How to Cite:
Supriya, N., Vidyasri, P., Shivaprasad, S., Murali, G., & Kumari, M. K. (2022). IoT for analyzing and investigating digital forensics tools using cloud computing. *International Journal of Health Sciences*, *6*(S3), 1934–1955. https://doi.org/10.53730/ijhs.v6nS3.5903

IOT for analyzing and investigating digital forensics tools using cloud computing

N. Supriya
Associate Professor, Department of Computer Science and Engineering, Malla Reddy Engineering College (A), Hyderabad, Telangana

P. Vidyasri
Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram Campus, Chennai

S. Shivaprasad
Professor, Department of Computer Science and Engineering (data science), Malla Reddy Engineering College, Secunderabad

Gudipati Murali
Professor, Department of Computer Science and Engineering, KKR & KSR Institute of Technology and Science, Guntur, Andhrapradesh

Matta Krishna Kumari
Assistant Professor, Department of Computer Science and Engineering, VFSTR (Deemed to be University), Guntur, Andhra Pradesh

***Abstract*---**One of these articles examines how cloud computing affects standard digital proof methodologies and offers some suggestions on how to improve digital proof reviews in the cloud. As Cloud-Computing gains traction as an IT business solution, it is attracting the attention of an increasing number of companies as a viable migrations path for their IT infrastructures and business strategy. The criminal's element among has made aware of the centralization of data stored in clouds. Then Data Centers and Clouds Service providers are becoming targeted for assault. Inside the coming years, implementing a Forensics-as-a-Service (FaaS) solution may be the only viable option, but until it is consented upon as a guideline and executed by service suppliers, participants are completely reliant on clients receiving a few assurances in their service level agreements to allow the retrieval of users and the systems logs on supply.

***Keywords*---**forensics-as-a-service, cloud computing, virtualization storage management, security, business model.

International Journal of Health Sciences ISSN 2550-6978 E-ISSN 2550-696X © 2022.
***Corresponding author**: Supriya, N.*
Manuscript submitted: 18 Nov 2021, Manuscript revised: 09 Feb 2022, Accepted for publication: 27 March 2022

Introduction

As seen by the rise in the global acceptance of the products it delivers, clouds computing is a constantly developing technology solution and business plan. Although clouds computing has roots in mainframes computing which has some parallels to regular Webhosting, the manner services are rendered differs significantly. Self-provisioning, automatic scaling, & pay-per-use are some of the added features that cloud consumers may get from offerings that improve reliability, efficiency, and adaptability [1-3]. In this sense, cloud computing may be viewed as a step in the evolution in the providing of Online services, helping corporations to simply outsource their IT needs while only charging for the services they utilize. CSPs like that as Google, Amazon, & Microsoft were pushing growth by converting their surplus capacity into such a commercial pay-per-use framework that includes ephemeral and flexible IT services [4]. This present development is also aided by internet providers' increased provision of high-speed internet & low-cost accessibility.

Its Cloud's seemingly limitless availability of unidentified computing power might be a fertile ground for just a new generation of cybercrime. A large amount of sensitive data is kept on the Clouds, including such credit cards and security numbers, making it a potential target for criminals. Additionally, everyone, even offenders, has accessibility to enormous computational resources, which provides easy-to-use encryptions technology & anonymized communications routes, making it less likely that their operations would be understandable to or monitored by officials [5]. Denial of service (DoS) assaults, for instance, was shown utilizing the Clouds as the weapon of choice. The testing was performed out as some kind of test basis for a customer's networks that used a $6 handmade "Thunder Clap" software, and the investigators utilized up to 10 virtual servers on Amazon's EC2 to conduct the assault, successfully knocking its customers firm off the Web. The invasion was undetected by Amazon during the test, and the study discovered nothing whatsoever to halt them from attempting to launch the invasion. The malware that orchestrated the assault was activated by a directive posted on a social media platform.

Regarding the possibility for this kind of Cloud-based offense, it's indeed clear that a collection of exhaustively admissible Cloud-specific methods and technologies is necessary. Because there are now no such instruments or techniques, existing forensic approaches might well be modified to operate with Cloud storage [6]. Existing digital evidence approaches, on the other hand, are primarily designed for off-line research, assuming that stored medium undergoing examination is entirely underneath the inspector's custody. Such approaches do not transfer well to Cloud-computing settings, posing several data gathering problems. Although cloud computing provides clients with versatile, rapid, on-demand, & cost-effective IT solutions, it alters the conventional features of data storage and retrieval [7]. Proof in the Clouds could be stored in many geographic regions on systems provided by different clients and controlled by a variety of Clouds Service Providers, rendering the collection of evidence complicated. This poses the dilemma of how to maintain the credibility and trustworthiness of information proof obtained from the Clouds for it to be utilized in a legal proceeding.

Related works

As part of a researcher’s effort named CLOIDFIN, Biggs and colleagues explored the influence of cloud computing on digital forensic inquiries. These authors recommend a global collaboration that includes fundamental modifications needed inquiries to be successful in cloud computing architecture [8]. Our researchers also proposed that cloud providers suppliers guarantee that regulations are followed and also that non-compliance is avoided. The writers, nevertheless, could not offer a specific answer to the challenge of preserving digital investigative proof in a cloud-computing context. In [9], we presented a methodology for archiving data for healthcare experts including hospitals. That method concentrates on the Amazon encryption technique for preservation & backup and restore, and only covers a small number of security concerns. The article, in an instance, presents backups and restore strategies that almost all clouds service suppliers offer. As a result, it's unclear how this approach, which concentrates on storing information from clinical services providers, can provide a universal solution that can assist investigators in non-medical electronic forensic investigation studies.

These researchers of [10] address the difficulties associated with clouds forensics. The study looks at how cloud-computing services may be used to perform a conventional digital inquiry. These authors admit that the results acquired via virtual machines (VMs) throughout various clouds deployment methods might vary substantially. The article suggests strategies tailored to individual companies. This paper proposed snapshots study copying for IaaS systems, for instance. These researchers also propose alternatives depending on several use scenarios, including SLA testing, detailed review, and the destruction of evidential information, among many others. This difficulty is that if all cloud service providers are obliged to duplicate digital objects, methods like forensic image copying might not have been feasible. This results in a considerable increase in the quantity of clouds storage needed [11].

Moreover, case-by-case research doesn't aid in the development of an effective strategy for assaults utilizing cloud computing services. Whereas computer evidence in cloud technology is an attractive research area, previous research has aimed at identifying the obstacles of conducting electronic examinations in the clouds. There seems to be little study into providing models or remedies that might tackle the inherent weaknesses in computer forensic retention at the cloud services layer. Almost majority of the new study has been on computer storage consistency or protection & security systems [12]. The problems become increasingly apparent with the emergence of the Internet of Things (IoT), which heavily relies on the clouds computing environment, therefore solutions that might theoretically overcome the issue for both perspectives are needed.

The field of digital forensics with IoT systems and mechanisms is still in its infancy. Nevertheless, numerous academics have sought to solve concerns connected collect information in IoT in distinct attempts. Data collecting and analysis methodologies, and possible research areas for improving digital forensics for the IoT ecosystems, were discussed in [13]. The report includes crucial forensic evidence that may be retrieved through existing IoT connected phones including Amazon Echo, Z-Wave sensors, and static routing. The study, though, somehow doesn't solve any problems for general-purpose IoT platforms and applications. This article, for instance, consists of specific equipment. Regrettably, most of those previous restricted scientific studies adopt a reactive instead of an aggressive strategy to digital forensics [14]. That example, determining the condition of an IoT system is exceedingly difficult if it defects. It would be wonderful if there was a system that took into account IoT platform tracking so that this data could be utilized as forensics evidence.

It's important to understand how computer evidence & cloud technology are established before attempting to describe Forensic investigations. Describe data processing as the application of empirically obtained and procedures ensure to the retention, gathering, verification, recognition, assessment, explanation, recordkeeping, and the processing of data available in digital sources to enable or promote the rebuilding of street crimes, or assisting in the prediction of unauthorized behavior that interrupts planning performance [15-16]. Cloud computing, thus according to NIST 2011, is a paradigm for willingness to contribute and participate, easy, on-demand networking access to a shared pool of customizable computational resources that can be swiftly provided and delivered with minimum administrative activity or service provider involvement [17]. In this respect, Clouds forensics can be defined as the application of accurate estimates for the conserving, gathering, verification, proof of identity, analysis, perception, paperwork, and data presentation obtained from computing environments in a somewhat way that the evidence's authenticity is preserved and probative in a legal proceeding.

Materials and Methods

This description given to the generalized procedures that offer a structure about which sounds forensic examinations could be built is network investigations learning theories. Though there are no universal forensics standard techniques that might be applied to all electronic forensic evidence, the procedure for each kind of offense seems to have some characteristics [18]. Because of the global nature of the modeling techniques, they may be used in a wide range of digital crimes investigations, regardless of technologies. Concerning a well-known investigative procedure, this study explores the contrasts among conventional & Digital forensics investigations. This Continental Spafford design is used for comparative reasons. Several stages of a digital forensics process are listed throughout this paradigm, which is also referred to as the Integration Of information Research Method: conservation, assessment, searching and gathering, reconstructing, & presenting.

Inside a typical digital forensic investigation, this conservation step includes protecting the digital scene's entrances, and maintaining any forensic information that may alter [19]. Separating the systems from the networking, gathering volatile data which would be destroyed if the machine was shut off, & detecting any suspect programs operating on the machine are all part of this procedure. Suspicious individuals must be identified and perhaps examined if they are registered. Logging data are regarded as eyewitnesses to the event and therefore should be protected when they're at risk of disappearing before the systems are cloned [20]. Direct physical retention in Clouds inquiries is confined to the accused's computer if one is accessible. Because the data is kept externally on virtual images, no further direct retention is feasible. Investigative groups could unintentionally protect information to the Clouds by serving conservation requests to the internet services. Forensic detectives should, nevertheless, have faith in the services supplier's ability to retain information in a digital forensics way utilizing tried and true procedures.

This objective of the Surveying phase is to find the evident sources of evidence & form a first explanation about what happened. Vulnerable proof, including such volatile memory storage, is recorded & gathered as quickly as possible to avoid harm or distortion. In a server infiltration scenario, Carrier and Spafford say the crime scene investigators would seek clear evidence of a rootkit deployment, examine applications records, and search for new system settings [21]. Although the system could be checked for proof, the investigators wouldn't have accessibility to any more data because internet services cannot be physically viewed. If and how possible evidence might be found will be determined by the Cloud storage type employed.

Apart from restricted user-specific applications customization options, the consumer seems to not influence the underlying architecture, including the operating systems, apps, or servers, inside the SaaS model. Throughout this case, an investigating officer has no incredibly simple means of determining substantiation on the webserver and must also be reliant on any application programming log data sent out by the service supplier; that's only conceivable if the network operator had also assembled a few forms of logging framework and tends to make the audit trails accessible, whether permanently or temporarily [22]. In regards to recognizable proof, the IaaS framework offers so much to an investigator. That consumer has great power out over the configuration of the imaginary example, and also the underpinning operating systems, inside an IoT ecosystem [23]. As a result, consumers have the option of installing logging technology to monitor user behavior, which may substantially increase the performance of a forensic analysis; nonetheless, this is not the usual. Despite this, forensics experts have had more accessibility to proof than that of the other 2 Clouds storage types, SaaS and PaaS.

This PaaS paradigm allows customers to design and install applications that used the company's computer languages, frameworks, capabilities, and resources. The customer has no access to the underlying Clouds infrastructure, such as the networking, servers, software platforms, or memory, but it does have influence well over installed apps and perhaps the application-hosting atmosphere's configuration options. Because they are confined to a certain log file, assuming such occur, this one has a terrible impact on an inspector's capacity to locate probable proof. This evidence from the crime scene's Exploration and Collecting Phase includes a detailed examination of the systems for electronic information. These findings of the Surveys Step are used in this stage to emphasize other sorts of research. For instance, once phrases are found from that other information, a search strategy may be done on this stage, or a low-level chronology of actively interacting can be examined to retrace a user's behavior. This is where the majority of the investigative time has been spent. Relics of evidential significance are gathered, generally, from computer storage media including such hard disks, memory chips drive, or other electronic content. This process of gathering such information entails making investigative image copies of these media devices, which may then be analyzed in a forensics laboratory. Data saved in volatile memory or active registry is retrieved using other techniques. So most examinations are carried out on a community scale, except certain networking forensics analyses, which may have been carried out now to look for prior occurrences in internet traffic archives.

This same Cloud's dispersed architecture creates new problems for investigative data gathering. Because data on the Cloud is distributed, forensics investigators must update their old methodologies to adapt to this new context. Additionally, researchers should understand how information is kept in the Clouds environment and, as a result, how it may be accessed whilst preserving data. Because contact here between the customer and the Cloud service is mostly through the Web, proof could be obtained locally from the client's Internet browsers history. Additional information, including such customer usernames and passwords for Clouds computing and text messaging, could be retrieved and decoded, allowing the investigators insight into the client's prior Internet interactions. Because network operators do not offer any system logs from the networking devices utilized either by patient's installations or programs, it is typically not essential to evaluate internet traffic at the system levels. If indeed the service offering is IaaS on the web servers side, forensics experts can take images of the virtual environment & examine these offsite in a laboratory just like any other data captured from a local computer.

Using PaaS, the issue is more complicated since the only knowledge accessible is application-specific statistics. The investigator could only get minimal data via SaaS, including such user-specific program setup parameters. Because the network operator would give the information for the investigation, the investigators would need to work more closely with both the service providers to grab information in a forensically sound manner. The service supplier is served with a court order, which allows them to conduct the investigation, gather the information, and provide it over to the investigators. That researcher should believe the honesty of the expert given by the CSP to investigate an enhanced safety, which necessitates a high level of confidence. Consumers should also have faith in the specialist's data gathering devices and software, and the Clouds infrastructure's right to receive, reconstruct, and deliver information. The authenticity and consistency of the collected information as admissible proof would be called into question if the proper documentation is disrupted at any point.

This physically criminal investigations reconstructing step includes arranging the analytical findings from the acquired traditional and cyber facts and developing an explanation for the occurrence utilizing the scene of crimes images. The proof is combined with scientific techniques to evaluate the occurrence hypotheses. This rebuilding step for the electronic event entails connecting the dots of the electronic puzzle altogether. That stage processes data is necessary complex analysis methods, including such appropriate file analytical or decoding, and summarize the information. That stage employs empirical tests to assess and refute ideas based on computer information, and to determine how and why the facts came to be. If digital forensics has still been lacking, the Searching Stage might well be restarted to find new proof.

When it comes to cloud-based incident investigations, the network operator has complete control over the quantity of data provided to the investigators that might make it difficult to recreate prior occurrences. Furthermore, owing to the physiological asymmetry of the information, placing it in the appropriate perspective and the proper chronological sequence might be a challenging process. That problem is aggravated by the fact because information stored in multiple geographic locations with multiple time zones might also have timestamp discrepancies owing to improperly synced computers timers, which would be a major problem for rebuilding event histories. Such problems might lead to incompletely digital artifacts, which could also jeopardize their reliability as court evidence.

Overall findings of the examination of all print and digital evidentiary artifacts are recorded and given to a court or administration during the development of the conceptual framework of a typical forensics inquiry. This presenting step includes investigators' findings, briefings, relevant paperwork, statements, witness statements, and court transcripts. The paperwork that supports each stage of the inquiry is very important since it creates traceable integrity of the evidence. Proof information should stay constant throughout any forensics investigation, and detectives must be capable of presenting their results, describing the significance and ramifications of all activities. Additionally, rigorous documentation and recordings for all stages of the inquiry must be preserved. In a Clouds examination, keeping such a tight record of the inquiry may be problematic, because data might well be kept in many places underneath various restrictions, rendering the collection of evidence difficult to manage.

Summary

Whenever submitted to a judge, the shortcomings of Clouds investigations along the different steps of the forensics procedure outlined above might call into doubt the evidence's legitimacy. To summarise, these are:

- Incapability to maintain a possible criminal case, which might also compromise the information artifacts' authenticity.
- This refusal or incapacity of service suppliers to give required information, including program or networking system logs.
- Restricted or no accessibility to archived data might result in a skewed view of the past.
- Partial information, including such fragmentary information or artifacts with changed information.

Challenges in cloud computing

Additional difficulties with performing digital forensics investigations in the clouds might influence the strength of the data collected, which would in return undermine the artifacts' trustworthiness in a legal proceeding. That study explores these difficulties and recommendations made for how to fix them in the part that follows. Multiple customers can share the same physical servers and access benefits offered by shared Cloud-computing hardwares and software at the same time thanks to multi-tenancy. Multi-tenant architectures might be concerning in some situations since they share a lot of resources, reveal a lot of potential susceptible connections, and therefore can happen on a huge scale. Throughout aspects of the investigation process, one such resource-sharing climate presents difficulties because forensic experts must consider not only the assistance used by an individual client, and yet also non-customer particular aspects of the multi-tenant facilities, and assets communicated with some other clients. Elements including such memory locations and CPU utilization are examples of common infrastructure. Network operators, for instance, will be hesitant to grant access to the available storage because it would most certainly require information about other consumers, violating privacy & confidentiality contracts.

Digital preservation is critical to the effectiveness of online forensics inquiries because it preserves the provenance and processing histories of datasets. An information object's lineage could reveal who developed and updated its information, making it a crucial part of any computer forensics inquiry. The amount of information authenticity that can be provided in the Clouds is determined by the Clouds model. The lineage of a data element in a SaaS Clouds solution, for instance, might well be hard to track because the network operator typically does not authenticate users to applications programming event logs. This same client has no way of knowing whether information has been disclosed or obtained by the adversaries in the event of an accounts penetration. That involves information that has been changed or perhaps even destroyed by a hostile external customer or by the service supplier, for instance, for added storage.

To offer back-ups & encourage higher automatic failover, cloud infrastructure is frequently dispersed across many sites, which may include various nations. This, nevertheless, brings up the question of sovereignty, which could also cause issues for the law enforcement community when attempting to create the trustworthiness of electronic information as proof. As per Garrie, a judge could only hold a hearing if it has authority out over participants and the case's actual content, but law enforcement authorities could only operate inside their permitted areas. If indeed the information is stored in another nation, this poses an issue. Various nationalities have distinct anonymity and privacy regulations, which might differ significantly from one country to the next. Some nations, for instance, have strong rules governing the privacy of financial records, and breaching such restrictions might lead to criminal repercussions. In this situation, retrieving all of the information necessary to solve a crime might well be impossible.

Throughout a digital forensics process, establishing the integrity of the evidence is standard practice, and it helps in providing a recorded human history of the inquiry, documenting how the information was gathered, processed, and stored so that it may be submitted as proof. The traceability commences when such an investigator maintains the environment and concludes whenever the information is submitted in judgment or to administration in a typical investigative inquiry.

Maintaining a positive chain of custody in Cloud-computing settings is more difficult than obtaining evidence physically because of the distant dynamics of the process. Proof should be acquired from distant computers in a verified & sensible manner in able to be submitted as factual information in Clouds examinations. In most cases, when prosecutors will be unable to obtain complete control of Cloud-based operations, authorities would have to depend on the network supplier's personnel to produce investigative reproductions of proof. The prosecutors must guarantee that the chain of custody is just not disrupted in this instance so that information proof from either the Clouds (gathered from third-party companies) may be submitted truthfully.

Present Service Level Agreements (SLAs), which govern the user agreements between the network operator and the Clouds client, usually never include measures for investigation process and data retrieval from the Clouds. Definite conditions are expected to install the regulations for the investigative collection of substantiation from of the Web, including such permission provided by the CSP to the consumer for forensic examination and provisos about how inquests are protected including both multi-jurisdictional and multi-tenant climates in form of regulatory laws, the secrecy of customer information, and security practices both in multi-jurisdictional and multi-tenant climates. With publics Cloud-computing, non-negotiable services agreements whereby the terms & conditions are fully dictated by the Clouds providers are currently the standard. In this situation, the client has little or no say with what the CSP is allowed to reveal in the instance of a clouds security incident. Finally, it is the customer's responsibility to establish an appropriate SLA with both the CSP which addresses any difficulties regarding retrieving proof from the Internet, including such various jurisdictions, information protection, including establishing a trustworthy provenance.

Proposed Method

Every one of the positively known methods could only be deployed in clouds environments, and researchers should rely on CSP for forensics data gathering. To address these issues, the proposed method is deployed beyond the internet. After gaining authorization from the International Telecommunications Unions (ITU) the proposed approach solves the data collecting concerns described by establishing a centralized forensics server and a forensics overlay dubbed Forensics Monitor Planes (FMP) just outside of the public Clouds. As a result, the researchers will not need to rely on the CSP to gather information. Figure 1 indicates the typical clouds forensics paradigm, which includes the addition of an FMP and forensics servers to improve clouds forensics. The forensic work instrument, including the Forensic Toolkit (FTK) diagnostics, E-Detection, that also runs in the background of the FMP, monitors all arrivals and departures interconnection in a clouds environment, and the monitoring data, is forensically replicated (i.e. bit by bit flow cryptography) and kept in a different evidence collection servers on the cyberattacks venue. The forensics tool also keeps track of how clouds service models behave. On clouds service model that combines VM, the toolkit captures a detailed examination of the present incarnation and saves it in dedicated investigations servers.

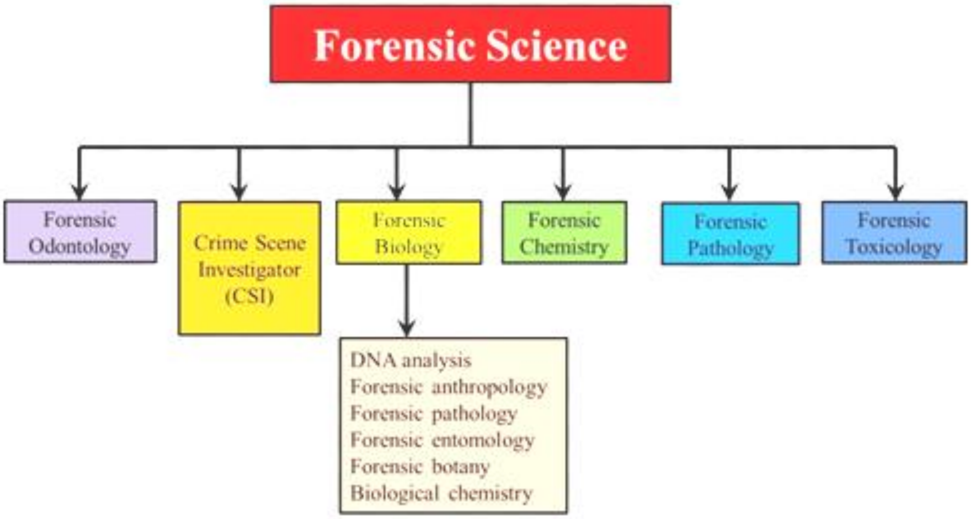


Figure 1. Proposed model

As a result, if such an incident occurs, all activities, including internet traffic in the particular clouds, were forensically photographed, or the demand handled in the clouds is collected, encoded, and kept in the forensics servers to reduce the trustworthiness of CSP. Because bit-by-bit streams imaging is done throughout the forensics computer vision applications, the meticulously photographed data remains unmodified. The forensic images recorded are not raw data and could only be analyzed using investigative software. Networking records are also collected from nearby network elements (gateways) and stored on a forensics database, providing strong evidence for identifying the intruder. Inside the instance of harmful behavior, the researcher could use their usernames and passwords to enter into the investigative computer and obtain evidence in the case within such a specified time limit. However, if indeed the researcher has reason to suspect something, he or she might acquire information from CSP and compare it to the information acquired from the investigative servers. In the case of an unexpected occurrence, forensics tools are operating in the forensics servers, but it captures the forensics image of the forensics computer, as there is a risk that a suspected would log in as a forensics expert and interfere with the information. A sequencing diagram illustrates the sequence of operations in our proposed approach in Fig. 2 for deeper understanding.

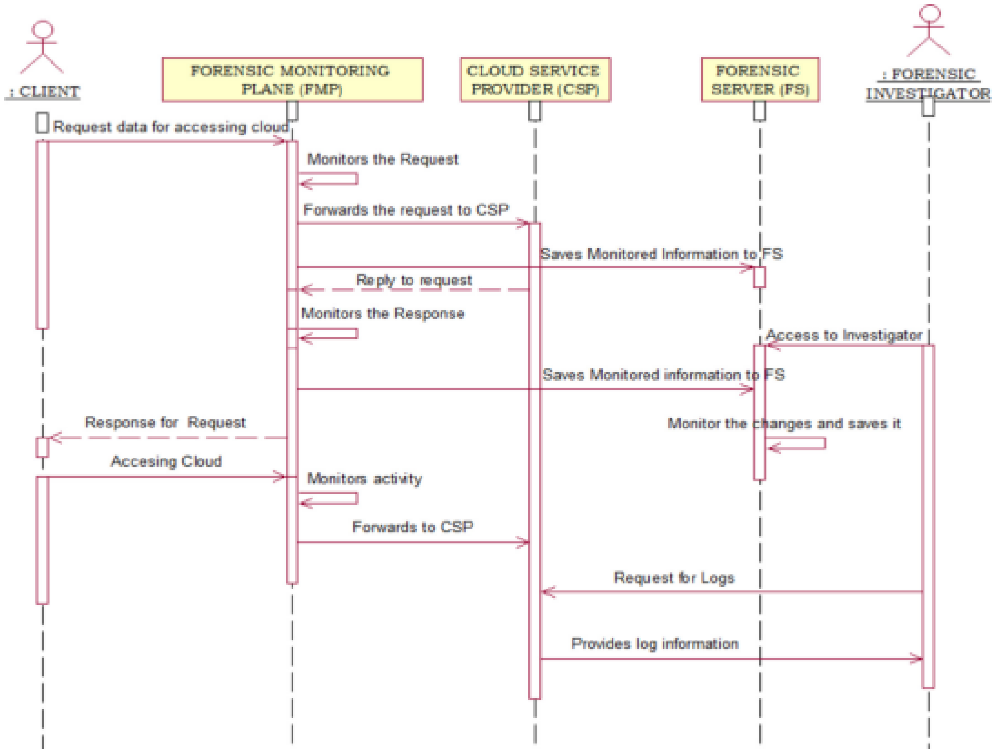


Figure 2. Model sequence

Resolve in cloud forensics

There seem to be numerous unsolved difficulties with performing electronic examinations on the Clouds, which have been worsened by the Cloud's volatile, ever-changing character. These sections aim to provide some solutions to some of the problems that arise during Clouds studies. There seem to be presently no cloud-specific toolkits accessible, therefore researchers must mix existing investigative tools and applications meant for offsite investigations. An assessment of present tools for acquiring evidence from Clouds settings would reveal any flaws, allowing new or modified methods to be created. Technologies may be created, for instance, to undertake forensics real-time assessment in the Cloud's dynamic environments. In so many situations, real evaluation provides useful information about the operating systems that statistical evaluation cannot, including such resource and register monitoring, but there are no comprehensive solutions for the Clouds. Some other important finding of the study may be the creation of databases that can be utilized as test-beds enabling instrument development. Testing ground statistics is critical for instrument development, yet there are presently no databases that reflect Clouds incidents.

In that instance, technologies may be created to undertake investigative real-time research in the Cloud's changing situation. In many situations, real research contains essential information that static analysis might give on the operating systems, such as allocation and registries monitoring, but there are currently no proper solutions for the Clouds. Some other interesting areas of research may be the creation of databases that can be utilized as test-beds for instrument evaluation. Testing ground information is essential for instrument development, however, there are presently no databases that reflect Clouds events.

This breakdown in communication about a Clouds offering's underlying architecture and processes makes an inquiry difficult. Although forensics experts may need knowledge on standard operating procedures as parts of an inquiry, network operators seldom disclose the systems in which client information is kept or handled. This lack of disclosure can indeed be warranted for a myriad of purposes, including sensitive information or the risk of disclosing underpinning infrastructures, which could expose a Clouds service to assault. Additionally, clouds service providers would not like to reveal organizational practices and systems since this information may be used by competition to better their products or perhaps even hurt the company's reputations.

[24] Cloud computing services must be held responsible to either the client and the supplier, unless both may verify that the Clouds is offering the services as promised. If an issue arises, individuals ought to be able to identify who is to blame and demonstrate the issue's existence to a 3rd party, including arbitration or a court. One such concept could benefit both parties: the client will be able to verify that whether support rendered to customers is indeed being done properly, and the network operator would indeed be able to address complaints and issues more easily. SLAs should include clear and exact operational details on how a forensics examination will be conducted by both the investigation committee and the internet providers in the case of a legal occurrence of events in the Clouds are to be performed to the top class. Duties must be specified explicitly so that everyone understands their tasks, skills, and limits. In addition, the legal repercussions of undertaking an inquiry in several locations and multi-tenant settings must be considered. This CSP may facilitate investigative information gathering under a forensics-as-a-service (FaaS) paradigm. Because the supplier controls the architecture, companies may retain and gather data not just from the virtual environment but also through construction monitoring systems, network capturing, and billing information. Clients would be assured that an inquiry would be easy to conduct in the event of an incident if the CSP deployed such services with little changes to the current Clouds infrastructure.

Challenges with IoT forensics

Any collection of data saved on physical resources for the benefit of doing a comprehensive examination or analyzing network records is not included in computer forensics for cloud computing. This is attributable to the fact that so many cloud-based services are often spread over several virtualized environments and networking devices [25]. As a result, it's critical should network investigation methodologies account for internet computing's dispersed character and respond to altering the way applications and services are delivered to suit this stochastic nature. Furthermore, obtaining forensics evidence in a cloud infrastructure requires cooperation from the network operator, who may have been hesitant to disclose material or grant researchers entrance to their cloud-based settings. Even if network operators cooperate with investigators, cyber-attackers may delete or alter any evidence of a targeted act intentionally. Additionally, depending on the cloud system, handling network investigation data might change.

This forensic evidences process in SaaS and PaaS is mostly focused on the customer suppliers, but in IaaS, it includes both customers and network operators. It is feasible for customers to replicate or photograph virtual computers for the investigation process using an IaaS. Copying in SaaS and PaaS, on the other hand, might not have been practicable or viable [26]. Besides that, IoT computer evidence adds another element of sophistication based on a variety of considerations such as (a) the quantity of dispersed IoT nodes, (b) the variation in IoT devices technical requirements, (c) the position of encrypted information, and (d) the total absence of forensics evidence due to IoT devices CPU and communication restrictions.

Furthermore, in cloud-computing settings, allocations of resources may be automatically configured depending on the amount or demand (i.e. auto-scaling). As a result, tampering with or stealing a commodity in a cloud-computing environment is exceedingly tough. In an IoT environment, however, IoT devices might be manipulated with, lost, or stopped communicating. It's almost hard to detect or ascertain the present state of IoT devices after it goes offline [27]. Imagine an IoT security camera that works as a network's edge device, continually capturing and processing images for vulnerability scanning to demonstrate the relevance of this. Suppose that somehow this IoT gadget is connected to a cloud-based interface. Assuming the IoT devices have been hacked with and are unable to communicate. It's virtually hard to re-establish a connection with the gadget or figure out what's causing the problem [28]. With that kind of IoT device linked to clouds, it's easy to overlook or overlook the reasons that influence IoT devices to go offline.

IOTF: IoT forensic framework

Computational power is dispersed to the edges of the networks in fog computing environments. The fog computing method, in general, is a networking paradigm wherein storage and distribution capabilities are located near mobility and IoT devices at the edge of the networks. Fog performs several essential activities, including data preprocessing and aggregating. The fog computing approach provides several benefits to IoT networks, including increased scalability, lower network congestion, quicker response, and the possibility for enhanced confidentiality and protection. As a result, filtering traffics and information coming to IoT systems is beneficial. In the event of a cyber-attack or risk, such data can be utilized as digital proof [29]. Moreover, by including such fog layers, it'll become capable to find when an IoT system is failing and retrace its histories in a rather manner that it could mine the information held onsite to assess its condition or issue warnings in a scaled, productive, and appropriate manners.

Designers present the IOTF: IoT Forensics Toolkit to address several of the aforementioned issues. IOTF makes use of the fog computing model, which allows knowledge to be sent to the edges of the network via a bridge. This is appropriate for data-intensive IoT systems with a high amount of installed IoT nodes. In these kinds of circumstances, the fog nodes or gateways could be programmed with the knowledge to filter the information that needs to be transmitted. This file transfer among an IoT system and fog nodes or gateways may then be used to retrieve forensics evidence through IOTF. Such fog nodes, for instance, could record an IoT product's previous known position [30]. This architecture may access system logs connected with problematic equipment in the event of a failure. Whenever the IOTF's investigative engine analyses the information & detects a potentially dangerous action, this should alert additional connected technologies or networks. As a result, the danger does not spread to other IoT systems, and the cyber-ability suspect's influence on additional Internet of things systems is limited.

Considering the intelligent refrigerators as an IoT system, which was discussed previously. Each refrigerator is attached to fog nodes on the local area network that screens the information that needs to be processed or sent. Suppose this IoT gadget is a component of a connected home system that includes, amongst many other things, smart LEDs, clocks, doorways, webcams, and voice assistants. Imagine that perhaps the fog gateways are used to interconnect various IoT systems. Such fog gateways have built-in technology that detects any unusual behavior just on the LED's side. In this example, most of the LED's commands come from a recognized Android-based smartphone browsing, but one of the most recent queries came from an unidentified user agent. Throughout this example, IOTF examines the system logs and finds that perhaps the user-agent hasn't altered in the last 3 months [31]. The user-agent linked with the most recent requests, nevertheless, doesn't fit this trend or the enrollment record. When IOTF detects a cybersecurity breach, it alerts nearby IoT systems in the connected networks through a protocol like MQTT to cease wirelessly processing commands till further notification [32]. Throughout this approach, IOTF makes it necessary to eliminate preemptive strikes, make future assaults more difficult for the offender, identify an assault as early as feasible, and immediately neutralize the impacts of the attacks. Figure 3 depicts a high-level design perspective of the proposed system.

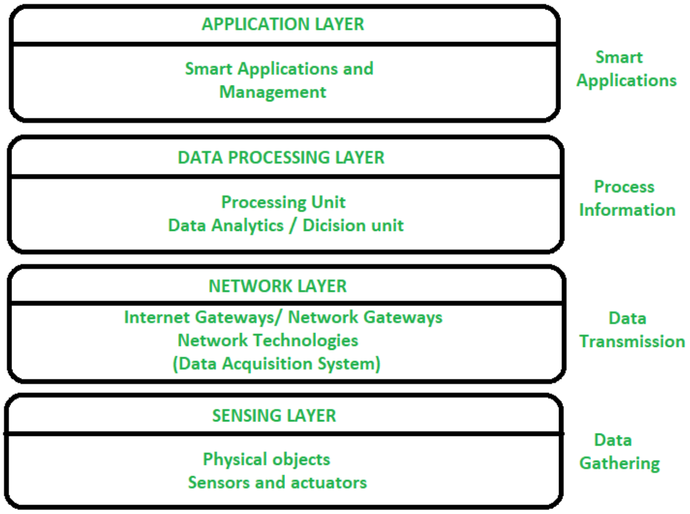


Figure 3. IOTF architecture

IOTF, as shown in Fig. 3, is some fog gateways (or nodes) that comprise of 6 components:

- Devices surveillance administrator,
- forensics analyzer,
- proof retrieval,
- incident reports,
- communications, and
- archiving

This communications module allows IOTF to connect with IoT devices in real-time. This communications module is in charge of correctly attaching IoT systems to the architecture and configuring the atmosphere in which they may transmit and receive information. This internal database (DB) is often used to keep track of all actions related to IoT devices connected with the frameworks. Every IoT system is assumed to have its unique identification. Every inbound and outbound communication among IoT systems plus external networks is recorded in the logging. The design of this log is comparable to that of available technologies for investigating networks traffic (e.g. tcpdump). It looks at traffic data to see whether there's anything suspicious going on, such as odd ports, IDs, or traffic volume, for instance. This forensics investigator starts gathering evidence for future inquiry if the surveillance administrator raises a signal of some questionable behavior. Suppose that many IoT systems are linked together with a designated specific port.

An inbound query to link to an odd port is acknowledged by the monitoring components. In this instance, the forensics analyst would raise suspicion, causing it to extract unstable information and put it in a constant position. According to how the system is set up or managed, this address might be locally or on the clouds. Furthermore, the forensics analyzer starts copying any information on the IoT nodes onto its internal memory. If a suspect behavior is detected by the forensics analyzer and it reaches an IoT system, the modules disable the machine and send reboot signals. This proof restoration component is in process of gathering & retrieving data from IoT systems that have been impacted. To put it another way, it produces a bit-stream image of all of the stored data on IoT systems. It also tries to figure out what activities are happening on the IoT system from afar.

This investigation reports module creates a statement after an IoT system has been evaluated to see if there has been a cyber attack or danger. If a possible danger is discovered, this component can generate warnings based on the evidence collected. A variety of crime scene investigations models have been presented in the literature. The architecture of our IOTF architecture, on the other hand, is founded on the DFRWS concepts established at the 1st Digital Forensics Research Workshop in 2001 that contain (a) recognition, (b) retention, (c) collections, (d) inspection, (e) research and (f) presentations. Designers feel that using a middleware framework like IOTF to build these components will be excellent for fog doorways. Designers present use possible conditions within the next 2 components to show the utility of our proposed IOTF architecture.

Study1

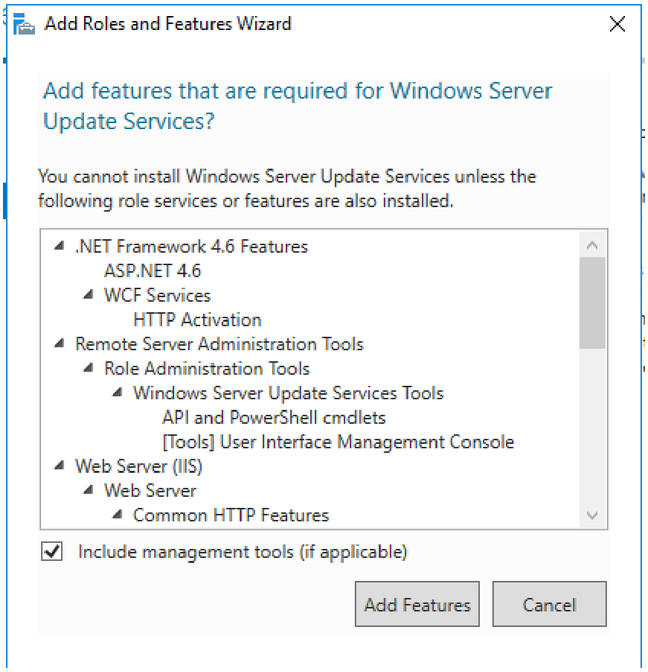
Considering Bob, who does have a digital refrigerator in his smart house, to demonstrate the utility of our proposed IOTF architecture. Suppose that this IoT gadget is a component of the modern house that also contains an IP camera, a smart locking system, and a voice assistant, among many other things. The fridge is linked to a fog gateway, which would be executing the IOTF management solution. Those machines use a Wi-Fi network to connect to IOTF and interact with it. The connection information should be kept internally on each device. Alice, a seasoned hacker, took advantage of a vulnerability in the WPA2 cryptographic protocols that allowed her to recognize the Wi-Fi network's login and passwords. Alice starts exposing more networking flaws and identifies several linked IoT gadgets. This user, Bob, normally communicates to the smart device via his smartphone, which would be geo-located. Alice, on the other hand, tries to connect to the smart refrigerator from an unknown position to IOTF. The surveillance administrator raises a signal in this situation, and the unidentified user's requests are analyzed. The tracking management modules then find that this authorized user sent an HTTP request for the necessary HTTP header elements lacking. This surveillance administrator element recognizes this as a malicious query in this situation and promptly stops it. Then it generates a signal, instructing the forensics analyst to examine the contents of the incoming requests and comparing them to previous queries to find any verifiable events or trends. This analyst collects enough data to determine that this would be a blatant attack. It connects with the case report component in this scenario, which subsequently sends Bob a warning with both the data.

Study 2

A fog gateway implementing the IOTF architecture is related to a no. of IoT nodes. The data transferred from IoT systems to the clouds is continually monitored by IOTF. IOTF, on the other hand, discovers that one of the IoT nodes is faulty or not functioning throughout a normal inspection. Manipulation, hardwares/software malfunctions, robbery, and damages are all possibilities for why an IoT system isn't reacting. Its surveillance administrator sends a signal to the forensics analyst, that starts looking into the IoT computer's past actions. This forensics investigation discovers that the IoT system has been irregularly communicating sensors information over the previous weekend. Even though the IoT system is configured to deliver fog gateways sensors data every hourly, IOTF assesses that perhaps the IoT system has failed to adequately communicate information and data 6 times in the last weeks based on its previous behavior. Inside this scenario, the forensics analyst transmits the information to the caring reports modules, which generates a report with a lower alerting rating, suggesting that the IoT computer's hardwares and software may be misbehaving.

Study 3

This investigative method begins by tracking back through the clouds computer's server records. That assault time is the most important indication for identifying the offender, however servers records are kept on the clouds service provider's servers, and the proposed approach gathers all information outsides of the clouds. So, for obtaining files from the servers, a remotely logging analyzer is utilized, and packet sniffing has been used to gather data in FMP. Servers records reveal comparable IP addresses at the time of the attacks during the authentication of information taken in FMP. Figure 4 depicts this. Additional examination of the collected packets reveals that HTTP packets overloaded the cloud servers, and the PsExec function, was used, as shown in Fig. 5. Such an existing IP traceback method is used to track down the agents from the client. The emphasis is on determining the source of the attacks. The usage of a DDoS assault is discovered after effectively finding the agent's systems. When searching the events records for the time of the attacks, the PsExec program is discovered executing on the agents that correspond to the attacks time. Figure 6 depicts this. The master-handler is not explicitly mentioned in the events logs of the clients.



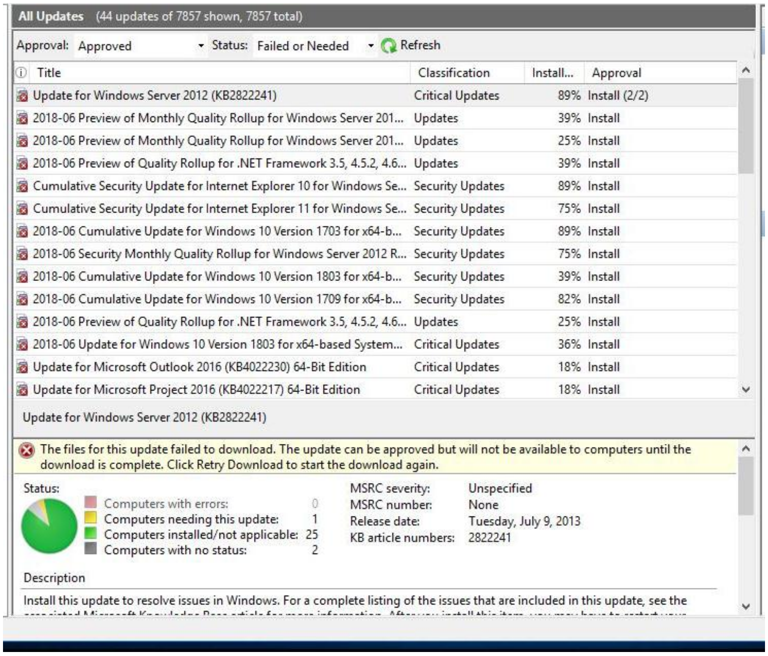
Add features that are required for Windows Server Update Services?

You cannot install Windows Server Update Services unless the following role services or features are also installed.

- .NET Framework 4.6 Features
  - ASP.NET 4.6
  - WCF Services
    - HTTP Activation
- Remote Server Administration Tools
  - Role Administration Tools
    - Windows Server Update Services Tools
      - API and PowerShell cmdlets
      - [Tools] User Interface Management Console
- Web Server (IIS)
  - Web Server
    - Common HTTP Features

☑ Include management tools (if applicable)

Figure 4. Server modification model



All Updates (44 updates of 7857 shown, 7857 total)

Approval: Approved Status: Failed or Needed Refresh

Title	Classification	Install...	Approval
Update for Windows Server 2012 (KB2822241)	Critical Updates	89%	Install (2/2)
2018-06 Preview of Monthly Quality Rollup for Windows Server 201...	Updates	39%	Install
2018-06 Preview of Monthly Quality Rollup for Windows Server 201...	Updates	25%	Install
2018-06 Preview of Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6...	Updates	39%	Install
Cumulative Security Update for Internet Explorer 10 for Windows Se...	Security Updates	89%	Install
Cumulative Security Update for Internet Explorer 11 for Windows Se...	Security Updates	75%	Install
2018-06 Cumulative Update for Windows 10 Version 1703 for x64-b...	Security Updates	89%	Install
2018-06 Security Monthly Quality Rollup for Windows Server 2012 R...	Security Updates	75%	Install
2018-06 Cumulative Update for Windows 10 Version 1803 for x64-b...	Security Updates	39%	Install
2018-06 Cumulative Update for Windows 10 Version 1709 for x64-b...	Security Updates	82%	Install
2018-06 Preview of Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6...	Updates	25%	Install
2018-06 Update for Windows 10 Version 1803 for x64-based System...	Critical Updates	36%	Install
Update for Microsoft Outlook 2016 (KB4022230) 64-Bit Edition	Critical Updates	18%	Install
Update for Microsoft Project 2016 (KB4022217) 64-Bit Edition	Critical Updates	18%	Install

Update for Windows Server 2012 (KB2822241)

The files for this update failed to download. The update can be approved but will not be available to computers until the download is complete. Click Retry Download to start the download again.

Status:

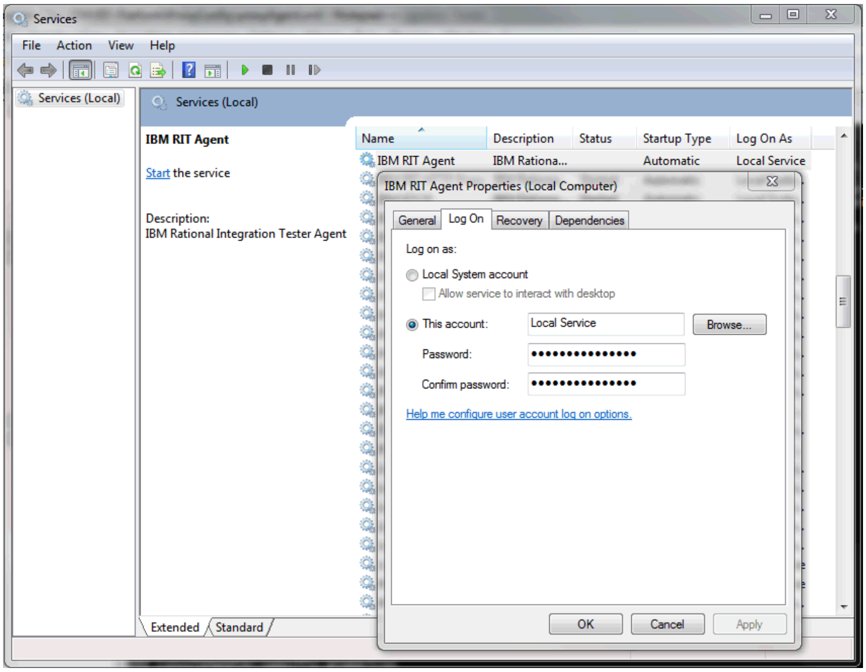
🟥 Computers with errors:	0
🟨 Computers needing this update:	1
🟩 Computers installed/not applicable:	25
■ Computers with no status:	2

MSRC severity:	Unspecified
MSRC number:	None
Release date:	Tuesday, July 9, 2013
KB article numbers:	2822241

Description

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the

Figure 5. Dataset



IBM RIT Agent

Start the service

Description:
IBM Rational Integration Tester Agent

Name	Description	Status	Startup Type	Log On As
IBM RIT Agent	IBM Rationa...		Automatic	Local Service

IBM RIT Agent Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: Local Service Browse...

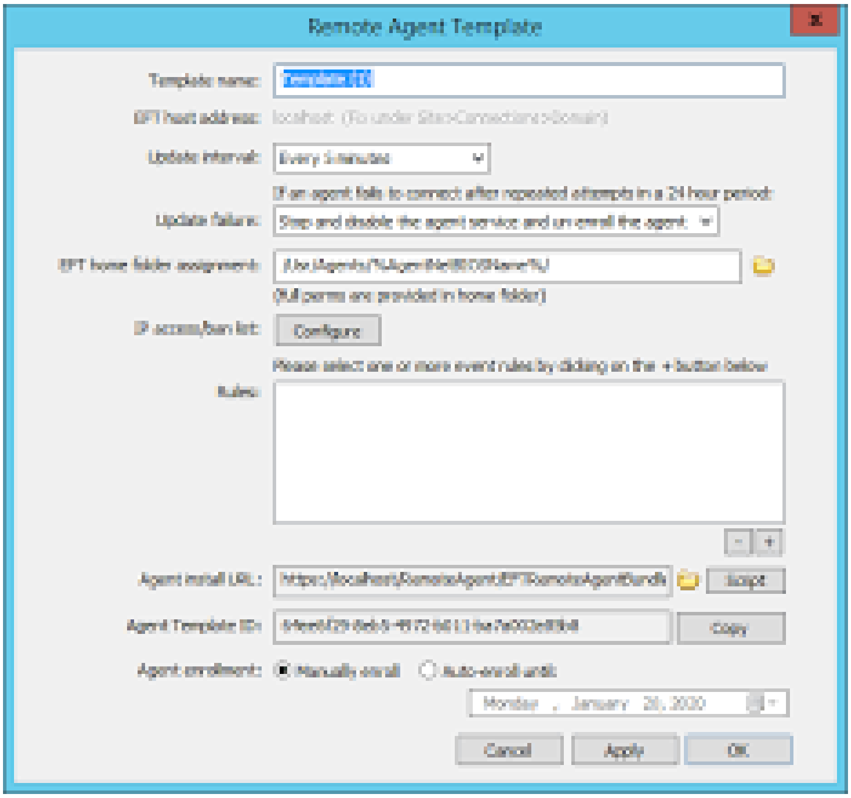
Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

Figure 6. Agents log information

This detective goes into the master's events logs, just as he did with the agents acting, and finds that the PsExec service has been launched, which corresponds to the attacks scenarios depicted in Fig. 7. The attacks code used only for initializing the agent's program that assaults the servers is revealed upon further examination on the master's systems using FTK analyst. This adds to the proof against the masters, causing the investigators to believe that the initial perpetrator is the matching expert.



Remote Agent Template

Template name: Template (1)

EFT host address: localhost (Fix under Site>Connections>Domain)

Update interval: Every 5 minutes

If an agent fails to connect after repeated attempts in a 24 hour period:

Update failure: Stop and disable the agent service and un-enroll the agent

EFT home folder assignment: /Usr/Agents/%AgentNetBIOSName%/

(full perms are provided in home folder)

IP access/ban list: Configure

Please select one or more event rules by clicking on the + button below

Rules:

Agent install URL: https://localhost/RemoteAgent/EFTRemoteAgentBundl

Agent Template ID: [illegible]

Agent enrollment: ● Manually enroll ○ Auto-enroll until:

Monday , January 20, 2020

Figure 7. Events log information

Conclusions

The impact of Cloud-computing on classical digital evidence methodologies was examined in this paper, and some potential solutions for improving computer forensics exploration in the Clouds were proposed, including the advancement of "Cloud-ready" examinations tools and Services Level Agreements with built-in providing for forensics investigations. The importance of accountability had also been discussed. The total fix for imaging incriminating documents in a Cloud-Computing environment may lie in the execution of a Forensics-as-a-Service (FaaS) as a benchmark and executed by service suppliers, which, once combined with conventional techniques and service levels agreements, allows the retrieval of helpful records/knowledge from the Clouds.

They demonstrated IOTF, and IoT forensics architecture capable of detecting and mitigating assaults on IoT devices in their early phases. As the number of IoT devices grows, so will the number of security vulnerabilities and assaults. Regrettably, existing forensics procedures are insufficient for collecting forensics evidence in the event of a cyber-attack on IoT systems. Researchers cover important difficulties related to cloud computing and IoT investigations all through the article. Specialists also spoke about how computer models like cloud environments could be able to assist us to solve these problems. They presented a forensics approach that is based mostly on the DFRWS Investigations Methodology. This entire structure of IOTF, and used cases & execution specifics, were also presented. With us, IOTF architecture was also utilized to give insights into how to improve forensic analysis for IoT applications. Designers want to test the efficiency of our IOTF architecture in the coming by installing IoT systems in a fog computing environment.

Due to the general fast expansion of cloud computing and the likelihood of cloud-related felony offenses in the virtual environment, the demand for clouds investigations is increasing. Clouds security is fraught with difficulties, and just a few academics have attempted to solve them. These problems experienced in clouds forensics, and the remedies identified in the researches, are discussed in depth in this study. A novel model for minimizing the problems of clouds forensics has been proposed and verified using a DDoS assault to see if the developed FMP captures all-important information's for forensics investigation linked to fraudulent activities. In the latter, the whole assault scenarios will be simulated in the clouds to see if the proposed FMP captures all essential information's on potential frauds. Additional components in the proposed solutions would be incorporated once they are completed.

References

[1] Khanafseh M, Qatawneh M, Almobaideen W. A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. Int. J. Adv. Comput. Sci. Appl. 2019;10(8):610-29.

[2] Hemdan EE, Manjaiah DH. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimedia Tools and Applications. 2021 Apr;80(9):14255-82.

[3] Li S, Qin T, Min G. Blockchain-based digital forensics investigation framework in the Internet of Things and social systems. IEEE Transactions on Computational Social Systems. 2019 Jul 26;6(6):1433-41.

[4] Alghamdi MI. Digital forensics in cyber security-recent trends, threats, and opportunities. Periodicals of Engineering and Natural Sciences (PEN). 2020 Jul 8;8(3):1321-30.

[5] Fernando V. Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges. In2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2021 Apr 19 (pp. 1-7). IEEE.

[6] Montasari R, Hill R. Next-generation digital forensics: Challenges and future paradigms. In2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) 2019 Jan 16 (pp. 205-212). IEEE.

[7] Dalezios N, Shiaeles S, Kolokotronis N, Ghita B. Digital forensics cloud log unification: Implementing CADF in Apache CloudStack. Journal of Information Security and Applications. 2020 Oct 1;54:102555.

[8] Rughani PH. Artificial Intelligence Based Digital Forensics Framework. International Journal of Advanced Research in Computer Science. 2017 Sep 1;8(8).

[9] Grigaliunas S, Toldinas J, Venckauskas A, Morkevicius N, Damasevicius R. Digital evidence object model for situation awareness and decision making in digital forensics investigation. IEEE Intelligent Systems. 2020 Aug 27.

[10] Khan Y, Varma S. Development and design strategies of evidence collection framework in cloud environment. Social Networking and Computational Intelligence; Springer: Berlin/Heidelberg, Germany. 2020 Mar 21:27-37.

[11] Akter O, Akther A, Uddin MA, Islam MM. Cloud Forensics: Challenges and Blockchain Based Solutions. International Journal of Modern Education and Computer Science. 2020;10(8):1-2.

[12] Kavin BP, Ganapathy S, Kanimozhi U, Kannan A. An enhanced security framework for secured data storage and communications in cloud using ECC, access control and LDSA. Wireless Personal Communications. 2020 Nov;115(2):1107-35.

[13] AlOwaimer BH, Mishra S. Analysis of web browser for digital forensics investigation. International Journal of Computer Applications in Technology. 2021;65(2):160-72.

[14] Wan Y, Xu K, Xue G, Wang F. IoTargos: A multi-layer security monitoring system for internet-of-things in smart homes. InIEEE INFOCOM 2020-IEEE Conference on Computer Communications 2020 Jul 6 (pp. 874-883). IEEE.

[15] Wan Y, Xu K, Wang F, Xue G. Characterizing and Mining Traffic Patterns of IoT Devices in Edge Networks. IEEE Transactions on Network Science and Engineering. 2020 Sep 25;8(1):89-101.

[16] Patil P, Sangeetha M, Bhaskar V. Blockchain for IoT access control, security and privacy: a review. Wireless Personal Communications. 2021 Apr;117(3):1815-34.

[17] Chaudhary O, Siddique AS. Cloud Computing Application: Its Security Issues and Challenges Faced During Cloud Forensics and Investigation. International Journal of Advanced Research in Computer Science. 2017 Mar 1;8(2).

[18] Huraj L, Šimon M, Horák T. Resistance of IoT sensors against DDoS attack in smart home environment. Sensors. 2020 Jan;20(18):5298.

[19] Nikkel B. Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Science International: Digital Investigation. 2020 Jun 1;33:200908.

[20] Atlam HF, Alenezi A, Alassafi MO, Alshdadi AA, Wills GB. Security, cybercrime and digital forensics for IoT. InPrinciples of internet of things (IoT) ecosystem: Insight paradigm 2020 (pp. 551-577). Springer, Cham.

[21] Horsman G, Sunde N. Part 1: The need for peer review in digital forensics. Forensic Science International: Digital Investigation. 2020 Dec 1;35:301062.

[22] Mohamed N, Al-Jaroodi J, Jawhar I. Cyber–physical systems forensics: Today and tomorrow. Journal of Sensor and Actuator Networks. 2020 Sep;9(3):37.

[23] Burri X, Casey E, Bolle T, Jaquet-Chiffelle DO. Chronological independently verifiable electronic chain of custody ledger using blockchain technology. Forensic Science International: Digital Investigation. 2020 Jun 1;33:300976.

[24] van Beek HM, van den Bos J, Boztas A, van Eijk EJ, Schramp R, Ugen M. Digital forensics as a service: Stepping up the game. Forensic Science International: Digital Investigation. 2020 Dec 1;35:301021.

[25] Horsman G, Sunde N. Part 1: The need for peer review in digital forensics. Forensic Science International: Digital Investigation. 2020 Dec 1;35:301062.

[26] Khalid T, Abbasi MA, Zuraiz M, Khan AN, Ali M, Ahmad RW, Rodrigues JJ, Aslam M. A survey on privacy and access control schemes in fog computing. International Journal of Communication Systems. 2021 Jan 25;34(2):e4181.

[27] Caviglione L, Wendzel S, Mazurczyk W. The future of digital forensics: Challenges and the road ahead. IEEE Security & Privacy. 2017 Nov 28;15(6):12-7.

[28] Feng X, Zhao Y. Digital forensics challenges to big data in the cloud. In2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) 2017 Jun 21 (pp. 858-862). IEEE.

[29] Al-Masri E, Bai Y, Li J. A fog-based digital forensics investigation framework for IoT systems. In2018 IEEE international conference on smart cloud (SmartCloud) 2018 Sep 21 (pp. 196-201). IEEE.

[30] Premkamal PK, Pasupuleti SK, Singh AK, Alphonse PJ. Enhanced attribute based access control with secure deduplication for big data storage in cloud. Peer-to-Peer Networking and Applications. 2021 Jan;14(1):102-20.

[31] Hou Y, Garg S, Hui L, Jayakody DN, Jin R, Hossain MS. A data security enhanced access control mechanism in mobile edge computing. IEEE Access. 2020 Jul 23;8:136119-30.

[32] Egala BS, Pradhan AK, Badarla VR, Mohanty SP. Fortified-chain: a blockchain based framework for security and privacy assured internet of medical things with effective access control. IEEE Internet of Things Journal. 2021 Feb 12.