


A Model of Cloud Forensic Application With Assurance of Cloud Log

More Swami Das, Department of CSE, CVR College of Engineering, Hyderabad, India

 <https://orcid.org/0000-0001-5266-0754>

A. Govardhan, Jawaharlal Nehru Technological University, Hyderabad, India

Vijaya Lakshmi Doddapaneni, Mahatma Gandhi Institute of Technology, Hyderabad, India

ABSTRACT

The key concepts of digital forensic investigation in cloud computing are examination and investigation. Cybercriminals target cloud-based web applications due to presence of vulnerabilities. Forensic investigation is a complex process, where a set of activities are involved. The cloud log history plays an important role in the investigation and evidence collection. The existing model in cloud log information requires more security. The proposed model used for forensic application with the assurance of cloud log that helps the digital and cloud forensic investigators for collecting forensic scientific evidences. The cloud preservation and cloud log data encryption method is implemented in java. The real-time dataset, network dataset results tell that attacks with the highest attack type are generic type, and a case conducted chat log will predict the attacks in advance by keyword ontology learning process, NLP, and AI techniques.

KEYWORDS

Cloud Computing, Cloud Forensics, Digital Forensic, Hyper Visitors, Virtual Machines

INTRODUCTION

Cloud computing is a model that provides on-demand services and network access to configurable resources for example servers, networks, storage and application services with minimum management effort with service provider interactions. Cloud Technology is emerging in recent years and providing services like cloud storage, reliable, scalable, flexible, and cost-effective solutions. It is used in data processing, network and virtual systems in the cloud management environment. Cloud technology, modern hypervisors are used in virtualization technology to monitor data. In the new digital era, cybercriminals use cloud computing as the trusted region for fraudulent activities due to cloud computing vulnerabilities (Lei Chen et al, 2019). Recent news reveals that cybercriminals are imitated cloud computing technology for cybercrimes in various areas in Hyderabad, Pune, and various metro cities in India. Some of the cybercrimes for example payment fraud digital payments, QR Code cheating has an increased crime rate in 2020 (Times of India, n.d). Cloud domains are used in application development, devices, systems, data management, deployment, analytics, visualization, distributed computers, data structures, network protocols, customer, security, legal sources, procedures and investigations in forensic. The Virtual Machines remote acquisitions, data acquisition in Crimes Digital forensic – cloud computing evidence, remote investigations needed a convenient Model (Josiah et al, 2012). Cloud computing applications includes email, virtual machines, hypervisor, IaaS provider,

DOI: 10.4018/IJDCF.20210901.0a7

This article, published as an Open Access article on July 2nd, 2021 in the gold Open Access journal, the International Journal of Digital Crime and Forensics (converted to gold Open Access January 1st, 2021), is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

which uses the tools for analysis. The collected data in Cloud services SaaS, PaaS, evidence of data, collection, identification, examination, analysis and reporting. (Aleksandra Petrescu et al., 2014).

Cyber cloud attacks cause cloud forensic applications a new discipline in the digital world. The essential characteristics, vulnerabilities that bring a safe zone for criminals. In digital forensics in cloud computing, remote investigators can collect forensic evidence from a source or provider. Cloud forensics is a digital forensic application in the cloud environment. Digital forensic is part of computer forensics used for data collection, identification, analysis and reporting of digital evidences. Identification is a complaint by individuals when intrusion detection systems or computer audits, system logs are used for identification of data. Cloud forensic consists of hybrid forensic approaches for example use of a remote live network, in which clients towards the generation of digital evidences. Traditional forensic investigations focus on evidence, track of data hard drive and solid-state drives. Cloud computing is a recent technology that helps user's in digital forensics, cloud computing is on-demand to use data centers expected to be Digital Forensics retail cost \$4.24 billion by 2025. The Cloud forensics tools are FROST, UFED Cloud Analyzer, Encase Enterprise, and Access Data FTK

The dependence on Cloud Service Provider (CSP) includes activities in the forensic process, there may be a way to alter the data this affects during the investigation process. The Proposed Model provides an environment in outside cloud environment secrecy scheme assurance of cloud log in cloud forensic applications.

Most of the research work is to examine the challenges of cloud forensic and visualize solutions that depend on CSP for forensic investigation. The objective of this contribution work in Cloud forensic is to put importance on the challenges faced by investigators during the investigation process, cloud forensic, logs, and hypervisor and virtualization technology. The rest of the chapter is organized as section 2 history and background, section 3 proposed model, section 4 results and discussions end with section 5 conclusion and future scope.

HISTORY AND BACKGROUND

The history of cloud forensics early in 1979 data collection process, rule evidence, from 1970 to 1985, this helps for identification forensic analysis, 1984 digital evidences, 2000 computer evidences, 2010 Network evidences, 2020 Computer activity logs are used for digital evidence data collection in Forensic study.

Related Work

According to (Devi Radha Rani et.al, 2016) Cloud computing is popular in various areas of life. Cloud forensic helps forensics investigators to find potential evidences, criminal activities in the cloud, and maintain security. Cloud forensic investigation, process security incidents in Cloud computing are most important in the field of IT, CSPs, methodologies, tools to assist cloud forensic applications.

A user activity log is the most important source of information to investigate in cloud forensics. (Stavros Simou et al, 2016) proposed a Cloud Log Assuring Soundness and Secrecy (CLASS) has logs are encrypted in the individual public key and decrypt the contents to prevent unauthorized modification of content. (Nazir Ahsan et.al, 2018) studied Cloud computing's most informative technology that provides service to clients on demand by CSP. Forensic enables those support investigations by logs in operations on criminal activities in the cloud. According to (Keyon Runa et.al, 2011), cloud computing is most information technology in technical, economical opportunities to CSP, security both providers and customers. Digital investigation in Cloud computing is used in small and large companies. Cloud requires privacy and Security in data. The policies of companies to provide security in distributed cloud environments and Security. According to (Josiah Dykstra et.al, 2011) Evidence in digital forensic, tools are used for Encase and Access Data Forensic Toolkit. Digital forensic, cloud computing is the nature of remote evidence to access trust in integrity and authentication.

According to (John R vice et.al, 2012) Criminals Computer engineers learn hacking fundamentals in high school and provide security to computers. The authors studied criminal investigation techniques used Evidence collection and security is essential, (Bill Nelson et.al, 2012) studied Computer forensics investigations data requires analysis and security. Framework model is used in Cloud forensic applications to investigate cloud log data.

Growth of Cloud applications in public and private sectors, the cyber attackers steal the data, damage the applications, the major challenges cloud service provider must provide security for Cloud application services to clients, (Sheik Khadar Ahmad Manj et.al, 2016) proposed Forensic experts in cloud, storing pieces of evidence that helps further legal process. (Iliyasu Yahaya Adam et.al, 2020) proposed a digital intelligence using machine learning, AI techniques used to find, detect and prevent criminal activities. Internet across the world, the various risks, attacks in the network, the cyber attacks, the (Sweta Bhattacharya et. al, 2020) proposed a XGBoost Method for finding the intrusions. intrusion system is a convenient handling the traffic and maintenance of tasks. The (Swarna Priya et.al, 2020) proposed a EECloudIoE architecture that optimizes e cluster chosen data traffic. IoT is communicating sensors, networks and intelligent devices, it provides application services to users like health, smart farming, etc.

(Celestine Iwendi et.al, 2016) proposed a model that protects cyber attacks by criminals to hack data. In the software industry, software in all domains. KeySplitWatermark protection, against cyber attacks. In world, applications requires computational power, high-speed internet-based applications. (Mahdi Aiash et.al, 2015) studied the incompatibility of security measures in infrastructure. Security considering in cloud computing, security measures security infrastructure. Security approaches, Information security, Access control, Service level agreement in management of services, for security cloud-based application. The advantage of hybrid approach provides information security to access control in service level agreement. The management has access service and monitoring security policies. The disadvantage is the hybrid model combines infrastructure and information measures. It is a necessity to design a new framework for security incidents.

Cloud computing is one of the most important technologies used in cloud Forensic applications. Cloud forensic constitutes data processing, evidence collection and recovery. Investigations in cloud log plays a critical role in privacy, security policies for Cloud security providers. (Sulema Khan et.al, 2016), proposed a Cloud log Forensic, investigation operation by analyzing malicious behavior by cloud log analysis. (Keyun Ruan et.al, 2013) proposed a model Cloud forensic investigation process to monitor log activity, cloud logs help in forensic application to find accurate investigations in cloud data. The summary of the Literature is described in Table 1.

Problem Definition

Designing a Cloud Forensic model helps Investigators to secure computer Cloud Forensic application involves preservation, identification, extraction, documentation, science computer evidences by logs. The Cloud Forensic application has Data User, Data Owner (CSP), Network Monitoring, and Investigator services.

PROPOSED MODEL

The proposed Cloud Forensic model helps users in the investigation process to find the Forensic investigation which depends on CSP and signed contracts. Framework model in Cloud Forensic process will collect, analyzing, digital evidences, which are legally acceptable. The proposed model has users and data owners, Forensic Investigator/Auditor, Cloud Service Provider, and Digital forensic Server is shown in Figure 1.

The Forensic Framework has virtualization technologies and monitoring activities. Cloud computing with computing power use technology. IT experts use services data, stored process data and

analyze the forensic study using distributed agents, the roles and responsibilities of each component, user, csp, network forensic monitoring are discussed here.

User and Investigator

Client uses browsers to access the APIs from CSP. Examples of CSP includes Amazon S3, Google, Microsoft etc. Information of a process in cloud digital provenance is necessary for a crucial feature in forensic investigation. Cloud security and privacy, knowledge, digital artifacts, logistics, legal issues are related to a cloud environment. CSP provides authorization to Data Owners and Users and CSP contains the record of all the activities that are performed by the Data Owner and User.

Cloud Service Provider (CSP)

Cloud computing technology is most used by World Wide Web (WWW), Smartphone and application services. Cloud computing characters are multi-tenancy, elasticity, pay as you go, reliability and availability of services. The Cloud Service Provider (CSP) provides services like infrastructure, high availability, clusters, data centers the level of interface data, access and applications. Infrastructure as Service (IaaS) has user server, hardware, storage, and Operating System, Platform as a Service (PaaS) development environment to users and Software as Service (SaaS) to manage application software (John R vice et.al, 2012).

Network Forensic Monitoring

Digital forensic is growing tremendously every year and it is essential and required for Forensic practitioners to store, process and analyze information. Forensics as a Service (FaaS) is an extraction of data, to store deleted data hidden files, and process cloud data. The Forensic tools (The Best Open, 2018) are described in Table 2 which helps for collecting evidence analysis and plays a critical role in data collection, analysis and reporting in various applications.

Forensic tools are used to investigate and collect strong digital evidences which is required for legal actions. By collecting data, digital evidence investigations which makes a critical role in finding criminals or hackers. The Technological advancements for selecting a process in digital forensic study that the tools help investigators. The feature extraction from links /log activities, examination and extraction of digital evidence. The Expert system use all relevant information. The use of AI and digital forensic process to find the reasons, digital information plays a crucial support to make judicial decisions.

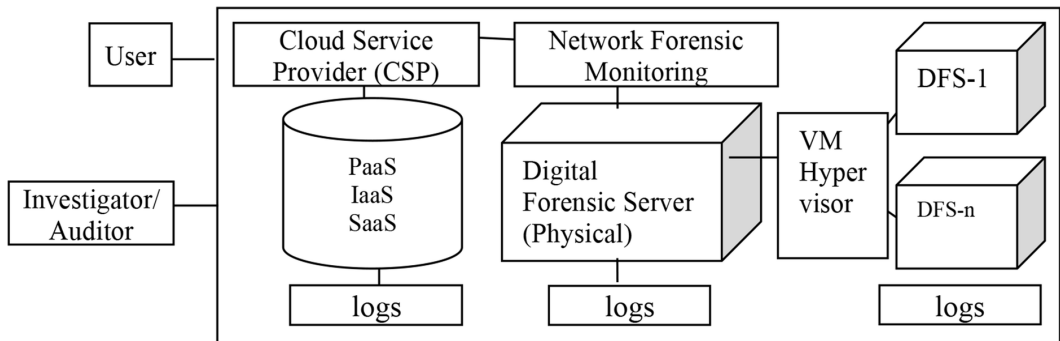
Investigation officer use ontology model which finds a crime matching mechanism with the help of activity log, monitoring and prediction tools. Digital evidences exhibit correlation of evidence that analyze the evidence and efficiency of human and computational resources.

Processing forensic data is on priority of available forensic examination. Digital forensic investigations with at each state includes acquisition, analysis, and presentation. Intelligent methods with optimal set of rules in cloud computing around the Globe, the security is the most significant task. The cloud services (IaaS, PaaS and SaaS), such as computing applications, network resources, software services, virtual services and Infrastructure. In cloud Forensic, cybercriminals are those who legitimately involved in destruction of security and hack the data to utilize services. Digital forensic application environment the cloud service provider, user, broker and Cloud auditor. Internal and external investigations are carried out in organizations to find the attacks. The challenges are Architecture/Model, data collection (example, data location, storage and recovery), analysis (for example logs, timeline activities), anti-forensic (for example data hiding), an incident for respondents, for cloud providers and trustworthiness), management and access, legal (ethics, service agreement, privacy). The cyber attackers are recognized by continuous monitoring in logs of activities in the cloud environment.

Table 1. Summary of Literature of Cloud Forensic study

Author and year	Merits	Observations
(Lei Chen et al, 2019)	Cloud Technology emerging work, digital forensic study evidence collection from storage	External storage is required security
(Josiah Dykstra et. al, 2012)	Forensic evidence from infrastructure as a service Model for cloud forensic data and analyze the reports	Cloud model loss of evidence when cloud resources are released
(Aleksandra Petrescu etl.al, 2014)	Monitoring activities in a cloud environment	Digital forensic cloud data not stored in a single system, Virtualization required and security for quality cloud services
(Devi Radha Rani et.al, 2016)	Cloud services challenges, collecting data evidence in the investigation process	Process of cloud forensic no standard framework
(Stavros Simou et al, 2016)	Forensic investigation activities and provide security and proposed investigation of security by incidents in cloud services	Investigations demands forensic process protection and security for online services
(Nazir Ahsan et.al, 2018)	A forensic investigation by Cloud logs	Security for both provider and cloud data user
(Keyon Runa et.al, 2011)	Cloud computing forensic investigation	Cloud logs required security
(Dominik Bark et.al, 2011)	Forensic investigation to find the evidence by multifactor authentication, policies for investigations Data processing evidence collection, digital framework in a distributed cloud environment	Compatible investigation process clear and transport to security is required
(John R vice et.al, 2012)	Criminal investigation techniques used	Evidence collection and security is essential
(Bill Nelson et.al, 2012)	Computer forensics investigations	Investigations data requires analysis and security
(Edington Alex et.al, 2017)	Framework model is used in Cloud forensic applications	Cloud forensic study investigation requires process steps
(Sheik Khadar Ahmad Manj et.al, 2016)	Data security proposed model trusted the third party with cloud forensic investigation team strong collection of evidence	Security is required for a cloud data environment
(Iliyasu Yahaya Adam et.al, 2020)	Investigation and intelligence use machine learning techniques	Automatic Framework use police enforcement in cyber and criminal activities
(Sweta Bhattacharya et. al, 2020)	Network various malicious attacks, cyber attacks, module Intrusion detection system to prevent cyber attacks	Framework intrusion prevention system is required with various machine learning techniques
(Swarna Priya et.al, 2020)	Optimization of network services by cloud-based Internet Everything and services	Cloud-based evidence and services to end-users
(Celestine Iwendi et.al, 2016)	Cyber attacks protection by key split watermark approach for detection of attacks	Users, servers provided with security and application-specific code
(Mahdi Aiash et.al, 2015)	Security in cloud measures, infrastructure and integrate information security approaches	Hybrid framework information and infrastructure design and validations are required
(Sulema Khan et.al, 2016)	Cloud forensic to investigate cloud log data and analyze the malicious behavior	Cloud investigations security interfaces to investigate the cloud log data
(Keyun Ruan et.al, 2013)	Cloud environment digital forensic investigation and analyze the data	Investigation process evidence collection requires more security

Figure 1. Cloud Forensic Model For Cloud log secrecy



Cloud services are uniquely to identify all application services by trusted party and cloud service provider. Forensic investigator to find the logs which are suspicious activities, and use of cloud services logins, activity logs, trusted party and forensic investigator to secure cloud applications.

To share the data in multiple copies on the cloud more than one local system. Cloud investigation process by analyzing digital evidence with the use of forensics method tools by high-performance computing, remote indexing. The tools are used in cloud service provider has preservation of log by the parser, which collects log source and keeps content secured. Accumulator is a filter which is used to fetch required content log at verification time, verification processes to find log information

Table 2. Tools used in Investigation

Nam of the Tool	Used in Investigations
Autopsy	An Autopsy is a UGI open source digital forensic program to used to analyze hard drive, smart mobiles it is also used to investigate the computer
Encrypted Disk Detector	Encrypted Disk Detector is used to find out encrypted physical drives in a system.
Wireshark	Wireshark is a network capture analyzer tool that is used in network analysis
Network Miner	Network Miner is a tool that is used as a forensic analyzer for Windows, Linux and MAC OS to detect and find OS, session, hostname, posts by packing sniffing or PCAP file
NMAP (Network Mapper)	Network Mapper is a popular networking security auditing tool. In Linux, windows and open source.
Forensic Investigator	A Forensic Investigator is a tool used with the Splunk app to combine
FAW	FAW (Forensics Acquisition of Websites) is to receive web pages in forensic investigation to capture entire page, all types of image, HTML webpage and integrate wire shark environment.
SIFT	SIFT (SANS investigative forensic toolkit) is used to find source incidents and responses.
ForensicUserInfo	ForensicUserInfo is used to find login count, groups and profiles path.
Paladin	Paladin forensic suite the world's most popular Linux forensic investigation tool.
Sleuth Kit	The Sleuth Kit tool is used to investigate, analyze and find evidence.
CAINE	CAINE (Computer Aided Investigate Environment) is a Linux forensic platform that uses 80 tools to analyze, investigate and integrate reports.
Oxygen Forensic Suite	Is a tool used to investigate, evidence in mobile applications.
Xplico	Is a Network Forensic Analysis Tool (NFAT) tool whose aim is to extract internet traffic data.

correct entries by Cloud Service Provider (CSP) and Investigation agency, and finally secret key shared to clients by an individual private key.

Forensic computing key stages are identification data, preservation data, Analysis of data, Reporting data, and presence of digital evidence submitted to the court. The collection is an activity to investigate, acquire the evidence to find and interpret data. Data collection process which helps to make the decision stage in Framework consists of the Presentation, identification, documentation, packing, transportation, examination and analysis. The proposed model in Digital forensic stages of awareness, authorization, planning and notification. The Stages are incidents, responding, data collection and analysis. In cloud forensic, the type of cloud services and the technology is used in investigations. Parallel stages of identification in collection, organization, presentation, verification is required. To Merge similarities of evidence and assign challenges to each stage, the digital forensics framework for identification reads the operation data, identifies all possible ways and resources for example. Hardware, software through investigations, Presentation have the preparation after identification of evidence locations and the collection has Detection and notification. The examination makes confirmation and authorization. The analysis makes the collection, and Presentation and decision are based on data, confirmation and decisions running with document evidence, after inquiry investigation of crimes, in the presentation stage the evidence is submitted to court law. Designing a cloud Forensic model which helps to secure computers and applications.

Forensic investigation requires at least two things CSP, customers. Cloud forensic investigation by agencies. Cloud computing services need customer services by CSP, in between the links between customers to Service provider. Each link chain interrupts or corrects each chain's responsibility between all the parties. Serious problems are identified in Service Level Agreement (SLA) by communication collaboration for example user name, password, and encryption keys. The Service Level Agreement is evidence, preservation and collection Investigation process seize hard disk, same copy to maintain integrity.

Digital forensic, legal considerations the investigation process steps have digital evidence, data collection, data preservation, Validation and documentation. The applications are military, law enforcement, corporate and academic etc. The Process of investigation in digital activities and events. In the Evidence/Forensic study, the evidence of data is to be submitted to the court. The Forensic examination, suspect the events in network activities to find the digital evidences. Perform the data analysis which helps the investigator to make decisions. The crime prioritization is to access data where information is in danger system, digital documentation to investigation which helps to save the systems in advance.

The investigation process conducts logs, activities, evidence and inquiries. Investigation tools equipment for data collection. Securing all evidences, and stored information by the investigator to search all relevant electronic evidences to analyze the data and send a report after the process of investigations steps such as data collection, examination data, analysis and reporting. The data Collection from sources examination is the extraction of data, analyze data and present analyzed reports.

The proposed Algorithm 1. Preservation of cloud log data encryption is as follows.

Algorithm: 1 Preservation of cloud log data encryption

Input: Log entries

Output: Encrypted log entries

Step1. Read log entries

Step2. For all the Log entries

Step3. Convert to Encrypted login entries in the database log

Step4. Proof log entries find the time and entry details

Step5. Publish the entry, time, signature, with Encryption Display the

Encrypted logs

Step 6.End

Virtual Machine – Hyper Visitor

Virtualization is Virtual machines with forensic framework network devices are used in the investigation process. Layered approach contains one, Management layer which has operations in forensics. Second, the Framework Virtualization layer is responsible to gathers raw data monitored from virtual machines, virtualization, cloud forensic applications helps in forensic investigators to find possible evidence, criminal activities in the cloud, and maintain integrity and security in the cloud. Cloud forensic investigation is a process that provides security incidents. Cloud computing has two layers one, virtualization use hypervisors, and second layer management which deals with security, validation, scheduling, hypervisor interface, load distribution. The network layer, communication protocols are used in cloud, CSP, data and network and components. The evidence that are strongly supports investigators from the log Table 3 shows Network Forensic Monitoring layers, methods and applications (Edington Alex et.al, 2017).

Table 3. Network Forensic Monitoring in VM and Hypervisor

Layer	Method	Application
Guest application	Dependable	Guest operating system
Guest OS	Remote Forensic software	Software
Virtualization	Introspection	Hypervisor
Host OS	Access hardware	Host Operating system
Physical Hardware	Access physical disk	Network

The network data set collected from (The University of New South Wales, n.d) consists of 70000 records consists of 49 fields namely source IP, destination IP, transaction, source, designation, 48 fields .attack_cat nominal. The name of each attack category. In this data set, nine categories e.g. Fuzzers, Analysis, Backdoors, DoS Exploits, Generic, Reconnaissance, Shellcode and Worms label 49 Label binary 0 for normal and 1 for attack records UNSW-NB15_1 file contains 70000 records log data, in which attacks are 22215, UNSW-NB15_2 file contains 70000 records log data in which 52749 records are attacks. The summary of the Network dataset attacks type analysis report is shown in Table 4.

The results of Network dataset attacks show the highest number of attacks are Generic type, and lowest attack category is worms and moderate type is exploited attack category.

RESULTS AND DISCUSSIONS

Digital investigation in forensics evidence data is collected, stored in a specific format and select appropriate data, based on feature selection investigation techniques. Technical aspects, the source and nature of evidence in forensic investigation. Web-based services depends on applications, for example, email, social networking in forensic acquisition uses virtual machines, use a remote forensic agents. The forensic analysis in desktop computers, the forensic investigator, remote access, guest virtual machine and find correlation evidences, introspection and investigation of human activities.

The Proposed Model is implemented in Java that contains as Cloud Service Provider (CSP), Data Owner, Data User and Investigator. The role of the Investigator is to verify whether authorized owners and users are making use of the cloud or not. The user/Auditor also contains all the activities

Table 4. Network Dataset Result – Attacks

S No	Attack category	UNSW-NB15_1 Total number of attacks	UNSW-NB15_2 Total number of attacks
	Total log records 70000	22215	52749
1	Analysis	525	607
2	Backdoors	533	369
3	DoS	1167	4636
4	Fuzzers	5408	1102
5	Exploits	5050	4667
6	Generic	7521	27882
7	Reconnaissance	1759	3115
8	Shellcode	222	323
9	Worms	24	40


owned by Data Users and Owners. Shown in Figure 2 stores all activities which are done by the Data user and Owner.

CSP environment trusted party guarantee of cloud services. if any malicious activity then evidences by the investigator by digital evidence, cloud logs, activities, and history. The auditor checks the corresponding logs, history of digital data. cloud environment digital artifacts, acquisition logistics and legal problems related to the cloud environment. Incident handling, tracking evidence, accountability in a cloud environment. Security environment with cloud infrastructure, network security, digital provenance, several issues of cloud forensic, cryptographic proof, data verification, integrity and cloud storage. Web service Forensic, digital forensic is identifying, extracting, collecting evidences from digital media. Evidence analysis to maximize integrity in the preservation of evidence analysis. Analyzing the data sources of information, and real story, evidence analysis and finally present the reports in evidence collection. Infrastructure as a service (IaaS), Cloud Service Provider(CSP), Physical computer, power, network systems etc Platform as a Service (PaaS) it provides application development environments, with servers, CSP and Software as a Service (SaaS), the services run on systems, the deployment model public, private and hybrid cloud models. Forensic investigation is a potential evidence from available to investigators in cloud environment applications. Cloud instances, live investigations to access the virtual instance of evidence collection, network layer, logs, events. ISO/OSI layer provides protocol communication to user client system, which client depends on IaaS, SaaS and PaaS, and potential evidences are collected in data process, application and network environment. Data provenance is digital provenance, metadata that contains a history of digital objects, who has ownership records, process history. PaaS software applications, which control customers, and provide CSP applications, the ability the customers use applications. PaaS, ability to collect, verify store, diagnostics configurable resources in runtime. IaaS is recovery evidence from incidents.

Figure 3 represents log details that are a list of all activities done by the Data Owner and Data User. It includes all uploaded and search files.cloud log. The goals are used to Investigate cloud log, data integrity, and cloud service providers (CSPs) to receive access to various cloud logs. The log provides useful information, like instance, bandwidth usage, analyze network log. Identify, fix bugs, logs are used to find activities of application, it helps network administrators/auditor to investigate and find attacks, analyze log file data. Cloud logging application services are referred to as log as service. Log files in organizations' resources to cloud storage, analysis, and cloud log analysis servers. computations cloud login to investigate malicious activities such as cloud application log, cloud network log, cloud system log and cloud firewall log etc. The cloud log is used to record all

Figure 2. Representation of Investigator Login

Investigaor/Auditor Login



Investigator Name (required)

Investigator Password (required)

Menu

- Home
- Cloud
- Data User
- Data Owner

logs in the cloud environment. To analyze cloud log, through analysis services with cloud forensics, cloud logs file to investigate malicious activities., cloud log accessible to cloud service provider(CSP) through ownership.

Software as services in cloud computing provides, with software development. cloud log data has number log entries, log file limit, log time data, content to log. after the cloud log file stored in a secured environment(i.e decrypted) format and it will protect integrity. Attacker proved evidence by CLF data integrity by Administrator, Cloud log, administrator prevents attacks and finally analyst of the cloud is a legal document is generated. to minimize vulnerabilities in cloud computing, CSP initiated with security constraints like logging, type, model, cloud computing and digital forensics. log as a service to cloud vendors. Cloud log vendors to deploy and implement security requirements.

Figure 3. Proof of Past Log on Files

Proof Of Past Log (PPL) On Files

ID	User Name	File Name	Task	Date & Time
1	QWJoaQ==	Rmlyc3QuanBn	VXBsb2Fk	MTevMDIvMjAyMCAgIDE0OjA0OjQ4
2	TW91bmlyYQ==	c2VjLmpwZw==	VXBsb2Fk	MTevMDIvMjAyMCAgIDE0OjA3OjA4
3	QW5vb3A=	Rmlyc3QuanBn	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ2
4	QWJoaQ==	VEguanWpni	VXBsb2Fk	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
5	TmI0aHlh	VEguanBn	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
6	TmI0aHlh	VEguanBn	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
7	TmI0aHlh	Rmlyc3QuanBn	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
8	QW5vb3A=	U2VjLmpwZw==	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
9	QW5vb3A=	c2VjLmpwZw==	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
10	QW5vb3A=	Rmlyc3QuanBn	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
11	QW5vb3A=	Rmlyc3QuanBn	U2VhcmNo	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
12	QWJoaQ==	dGhpcmQuanBn	VXBsb2Fk	MTkvMDIvMjAyMCAgIDExOjEzOjQ1
13	QW5vb3A=	Rmlyc3QuanBn	U2VhcmNo	MjQvMDIvMjAyMCAgIDExOjEzOjQ1

Menu

- Home
- Attackers
- View Files
- Upload File
- Delete Files
- Logout

Table 5. Types of logs

Log type	Description
Host	IP address
Username	The system name
Time zone	Asia, India
Request	Get resource
Status	Success/failure
Bytes	Number of bytes data transferred during HTTP request

Vulnerability key security parameters that collect evidences for the investigation. Process of record events files during execution of operating system process, network, application logging. Log entries each log entry contains most useful information. user id, date, time, web server finish request, client, HTTP status code, web server etc.

Investigator to identify sources of messages captured from many devices detect various audit logs generated track of the system network security, the IDS, firewalls will record logs.

Real-time collect the data events, security log at regular intervals. types of logs, log, system application, the device network communicates to the user, record communication event log file. The type of logs that contain information is described in Table 5.

Application log recorded for application such as web application system log, system log generated by operating system events, devices. Security log contains security information like instance, malware detection, time of malicious detection. example. Event log analyzer will be used in event monitoring services setup log set log perform installation e.g. web server installation, application deployment. Network log file contains related network events, priority time, web server log records all the events on a web server, IP address, date of the event, request .audit log information contains unauthorized access of system, network inspection roles, login, destination, timestamp etc. virtual machine log; file log event is performed on a virtual machine. Ex. JVM controller, VM log auditor. the application log created by developers, the log is the most important information for higher levels of operations.

Logging mode is a process to record an event at the time of execution. To investigate problems, logs to identify susceptibilities, recovery of log investigate vulnerabilities. Login model has two types one circular log used in transaction recovery, no maintenance required, application failures, minimum human intervention, re-use logs, and disadvantage, lack of long term storage, no recovery. second, linear logging, media, application, applicable software, failure, media failure, recover damage in queue files and disadvantage, request maintain, slow process and never reused, it degrades performance.

Investigation log to identify different vulnerabilities and malicious behavior, Cloud forensic services investigations to log. Figure 4 shows cloud forensic log analysis that consists of investigator, series, firewall, application and analysis.

The user access log data in real-time, log data in CSP uses the encrypted form to make original and invisible to an intruder is invisible to access the data.and Figure 5 shows Cloud Log Encryption data is implemented in Java.

Forensics investigation process is secure, precautions in firewalls to prevent attacks. The collection of forensic evidences, forensic service, crimes, legal problems, examination and the Target machine. In this the forensic tools are used on the remote acquisition of data with Forensic software, forensic logs and cryptographic checksum. The security of web site code is maintained by webmaster system in network security admin privileges. In Digital Forensic study needs the Electronic evidence, Forensic services, Data recovery is recovery data, Evidence data collection, Data seizure process, Data de-duplication and Preservation of digital evidence Identification are used in Computer Image, document, verification and authorization. Smart applications are used in the world, IoT applications

Figure 4. Cloud forensic- application investigator cloud log and analysis

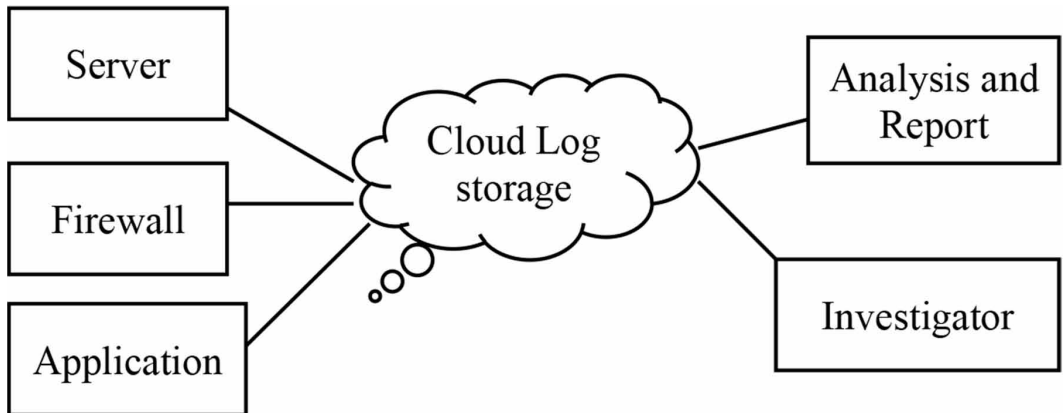


Figure 5. Representing Encrypted Details

ID	User Name	File Name	Task	Date & Time
1	Abhi	First.jpg	Upload	11/02/2020 14:04:48
2	Mounika	sec.jpg	Upload	11/02/2020 14:07:08
3	Anoop	First.jpg	Search	19/02/2020 10:13:46
4	Abhi	TH.jpg	Upload	19/02/2020 11:46:55
5	Nithya	TH.jpg	Search	19/02/2020 11:48:27
6	Nithya	TH.jpg	Search	19/02/2020 11:48:58
7	Nithya	First.jpg	Search	19/02/2020 13:56:15
8	Anoop	Sec.jpg	Search	19/02/2020 14:00:23
9	Anoop	sec.jpg	Search	19/02/2020 14:02:43
10	Anoop	First.jpg	Search	19/02/2020 14:36:40
11	Anoop	First.jpg	Search	19/02/2020 15:30:37
12	Abhi	third.jpg	Upload	19/02/2020 15:37:26
13	Anoop	First.jpg	Search	24/02/2020 09:44:21

Menu

[Home](#)

[Attackers](#)

[View Files](#)

[Upload File](#)

[Delete Files](#)

[Logout](#)

use sensors, communication, the internet, cloud storage and analysis. Cloud Technology flow of traffic information in various applications services.

High-performance computational resources, storage servers, expert systems, networks, users comfortable using cloud log as service. Cloud log forensic service logs collects data from devices, systems, networks, other resources.

In forensic investigation three categories of people are involved 1) investigation, 2)synchronization and 3) security each group objective solution, the main goal is to describe infrastructure used to test solution, and experiment on target logs, investigation to find vulnerabilities in cloud logs, synchronization: cloud log is in different locations and used in a forensic investigator to check modifications.

Data quality assurance, security logs are used to record events, origin of attacks in multiple heterogeneous resources, network systems. The proposed log as service Proof of Past log is evidence to prevent and use of altering log files.

Cloud log operations in encrypted log data, real-time attacks, log file encrypted before sending them. log as a service in system, network process in a specified timeline, log steps, time process, logs, execution logs to manage the resources, the administrative staff, and security checks logs, integration and operation the log in various locations, visibility of logs are monitoring in real time environment. The log files in cloud servers. Parameters in the log as service. Forensic is an investigation of CSP log, access the log as a service with CSP for users charging a price for various cloud services. Log format, encryption of log provides the security of information. For Example, Cloud log service providers are IBM Smart Cloud analytics, analyze operational data integrated sources to find the root cause for paper trail provides log as service in API, provide hosted management logs, text log, command line, web or email. Splunk storm, cloud log management help users to monitoring, diagnosing, various cloud applications ex. AWS, Google App Engine, Loggly, collects various source or devices, log check the status of application in web service applications. Use case Cloud Log as Forensic: Investigate, project, process, real-life situations, different logs, in CSP, focused on 1) cloud technology 2) log type 3) advantage 4) result (outcome).

For example, Processor in Payment Systems, Many more transaction in a day, e-commerce, provides, parole, mobile transactions, etc. vulnerabilities, attacks provide log help to analyze activities to find the root cause for malicious activities in early stages, Investigates user to analyze log forensic, which respond malicious activities in investigation in and find the suspicious events. log data collection, log forensics in bank holds million clients events per day are generated from log files in network equipment, security services and, databases. Investigation finds fine root cause analysis, response suspicious events and threats. The proposed model helps the cloud service providers to prevent attacks or crimes in advance

Cloud log forensics security requirements process cloud computing, location, storage, and organization. risk organizations due to vulnerabilities, attacks. The log file generation, monitoring will minimize threats, and exploitation of Cloud Service Providers. CSP to protect log file, and forensic process helps to prevent attacks in future.

The confidentiality is preservation of user information in the cloud log file, the integrity is cloud log file which provides evidence from attacks. The non-modification of cloud log availability of access cloud log files resources. Authenticity: cloud log files, investigation, log files in legal permission to investigation agency. Privacy log data, user application, in cloud computing applications. Every stage CLF (Cloud Log Forensics) generator analyzes the data.

Cloud log foundations in future directions are log generation, collection, analysis in secured environment. Log generation use various tools in configuration files. Log collection is collected by cloud agent from various sources in cloud applications, Network Cloud log, storage resources to record cloud log and process information. The confidentiality, data, alter data on the network. Log storage: location, resource in logs are stored and analyzed.

Cloud forensic investigator to monitor log activity. Cloud logs forensic study to investigate the cloud data. In this article, a case study of Jesses ChatLog dataset (University of New Haven, n.d), which has a total of 1100 log records namely in each year 2010 contains 564 logs, 2011 consists of 458 and 2012 consist of 78 log records of chat data by Table 6 suggests that prediction of cloud log based on data ontology and The crimes in cyber attacks the policy for Intelligence in Cloud Forensics will preventive measures to be taken with use AI and Machine learning methods. The evidence collections play a critical role in case investigations. Forensic intelligence that enables critical analysis.

The data through the network send to cloud storage, the cloud data analysis, and analyze data, the machine learning helps to analyze the cloud data. The data is very much useful to make decisions, and cloud computing integrating the devices and applications in various sections.

Table 6. JessesChat Logs dataset log activity keywords analysis

Log activity records	Keywords in log	Ontology Keyword	Predicting suspicious activity based on Prediction
Aug 2010 31 logs	now answering, invite, video call, offline, sweet, course, ideas, good, party, scooters, food, tonight, go, new post, laptop, doing, smart, radio, excited, amazing, online, think, online, music, status, house, offline, busy, online, ride, avoid, check, going, confirmed, go down, today, cool, video call, file transfer, screen, canceled, birthday, <i>hacked</i> , talking, going, hungry, lazy, school,	hacked	The system or data hacked
Dec 2010 49 logs	possible, offline, relative, online, Christmas, bight, computer, tv, today, sleep, pick, eating, entertainment, called, call police, hello, oh my god, burgers, laughed, scary, cute, money, thank you, real, tonight, idle, online, oh god, i love, cool	call police	Criminal activity investigation is required

CONCLUSION AND FUTURE SCOPE

Collect data for the investigation process in a situation where hypervisors, snapshots as forensic data. The Crucial business process, SLA, security, forensic investigation, best practices, external systems with encryption and provide security in logs. Forensic investigation is running live and shutdown systems the Volatile data IaaS, and persistent storage. Virtual introspection are used to future attacks on the system. Forensic specialists follow steps to protect the data evidence such as files, photos, documents, logs, etc, to recover the data, to access possibly and logically to analyze, print and overall analysis to Provide opinion /devices based on data recovery and expert consultation. The Use of computer Forensic investigations are used in a criminal investigations, Civil litigations, Insurance claims, Corporation companies for evidence related to harassment to women's and Law enforcement officials.

Computer Evidence to accelerate, authenticate, complete, precise, convincing and conform with the law. Cloud computing requires security, digital forensic, cloud environment, and reconstructing the environment. The scenarios, hypotheses, in CSP logs and finds evidential artifacts in digital investigations. The CSP, SLA, proves that the investigation in cloud data, these application users must follow set of guidelines like strong passwords, periodically change passwords, two-way authentication layer protections required in OTP in financial transactions. Never share any personal data, and do not click unknown link URL in emails. Do not respond to fake calls asking to share OTP, update KYC, bank calls and Insurance calls. The propped model of cloud forensic cloud-log is implemented in Java and future it extend the model Future Monitoring cyber, Credit card, Fingerprint, digital sign, voice, Iris. The tools in forensic analysis with the use of the tools, review analysis tool to investigate search validate forensic applications. Log files sources running huge applications, where millions of cloud users use the framework which has cloud log data, volume, data investigate and find malicious activities performed by the attacker. Cloud log security, it provides data confidentiality availability and integrity attacker find cloud log and unable to decrypt data. The experiments are conducted in Java Cloud log security encryption, and network data attacks results show the highest attack type is generic, lowest attack type is worms, and moderate attack type exploits. Conducted a case study cloud log using chat log keyword ontology learning process, Natural Language, Machine learning and AI techniques to predict the attacks in advance. The various tools used in the investigation process are discussed.

Cloud log future directions in real-time cloud log visualization, Cloud log forensic API, Cloud log forensic tools, chain of custody. The metadata support forensics, selection of relevant CSP / investigation, correlation of and cloud log.

REFERENCES

- Adam, & Varol. (2020). Intelligence in Digital Forensics Process. In *Proceedings of 8th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE.
- Ahsan, Wahab, Idris, Khan, Bechara, & Choo. (2018). Assurance of Cloud Log in Cloud Forensics System. *IEEE Transactions on Sustainable Computing*, 1-6.
- Aiash, Colson, & Kallash. (2015). Introducing a Hybrid Infrastructure and Information Centric approach for secure Cloud Computing. *Proceedings of International Conference on Advanced Information Networking and Applications*, 154-157. doi:10.1109/WAINA.2015.80
- Bhattacharya, S., S, S. R. K., Maddikunta, P. K. R., Kaluri, R., Singh, S., Gadekallu, T. R., Alazab, M., & Tariq, U. (2020). A Novel PCA-Firefly based XGBoost Classification Model for Intrusion Detection in Networks using GPU. MDPI. *Electronics (Basel)*, 9(2), 1–16. doi:10.3390/electronics9020219
- Birk, D., & Wegener, C. (2011). Technical Challenges of Forensic Investigations in Cloud Computing Environments. In *Proceedings of Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 1-10). IEEE.
- Chen, L., Nhien-An, L.-K. S. S., & Xu, L. (2019). *Cloud Forensics Model, Challenges, and Approaches*. Wiley Online Library.
- Dykstra, J., & Sherman, A. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation, Elsevier*, 9, 90–98. doi:10.1016/j.diin.2012.05.001
- Edington Alex, M., & Kishore, R. (2017). Forensics framework for cloud computing. *Computers & Electrical Engineering, Elsevier*, 60, 193–205. doi:10.1016/j.compeleceng.2017.02.006
- Iwendi, C., Jalil, Z., Javed, A. R., Thippa, R. G., Kaluri, R., Srivastva, G., & Jo, O. (2016). KeySplitWatermark: Zero Watermarking Algorithm for software protection against Cyber-attacks. *IEEE Access: Practical Innovations, Open Solutions*, 4, 1–12.
- Khan, Gani, Wahab, Bagiwa, Shiraz, Khan, Buyya, & Zomaya. (2016). Cloud Log Forensics: Foundations, state of the Art, and Future Directions. *ACM*, 49(1), 1-42.
- Nelson, B., & Amelia, P. F. E. (2011). *Christopher stunts*. Computer Forensic and Investigation. Cengage Learning.
- Petrescu, A., & Patriciu, V.-V. (2014). Logging System for Cloud Computing Forensic Environments. *CEAI*, 16(1), 80–88.
- Rani, , Sultana, & Saravana. (2016). Challenges of Digital Forensics in Cloud Computing Environment. *Indian Journal of Science and Technology*, 9(17), 1–7.
- Ruan, K. (2013). *Cybercrime and Cloud Forensics: Applications for Investigation Processes*. IGI Global.
- Runa, Cathy, Kichadi, & Crosby. (2011). Cloud Forensics. In *Proceedings of IFIP International Federation for Information Processing*, (AICT 361, pp. 35-46). Academic Press.
- Sheik, K. A. M., & Lalitha Bhaskari, D. (2016). Cloud Forensics A Framework for Investigating Cyber attacks in Cloud Environment. *Procedia Computer Science*, 85, 149–154. doi:10.1016/j.procs.2016.05.202
- Simou, Kulonates, Grizzlies, & Mouridi. (n.d.). *A survey on cloud forensics challenges and solutions: Security and Communication Networks*. John Wiley & Sons, Ltd.
- Swarna, P. R. M., Bhattacharya, S., Praveen, K. R. M., Siva, R. K. S., Lakshmana, K., Kaluri, R., Hussien, A., & Gadekallu, T. R. (2020). Load Balancing of energy cloud using wind driven and firefly algorithms in internet of everything. *Journal of Parallel and Distributed Computing, Elsevier*, 142, 16–26. doi:10.1016/j.jpdc.2020.02.010
- The Best Open Source Digital Forensic Tools. (2018). *H-11 Digital Forensics*. <https://h11dfs.com/the-best-open-source-digital-forensic-tools/>
- The University of New South Wales. (n.d.). *The UNSW-NB15 Dataset Description*. Retrieved December 22, 2018, from <https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/index.php>

Times of India. (n.d.). *Cybercrime*. Retrieved December 21, 2020, from <https://timesofindia.indiatimes.com/topic/cybercrime>

Vice. (2012). *Computer Forensic Computer Crime scene investigation*. Firewall Media.

M. Swami Das is working as an Associate Professor in CSE dept, CVR College of Engineering, Hyderabad. He completed B E(CSE) in 1998 from CBIT, (affiliated to Osmania University), Hyderabad, and M Tech (CS), from JNTU Kakinada in 2002, and Passed Ph.D. in JNTUH Hyderabad. He has 20 years of Experience in Teaching, Industry, and Research. His research interests are Web services, Forensic Applications, Cloud computing, IoT, and Data mining.

A. Govardhan (PhD) is presently a Professor of Computer Science & Engineering, Rector and Executive Council Member, Jawaharlal Nehru Technological University Hyderabad (JNTUH), India. He served and held several Academic and Administrative positions including Registrar I/c., Principal (JNTUH CEH), Director (School of Information Technology, JNTUH), Director of Evaluation (JNTUH), Principal (JNTUH CEJ), Head of the Department (JNTUH CEH), Chairman and Member of Boards of Studies and Students' Advisor. He is the recipient of 33 International/ National Awards and Merit Scholarships including Inspiring Educationist Award (2019), Dr. APJ Abdul Kalam Excellency Award (2018), Best Senior Scientist Award (2018), Dewang Mehta Academic Leadership Award (2017), Dr. Sarvepalli Radhakrishnan National Award, A.P. State Government Best Teacher Award (2012), Pride of Asia International Award, Best Principal, Bharat Seva Ratna Puraskar, CSI Chapter Patron Award, CSI Service Award, Bharat Jyoti Award, International Intellectual Development Award and Mother Teresa Award for Outstanding Services, Achievements, Contributions, Meritorious Services, Outstanding Performance and Remarkable Role in the field of Education and Service to the Nation. He is a Member on Advisory Boards/ Academic Boards/ Technical Program Committee Member for more than 100 International/ National Conferences. He has guided 90 Ph.D theses, 1 M.Phil and 135 M.Tech projects. He has published 555 research papers at International/National Journals/Conferences including IEEE, ACM, Springer, Elsevier, IGI Global, Taylor & Francis and InderScience. He has organized 5 International Conferences, 25 FDPs/Workshops. He has delivered more than 150 Keynote speeches and invited lectures on various latest topics including Data science, Information Retrieval Systems, Cyber Security, Art of Doing Research, National Educational Policy-2020. He served as a panel member in more than 25 panel discussions. He has Chaired 22 Sessions at the International/ National Conferences in India and Abroad. He has the Research Projects (Completed/ Ongoing). He was the Institute Project Director during TEQIP-II and TEQIP-III including a Centre of Excellence in Disaster Management. He has 26 years of Teaching and Research experience. His areas of research include Databases, Data Science, Security, Information Retrieval Systems and Educational Leadership. He is a Fellow (CSI and IEI), Life Member/ Senior Member/ Member in several Professional and Service Oriented Bodies including ISTE, CSI, ISCA, ACM, IEEE, IAENG, WASET, FSF, ISOC and IACSIT.

D. Vijaya Lakshmi is working as a Professor and Head of the Dept of IT, MGIT, Hyderabad. She received a Ph.D. from JNTUH, Hyderabad, is a member of MEACSE, IJCAR. She is holding Games and Sports Committee Convener, Presiding Officer in Women Welfare Cell, MGIT. She is guiding four research scholars in JNTUH Hyderabad. Her research areas include image processing, web services, data mining and security. She has more than 25 years experience in teaching, research and administration.