However, Yan W. in 2012 Efficient and quick strategy does obtain a correlation signature from suspending malware folks for the cloud-based fatty frameworks which are at the core of CAS which is cross malware inquiry and large scale for the CAS uses a novel technique that is Advanced Persistent Threats where the big scale shows that CAS does recognize a bigger number
of malware tests where malware affiliation marks at inline haste. The malware advanced includes more of non-PE malware, contents malware as well as portable malware which describe a clue for a safety investigation framework (SIF) assist in the investigation and also the outlining of multi companies APTs [70]. Besides, Ussath M.et.a.l in 2015 the system uses distinctive data sources, similar to log documents, and points out areas of interest from the legal studies and malware investigations, in order to give a comprehensive plan for the distinctive phases of an advance. SIF strives to enhance the effectiveness of studies and reveal undetected complex elements of an advance [71].

A summary of researches that use different methods, approaches, algorithms in Digital forensics is described in figure 3. However the analysis and statistics of these methods are shown; which had the analysis many of researches and the statistics about them regarding what is the most used technique and what is the technique that need to be more studied in digital forensic There are tools and algorithms that may be very useful and efficient in forensic analysis that has not been used and studied by any researcher and this inspired us to do this research about these effective methods.

As shown in figure 3 that the most used techniques in digital forensics and detection and response APT attack were in machine learning techniques followed by analysis techniques then detection. Followed be malware. However, as we can see that the PSO, elastic and Kebana and Fog computing has not been studied by any of the researchers in the sample that was selected.

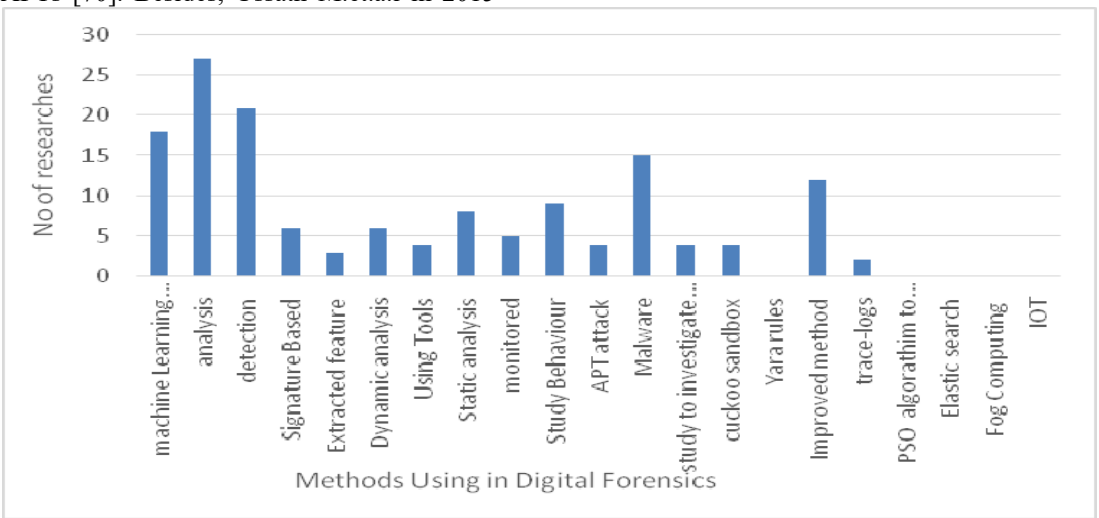

Figure 3: The Statistics of the Number of Methods Using in Digital Forensics

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. PROPOSED METHOD

To design and implement enhanced PSO algorithm for detection of APT attacks infection and studying its spreading behavior in FOG environment, in other words, this study aims at developing a new approach to Integrate Cyber Threat Intelligence with Digital Forensics analysis in a proactive security approach.

Through the review section we shall realize the importance and effectiveness of PSO, However it has some shortcomings which provide us the motivation to propose an optimized method.

The disadvantages of particle swarm optimization (PSO) algorithm are that it is easy to fall into local optimum in high-dimensional space and has a low convergence rate in the iterative process. To deal with these problems, an adaptive particle swarm optimization algorithm based on a directed weighted complex FOG computing environment is proposed. Particles can be scattered uniformly over the search space by using the topology of the small-world network to initialize the particle's position.

At the same time, an evolutionary mechanism of the directed Agents in PSO Algorithm is employed to make the particles evolve to enhanced to detect APT attack which will do guarantee an optimal solution is ever found in collection digital evidence to detection and classification APT attack and Study of propagation behavior

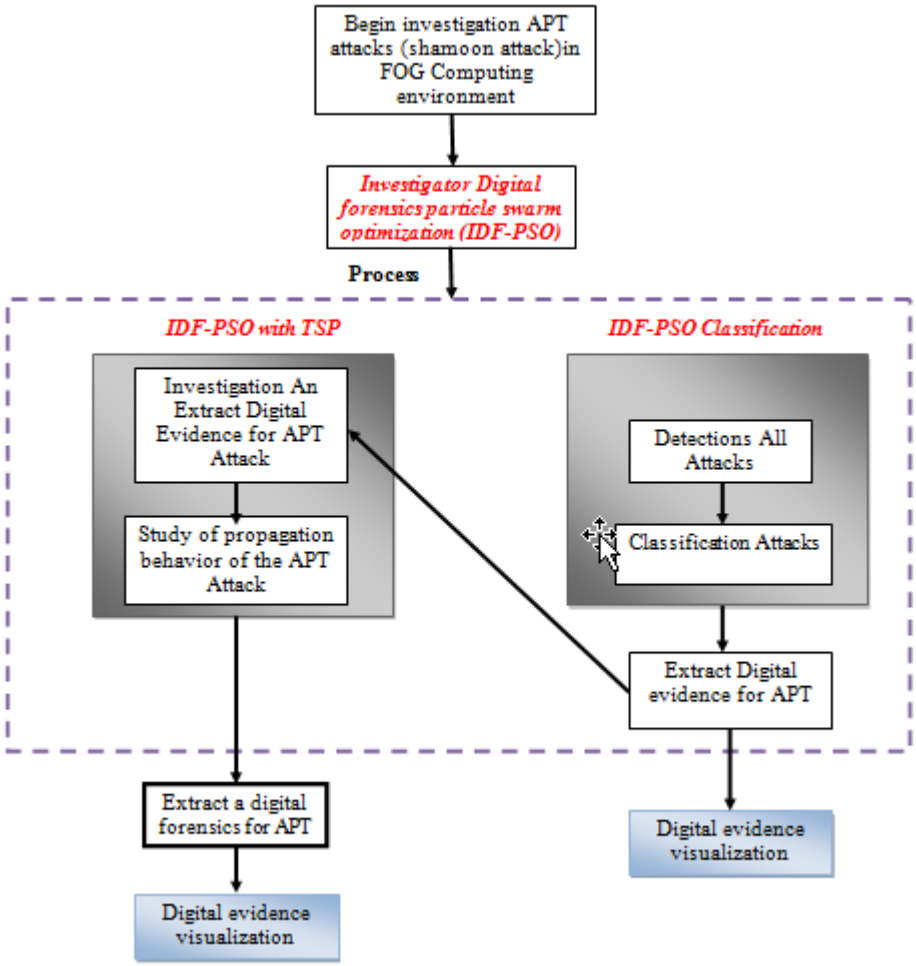

Figure4: steps of the study in detection infection APT Attacks and response in FOG

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We are willing to achieve the proposed method by effectively perform (APT attack) detection and identification and analysis of the behavior of its spread to develop an inverse in the collection of data source using artificial intelligence methods.
Improved mechanism is proposed using Parallel (HYBRID) as illustrated in figure 4, to exploit the time detection, determination and analysis of APT propagation behavior to save time and exploit the search for the largest possible space in the edges within the cloud.

In the beginning, we note that we use the Advanced Digital Forensics Swarm Optimization (IDF-FPSO) algorithm to investigate and collect digital evidence by identifying and detecting APT attacks and analyzing their propagation behavior within Fog Computing Nodes in two ways:
First: - Identify and detect APT attacks and distinguish them from other attacks through the use of (classification IDF-PSO).
Second: When identifying and detecting that these attacks are due to the APT attack, their propagation behavior will be analyzed using IDF-PSO with TSP in the foggy environment.
TSP = Traveling salesman problem

Thirdly the results of the investigation will be presented to collect digital evidence and the results of the propagation behavior of the APT attack.

Here the process will be used real simulation test (real life test) as illustrated in figure 5.

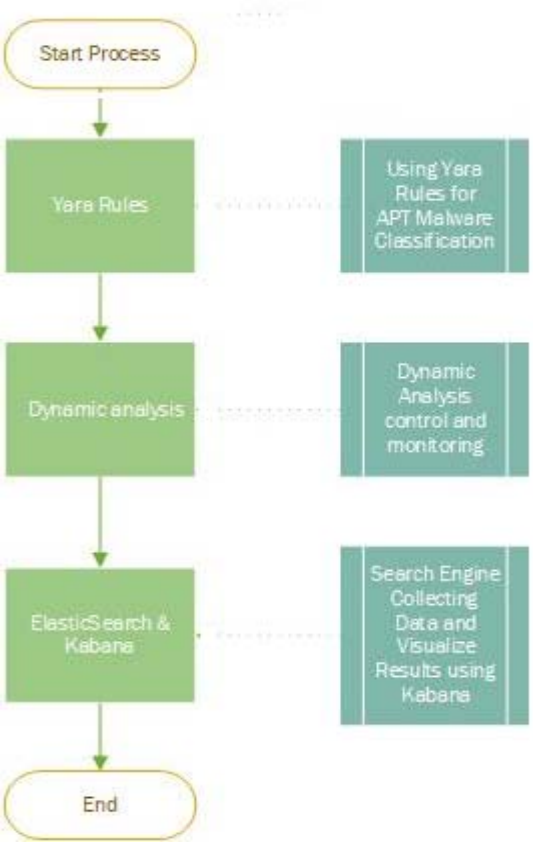

Figure5: Experimental practical steps (real life).

Where we are in this part when identifying and detect attacks APT attck will be analyzed by the beginning of the yara rule We know that yara rule is a statement of rules containing signutures of different types of attacks and used to classify the type of attack and its seriousness by knowing the signatures of the attack

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The second phase:
The APT attack will be analyzed through dynamic analysis through which we will examine the movement of packets to identify the source of attacks and locations of target data hits.
The Third Trip
In the process of analysis we use (kabanah) to analyze the attacks of APT we need to isolate the environment from the investigation of the other devices used to protect the other devices from injury as well as isolating the environment for the investigation process to monitor packets of the source knowledge attacks and places targeted data.

Finally, in the third phase the results will be presented in a precise analysis by Elastic search.

The proposed study has the following goals:
To design and implement enhanced PSO algorithm (IDF-PSO) for detection of APT attacks infection and studying its spreading behavior in FOG environment, in other words, this study aims at developing a new approach to Integrate Cyber Threat Intelligence with Digital Forensics analysis in a proactive security approach.

- To apply Yara-rules classifier in APT using a sample of Shamoon Data set Malware
- To Enhance Dynamic Analysis (detection and mentoring) over FOG infrastructure.
- To enhance elastic search kibana data visualization results
- To integrate Security Orchestration and Automation Response (SOAR) Solutions with featured Fog Nodes. And improve Incident Response cybersecurity operations.
- To identify the malicious insider and reduce the amount of stolen information with espionage attacks in Fog nodes.
- To enhance forensic analysis over Fog Nodes (Memory analysis & Bit Stream Imaging)

The proposed method has some advantages and they are:

1. Early detection of APT attacks in the cloud environment prior to their arrival in the cloud environment
2. Proper exploitation of Meta Heuristic in the cloud environment.
3. Utilizing methods to analyze the prevalence behavior of APT attacks.
4. Examine the data type affected by the APT attack.
5. Quick response in the initial ability to investigate and collect evidence for those APT attacks in the ambient environment.

5. SUMMARY AND FINDINGS

This survey discusses the Cloud computing technology is used in big enterprises and by the end-user. Then it discusses the Fog computing that has been raised to be a technology tool to protect the cloud environment where it reduces the delay in cloud computing, and it solves the security problems. Whereas Cloud computing became trending technology. It consists of distributed and the parallel system it had many security problems that have been solved by Fog computing. The survey then discussed the APT Attack and clarify that the primary reason the APT is successful is that it is another risk that numerous organization is not set up to deal with. While a portion of the APT assaults is robotized, then it discusses the APTs attacks classifying .then it describes the analysis of the incident response of APT attack reports in the Middle East.
The survey shows the effect of surveillance in industries and Shamoon Industrial Espionage. Cloud forensic is a critic progression that helps in achieving the cloud model as well as rebuilding the past cloud computing functions which give numerical evidence. However, it gives the difficulties of digital forensics and cloud computing in three-dimension that is the legal aspect, technical dimension and organizational. Fog forensics in other case is shown as a science that is applied to examination, collections, identifications, and even data analysis which retains the data, the preservation of strict chain data storage and the integrity. There is a vivid data when giving a conclusion about cloud and fog forensics and one of the primary differences is the solutions in fog forensics which gives differences amid fog computing and cloud computing. Fog forensics gives localization that is vital in initiating fewer challenges in cloud legal challenges, for instance, cross border issues. Besides, we can easily conclude the problem of logging and the chain of dependency in fog forensics.
The survey also provided a summary of the literature of Surveys, and we concluded that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

several types of research had discussed challenges, cloud forensics, solutions, evidence, the analysis techniques, future advance, APT, methods and tools, Pros, Detection, Digital forensics, and Cybercrime investigation. With digital forensics and method and tools were the most discussed topics. But no one of the researchers has discussed the use of PSO algorithm in digital forensics or Yara rules or result visualization in digital forensics

Finally the survey discussed the related work and summarize the researches whereas we have shown that the analysis of many researches and the statistics about them regarding what is the most used technique and what is the technique that need to be more studied in digital forensic There are tools and algorithms that may be very useful and efficient in forensic analysis that has not been used and studied by any researcher and this inspired us to do this research about these effective methods.

We concluded that the most used techniques in digital forensics and detection and response APT attack were in machine learning techniques followed by analysis techniques then detection. Followed be malware; however, as we can see that the PSO, elastic and Kebana and Fog computing has not been studied by any of the researchers in the sample that was selected. Since using PSO in digital forensics have not been used by any of the researchers as well as the data results in visualization and Yara rules and Fog computing in digital forensics we propose an enhanced method for digital forensics investigation under the APT in the fog environment of industrial espionage. The work will help in detecting and responding to APT espionage attacks and by studying the behavior of these attacks in order to improve digital forensics analysis and enhance result visualization in a fog computing environment and

REFERENCES

[1]. Osanaiye O., Choo K.-K.R., Dlodlo M., (2016), "Distributed denial of service (DDoS) resilience in the cloud: review and conceptual cloud DDoS mitigation framework", J. Network Comput. Appl.Vol., No. 67, PP. 147–165.

[2]. Khan, A., & Gill, N. S. (2018). Review of Security Methods in Cloud Computing. *IJRAR-International Journal of Research and Analytical Reviews*, 5(3), 1076-1080.

[3]. Sasikala, P. (2013), "Research challenges and potential green technological applications in cloud computing." International Journal of Cloud Computing, Vol.2, No. 1, pp. 1-19, 2013.

[4]. Shanhe Yi, Zijiang Hao, Zhengrui Qin, and Qun Li, (2015), "Fog Computing: Platform and Applications", Dept. Of Computer Science, College of William and Mary, IEEE.

[5]. Saharan K. and Kumar A., (2015), " Fog in Comparison to Cloud: A Survey", International Journal of Computer Applications, Vo. 122, No.3, PP.10-12

[6]. Ibrahim M., (2016), "Octopus: An Edge-Fog Mutual Authentication Scheme", International Journal of Network Security, Vol.18, No.6, PP.1089-1101.

[7]. Fakeeh K., (2014), "Privacy and Security Problems in Fog Computing", Communications on Applied Electronics, Vol.4, N.6 PP.1-6.

[8]. Khan S., Parkinson S., and Qin Y. , (2017), "Fog computing security: a review of current applications and security solutions", Journal of Cloud Computing: Advances, Systems, and Applications, Vol.6, N.19, PP.1-22.

[9]. Kumar H., Shinde S., and Talele P., (2017)," Secure Fog Computing System using Emoticon Technique", International Journal on Recent and Innovation Trends in Computing and Communication, Vol 5 Issue: 7, PP.801-808.

[10]. Mukherjee M., Matam R., Shu L., Maglaras L., Ferrag M., Choudhury N., and Kumar V.,(2017), "Security and Privacy in Fog Computing: Challenges", Access IEEE, vol. 5, pp. 19293-19304.

[11]. Kumar G. and Kavitha S., (2017), "A Survey on Security and Privacy Issues In Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 7, PP.13348-13352

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[12]. Zhao G.; Xu K.; Xu L. and WuB.,(2015),” Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis”, IEEE Journals & Magazines, Vol.3, PP.1132 – 1142.

[13].Rot A. and Olszewski B., (2017), " Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection ", Position papers of the Federated Conference on Computer Science and Information Systems, Vol.12, PP. 113–117.

[14].Brandon, J.,(2013), " Adobe data breach highlights the company’s security shortcomings", experts say.

[15].Nurit G., Yaron G., Ehud G., (2013), "Mining meaningful and rare roles from web application usage patterns", Computers & Security, Vol. 82, pp. 296-313

[16]. Singh J., Pasquier T., Bacon J., Ko H., and Eyers D., (2016),” Twenty security considerations for cloud-supported Internet of Things”, IEEE Internet of Things Journal Vol. 3, Issue: 3 .PP.1-16.

[17].Kaynar K. and Sivrikaya, F., (2016), "Distributed attack graph generation". IEEE Trans. Dependable Secure. Comput., Vol. 13, PP. 519–532.

[18].Lu J.; Zhang X. ; Junfeng W.; Lingyun Y. ,(2017), “APT Traffic Detection Based on time transform”, International Conference on Intelligent Transportation, Big Data & Smart City, Changsha, China, 17-18 Dec. 2016, PP.10-13.

[19].Herløw L. and Hansen S., (2015), " Detection and Prevention of Advanced Persistent Threats", published Master Dissertation, but computing, Kongens Lyngby, Denmark.

[20].Semantic, (2018), "Advanced Persistent Threats: A Symantec Perspective", https://www.symantec.com

[21].Passeri P., (2018), " June 2018 Cyber Attacks Statistics", Hackmageddon Information Security Timelines and Statistic, https://www.hackmageddon.com/2018/07/23/june-2018-cyber-attacks-statistics

[22].Glitz A. and Meyersson E., (2017), " Industrial Espionage and Productivity", IZA – Institute of Labor Economics, No. 10816, PP.1-44.

[23] Berendt, B., Büchler, M., & Rockwell, G. (2015). Is it research or is it spying? Thinking-through ethics in big data AI and other knowledge sciences. *KI-Künstliche Intelligenz*, *29*(2), 223-232.

[24]. Morrissey, K. M., Yuraszeck, T. M., Li, C. C., Zhang, Y., & Kasichayanula, S. (2016). Immunotherapy and novel combinations in oncology: current landscape, challenges, and opportunities. *Clinical and translational science*, *9*(2), 89-104.

[25].Alelyani S. and Kumar H., (2018), " Overview of Cyberattack on Saudi Organizations ", Published by Naif Arab University for Security Sciences, Vol. 1, Issue 1,pp.42-50.

[26] Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2015, April). Cloud forensics: a review of challenges, solutions and open problems. In 2015 International Conference on Cloud Computing (ICCC) (pp. 1-9). IEEE.

[27].Zawoad S., Hasan R., and Skjellum A, ",(2015) OCF: an open cloud forensics model for reliable digital forensics. In Cloud Computing (CLOUD) ", IEEE 8th International Conference o, pp. 437-444.

[28] Rajasekaran, S., Ni, Z., Chawla, H. S., Shah, N., Wood, T., & Berger, E. (2016). Scalable cloud security via asynchronous virtual machine introspection. In 8th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 16).

[29].Pichan A., Lazarescu M. and Soh S., (2015), " Cloud forensics: Technical challenges, solutions, and comparative analysis ", Digital Investigation Elsevier, Vol. 13, PP. 38-57.

[30].Wang Y. , Uehara T. and Sasaki R., (2015), " Fog Computing: Issues and Challenges in Security and Forensics ", IEEE 39th Annual Computer Software and Applications Conference, Taichung, Taiwan.

[31].Mouradian C., Naboulsi D., Yangui S., Glitho R., Morrow M., and Polakos P.,(2018),

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges", Communications Surveys & Tutorials IEEE, vol. 20, no. 1, pp. 416-464.

[32].Rani D., Sultana S., and Sravani P., (2016)," Challenges of Digital Forensics in Cloud Computing Environment", Indian Journal of Science and Technology, Vol 9, No.17, PP.1-7.

[33].Ambreen R.., Dubey S. and Nadeem S., (2016), "review of apt attacks: how big data fights back", international journal of engineering sciences & research technology, Vol.5, No.9, PP.385-389.

[34].Jusas V., Birvinskas D, and Gahramanov E., (2017), "Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions", Symmetry Journal, VOL.9, No.49, PP.1-20.

[35].Joseph A. And Singh K., (2016), "A Survey On Latest Trends And Challenges In Cyber Forensics", International Journal Of Advances In Electronics And Computer Science, PP.75-78.

[36].Rana N., Sansanwal G., Khatter K. and Singh S., (2016), "Taxonomy of Digital Forensics: Investigation Tools and Challenges", Computers and Society.

[37] Mahmood, T., Nawaz, T., Ashraf, R., Shah, M., Khan, Z., Irtaza, A., & Mehmood, Z. (2015, December). A survey on block based copy move image forgery detection techniques. In 2015 International Conference on Emerging Technologies (ICET) (pp. 1-6). IEEE.

[38] Jetunmobi A., Rukayat A., Uwadia, Charles O., and, Florence A., (2016)," A Survey and Critique of Digital Forensic Investigative Models", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12, PP.496-508.

[39] Zafar, F., Khan, A., Malik, S. U. R., Ahmed, M., Anjum, A., Khan, M. I., ... & Jamil, F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. Computers & Security, 65, 29-49.

[40].Jayamagarajothi M. and Murugeswar P., (2017), "A Survey on Data Mining and Digital ForensicsTechniques for Intrusion Detection and Protection System", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, PP.159-164.

[41].Sun J., Shih M., and Hwang M., (2015), "A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure", International Journal of Network Security, Vol.17, No.5, PP.497-509.

[42].Naresh S. and Singh H., (2017), "Digital Forensic: Issues and Challenges in Cloud Computing Environment", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.10, PP. 67-73

[43].Udayakumar N., Anandaselvi S., And Subbulakshmi T,(2017),” Dynamic Malware Analysis Using Machine Learning Algorithm”, Proceedings of the International Conference on Intelligent Sustainable Systems, Palladam, India 7-8 December 2017, pp 795-800.

[44].Alkhateeb E., (2017),” Dynamic Malware Detection using API Similarity”, IEEE International Conference on Computer and Information Technology, PP. 297-301.

[45].Aslan Ö. and Samet R., (2017), “Investigation Of Possibilities To Detect Malware Using Existing Tools” Ieee/Acs 14th International Conference On Computer Systems And Applications, Pp.1277-1284.

[46].Cab˘au G., Buhu M., And Opris¸a C., (2016),” Malware Classification Based on Dynamic Behavior”, 18th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania 24-27 Sept. 2016, PP. 316-318.

[47] Choi J. And Choi C., (2015),” Ontology-based APT Attack Behavior Analysis in Cloud Computing”, 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications, Krakow, Poland 4-6 Nov. 2015, PP.375-379

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[48].Darshan S., Kumara A., and Jaidhar C., (2018)," Windows Malware Detection Based on Cuckoo Sandbox Generated Report Using Machine Learning Algorithm" 2016 11th International Conference on Industrial and Information Systems (ICES), Roorkee, India, 3-4 Dec. 2016, PP.534-539.

[49] Mohaisen, A., Alrawi, O., & Mohaisen, M. (2015). Amal: High-fidelity, behavior-based automated malware analysis and classification. computers & security, 52, 251-266.

[50] Fowler J., (2016), "Delta Encoding of Virtual-Machine Memory in the Dynamic Analysis of Malware", 2016 Data Compression Conference (DCC), Snowbird, UT, USA, 30 March-1 April 2016, PP.592.

[51].Gandotra E.; Bansal D. And Sofat S.,(2017), " Zero-day malware detection", 2016 Sixth International Symposium on Embedded Computing and System Design (ISED), Patna, India, 15-17 Dec. 2016, PP.171-175.

[52].Ge L.; Wang L. And Xu L., (2016)," An APT Trojans Detection Method for Cloud Computing Based on Memory Analysis and FCM", 2016 3rd International Conference on Information Science and Control Engineering, Beijing, China, 8-10 July 2016, PP.179-183.

[53].Guri M.; Kedma G.; Sela T.; Carmeli B.; Rosner A. and Noninvasive Y., (2014)," detection of anti-forensic malware", 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE), Fajardo, PR, USA, 22-24 Oct. 2013, PP.1-10.

[54].Hu, W. and Tan Y. , (2017), "On the Robustness of Machine Learning-Based Malware Detection Algorithms", 2017 International Joint Conference on Neural Networks (IJCNN), 14-19 May 2017, PP.1435-1441.

[55].Imran M.; Afzal M. And Qadir M., (2016), "Using Hidden Markov Model for Dynamic MalwareAnalysis: First Impressions", 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, 15-17 Aug. 2015, PP.816-821.

[56].Jain A. And Singh A., (2018)," Integrated Malware Analysis Using Machine Learning", 2017 2nd International Conference on Telecommunication and Networks (TEL-NET 2017), Noida, India, 10-11.

[57].Kruczkowski M. And Szynkiewicz E., (2014)," Support Vector Machine for malware analysis and classification", 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT), WarsawPoland, 11-14 Aug. 2014, PP.415-420.

[58].Li J.; Zhai L.; Zhang X. And Quan D., (2014), "Research of Android Malware Detection Based on Network Traffic Monitoring", 2014 9th IEEE Conference on Industrial Electronics and Applications, Hangzhou, China, 23 October 2014, PP.1740-1744.

[59].Mangialardo R. And Duarte J., (2015)," Integrating Static and Dynamic Malware Analysis Using Machine Learning", IEEE Latin America Transactions, Vol. 13, Issue .9, PP. 3080 – 3087.

[60].Morioka, E. And. Sharbaf S.,(2016)," Digital Forensics Research on Cloud Computing: An investigation of Cloud Forensics Solutions", 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 10-11 May 2016,

[61].Mthunzi S., Benkhelifa E., Jararweh Y. and Al-Ayyoub M.,(2017), "Cloudlet Solution for Digital Forensic Investigation of Multiple Cases of Multiple Devices", 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, Spain, 8-11 May 2017, PP.235-240.

[62].Nakagawa N.; Teshigawara Y.and Sasaki R., (2016), "Development of a Detection and Responding System for Malware Communications by Using OpenFlow and Its Evaluation", 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec),

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Jakarta, Indonesia, 29-31 Oct. 2015, PP.47-51.

[63].Narayanan B., Boundjou O., and Kebede T., (2017), "Performance Analysis of Machine Learning and Pattern Recognition Algorithms for Malware Classification", 2016 IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS) Dayton, OH, the USA, 25-29 July 2016, PP.338-342.

[64].Pascal C. And Barbu I., (2017), "Dynamic analysis of malware using artificial neural networks Applying machine learning to identify malicious behavior based on parent process hierarchy, 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Romania, 29 June-1 July 2017.

[65].Pektaş A.; Acarman T.; Falcone Y. And Fernandez J., (2016), "Runtime-Behavior Based Malware Classification Using Online Machine Learning", 2015 World Congress on Internet Security (WorldCat), Dublin, Ireland, 19-21 Oct. 2015, PP.166-171.

[66].Pirscoveanu R.; Hansen S.; Larsen T.; Stevanovic M. And Peders J.,(2015), "Analysis of Malware behavior: Type classification using machine learning", 2015 International Conference on Cyber Situational Awareness, Data Analytics, and Assessment (CyberSA), London, UK, 8-9 June 2015.

[67].Qbeitah M., and Aldwairi M., (2018), "Dynamic Malware Analysis of Phishing Emails", 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 3-5 April 2018.

[68].Qiao Y. ; Yun X. And Zhang Y. , (2017), "How to Automatically Identify the Homology of Different Malware?", 2016 IEEE TrustCom/BigDataSE/ISPA , Tianjin, China, 23-26 Aug. 2016.

[69]. Zhao G. And Xu K., (2015), "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis", SPECIAL SECTION ON BIG DATA FOR GREEN COMMUNICATIONS AND COMPUTING, VOL3, PP. 1132 – 1142

[70] Sun, H., Wang, X., Buyya, R., & Su, J. (2017). CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices. Software: Practice and Experience, 47(3), 421-441.

[71].Ussath M.; Cheng F. And Meinel C., (2015)" Concept for a Security Investigation Framework", 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 27-29 July 2015.

[72] Sun, W., Lin, A., Yu, H., Liang, Q., & Wu, G. (2017). All-dimension neighborhood based particle swarm optimization with randomly selected neighbors. Information Sciences, 405, 141-156.

[73] Abbassi, R., Abbassi, A., Heidari, A. A., & Mirjalili, S. (2019). An efficient salp swarm-inspired algorithm for parameters identification of photovoltaic cell models. Energy conversion and management, 179, 362-372.

[74] Yara in a nutshell," [Online]. Available: https://plusvic.github.io/yara/. [Accessed 24 November 2018]