ABSTRACT

Cloud computing is emerging as a powerful business solution having the potential to provide an abstraction between the computing resource and its underlying technical architecture. The pay per use concept of this technology provides an economic solution to many IT companies. With the increase in criminal acts, computer forensics has emerged as a necessary discipline in information technology. Forensics practices have been in existence over the last few decades, but they came into the limelight in the recent decade as cyber crimes and the involvement of digital devices in crimes is increasing drastically. Computer forensics has its footprint in every field of information technology, thus helping law enforcement and military to track criminals. Computer forensics is advancing with practices, tools, procedures etc, but it faces many challenges when dealing with cloud computing.

This project identifies the challenges of conventional digital forensics in cloud environment and suggests possible solutions. As cloud computing is a client-server model, this project focuses on forensic analysis of both the client and cloud provider environment. The project developed a prototype called trusted monitoring system which provides necessary evidence for investigators at the provider side. Forensic analysis at the client side indulged the analysis of three freeware cloud tools Cloudatag, QTweb and Amazon cloud drive, using conventional forensic tool like FTK.
# TABLE OF CONTENTS

Abstract .................................................................................................................. ii

Table of Contents ................................................................................................... iii

List of Figures .......................................................................................................... v

List of Tables ........................................................................................................... vii

1. Background and Rationale ................................................................................... 1
   1.1 Cloud Computing .............................................................................................. 1
   1.2 Cloud Computing Service Models ................................................................. 2
       1.2.1 Infrastructure as a Service ........................................................................ 2
       1.2.2 Software as a Service ............................................................................. 2
       1.2.3 Platform as a Service ............................................................................. 3
   1.3 Security Issues In Cloud Computing ............................................................ 3
       1.1.4.1 Security of System and Database ....................................................... 3
       1.1.4.2 Networking Security ........................................................................... 4
       1.1.4.3 User Authentication .......................................................................... 6
       1.1.4.4 Data Security on Cloud Side ............................................................... 7

2. Narrative ................................................................................................................ 9
   2.1 Technical Constraints Challenging Cloud Forensics .................................. 10
       2.1.1 Location .................................................................................................. 10
       2.1.2 Time ....................................................................................................... 10
   2.2 Forensic Analysis Challenges in Cloud Computing .................................... 11
       2.2.1 Identifying the Structure of the Computing Environment .................. 11
           2.2.1.1 Temporal Extent .......................................................................... 12
2.2.1.2 Spatial Extent .................................................................12
2.2.1.3 Dependency Analysis .....................................................12
2.2.2 Attribution of Data ...........................................................13
2.2.3 Semantic Integrity .............................................................13
2.2.4 Stability of Evidence ........................................................14
2.2.5 Presentation and Visualization of Evidence .........................14
2.2.6 Cross-Jurisdictional Aspects ............................................15
2.3 Proposed Solution to the Challenges ......................................15
3. System Design .....................................................................19
3.1 Implementation at Cloud Provider Side ................................19
3.1.1 Media Manager Application ............................................20
3.1.2 Trusted Monitoring System .............................................27
3.2 Forensic Analysis at Client Side ..........................................30
3.2.1 Cloudatag Media Manager ............................................30
3.2.2 Amazon Cloud Drive ..................................................31
3.2.3 QT Web Browser ..........................................................32
4. Testing and Evaluation ........................................................34
4.1 Testing Methodology ..........................................................34
4.2 Forensic Tool Used: FTK ..................................................34
4.3 Testing at Provider Side ....................................................34
4.4 Forensic Analysis at Client Side .........................................39
4.4.1 Forensic Analysis of Amazon Cloud Drive Using FTK ..........39
4.4.2 Forensic Analysis of Cloudatag Using FTK ......................44
4.4.3 Forensic Analysis of QT Web Browser Using FTK……………………………….44

4.5 Evaluation of Results…………………………………………………………………….55

5. Conclusion and Future work………………………………………………………………56

Bibliography and References………………………………………………………………57

Appendix A……………………………………………………………………………………59
LIST OF FIGURES

Figure 1: User Login Page………………………………………………………………………21
Figure 2: New User Register Form……………………………………………………………...22
Figure 3: User Home Screen…………………………………………………………………..22
Figure 4: Upload Image………………………………………………………………………….23
Figure 5: User Photo Gallery…………………………………………………………………….23
Figure 6: Image Download………………………………………………………………………24
Figure 7: Admin Login Page…………………………………………………………………….24
Figure 8: Registered Users………………………………………………………………………25
Figure 9: Images Uploaded Record……………………………………………………………..25
Figure 10: Users Download Activity……………………………………………………………26
Figure 11: Password Reset for User……………………………………………………………..27
Figure 12: Violated Image Size Upload (Rule 1)………………………………………………28
Figure 13: Over Limit Upload Record (Rule 2)………………………………………………...29
Figure 14: Over Limit Download Record (Rule 3)……………………………………………..29
Figure 15: Forbidden Ip Activity (Rule 4)………………………………………………………30
Figure 16: Uploading Images to Cloud…………………………………………………………31
Figure 17: Media on Cloud……………………………………………………………………..31
Figure 18: Home screen of Amazon MP3 Uploader…………………………………………32
Figure 19: QT Web Browser……………………………………………………………………33
Figure 20: Uploading 826KB image………………………………………………………………35
Figure 21: Log entry for rule 1 violation………………………………………………………35
Figure 22: Log entry for rule 2 violation………………………………………………………36
Figure 23: Log entry for rule 3 violation………………………………………………………37
Figure 24: Log entry for rule 4 violation………………………………………………………38
Figure 25: Start a New Case Dialog Box……………………………………………………..39
Figure 26: Creating New Case…………………………………………………………………40
Figure 27: FTK Case Log Options .................................................................40
Figure 28: Refining the case data……………………………………………………………...41
Figure 29: Adding evidence from image of drive……………………………………………..42
Figure 30: Analyzing evidence of Amazon MP3 Uploader…………………………………43
Figure 31: Music files uploading details retrieved……………………………………………..44
Figure 32: Cloudatag Analysis Case…………………………………………………………45
Figure 33: Adding the cloudatag evidence for analysis………………………………………..45
Figure 34: Hex format view of cl2.jpg image…………………………………………………46
Figure 35: Native view of the Lighthouse.jpg image………………………………………...47
Figure 36: Filtered Text format view of Lighthouse.jpg image………………………………48
Figure 37: QT web browser forensic case start……………………………………………….49
Figure 38: Adding the evidence………………………………………………………………50
Figure 39: List of files retrieved from evidence………………………………………………51
Figure 40: Data extracted from cookies file…………………………………………………..52
Figure 41: Extracting browsing history from history file……………………………………53
LIST OF TABLES

Table 1: Evaluation of Results............................................................54
1. BACKGROUND AND RATIONALE

1.1 Cloud Computing

Cloud computing is an internet based computing paradigm in which software, information and shared resources are provided to users only on demand, resulting in optimized resource management. In this paradigm, services are provided to users by the cloud service providers and only upon client’s demand. These resources are allocated like public utilities similar to electricity. This computing paradigm provides a new supplement, consumption and delivery model to the present internet based IT services. The service involves a dynamic service delivery system and virtualized resources.

Cloud computing facilitates business applications to customers on their demand. Here business applications are accessed by customers from another Web service that can be a browser or software. Services such as software and data are stored on servers and allocated upon request. Generally, services are hosted in virtual data centers. So the virtualized data centers act as back end platforms for this computing paradigm [Edwards 2009].

Technically cloud computing can be defined as “a computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction” [Bhardwaj 2010]. The cloud paradigm has five main characteristics - broad network access, on-demand self-service, rapid elasticity, resource pooling, and measured service. The infrastructure of cloud computing mainly consists of reliable services which are delivered through virtualized data centers and built on servers [Edwards 2009].
1.2 Cloud Computing Service Models

Cloud computing is all about moving the services like data, computation, etc for the purpose of cost and business advantage from a global transparent location to requested internal locations. Resources at centralized location are easy to access and are cost effective, thus increasing opportunities for enhanced analysis, integration and collaboration on a common single platform [Jiyi 2010]. Based on the type of service provided, the architecture of cloud computing is categorized into three service models Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

1.2.1 Infrastructure as a Service

This single tenant cloud layer caters customers a platform virtualized environment as service. The cloud computing resources are shared to contracted clients at pay per use basis. Rather than owning a server, networking devices, software, data, etc the clients request cloud computing vendors for completely outsourced services. This to a great extent minimizes the client’s infrastructural investment. The flexibility in terms of finance and functionality makes this service model a best solution for reducing the infrastructural cost and efficient management of client’s ever changing requirements which is difficult to achieve using internal resources or co-location services [Ramgovind 2010].

1.2.2 Software as a Service

This type of service provides software as service to requested clients. The model also operates in virtualized environment and prefers to use pay per use pricing model. Thereby, the cloud computing vendors lease the software and software applications to contracted clients. The SaaS software services are generally deployed over the web or behind the firewall to run on client’s computer [Jiyi 2010]. The traditional way is accessing software remotely via web browser. This service allows customization of software based on client’s requirement and the billing is done accordingly. The SaaS vendors can host the software on their own data
centers or with co-location vendors or they may be outsourced to IaaS vendors. As access to Saas services is through a web browser, the browser security is a major concern and a precaution to the Saas providers. Most Saas vendors enable web services security, data encryption and secure socket layer certificates for delivering software or software applications over the web in a secure manner [Ramgovind 2010].

1.2.3 Platform as a Service

Platform as a Service provides development environment as a service. In PaaS, an individual can use the middleman equipment and develop his own programs. Users can access programs that are developed directly through the internet and using other servers on which these programs are hosted. Platform as a service is similar to IaaS (Information as a service) but, it provides additional functionality. The virtual machine in PaaS layer acts as a catalyst. The virtual machines in the PaaS layer must be protected against malicious attacks in PaaS layer. Extra care must be taken in PaaS layer while transferring the data across different network channels by performing authentication checks and maintaining integrity of data. The client using PaaS service must transfer most of their investments from capital to the operational expenditure. The client must agree to the lock-in and additional constraints that are imposed by the additional functional layers [Ramgovind 2010].

1.3 Security Issues In Cloud Computing

1.3.1 Security of System and Database

In cloud computing, the server and the database in the front end must be trusted to utilize the services offered. After this condition is met, the enterprise can then utilize the services that are offered by the cloud computing. As a result, the goals of enterprise such as reducing budget, storage costs and costs associated with manipulating requirements for personnel or enterprise is achieved. The enterprise or personnel can utilize the services that are offered by the cloud computing by storing their data on the storage that is provided by the
ISP (Internet Service Provider). Hence, by storing the data on the remote side, the enterprise or personnel can cut down their costs. Confidentiality, integrity and authentication play a very important role in services that are offered by cloud computing on the remote side. In order to protect the intranet from internet hacking, analyzing the attacking behavior is mandatory. A honey net can be deployed on to an intranet. A honey net contains many honey pots that store important information regarding personnel wage, salary, development projects military information or critical news that are stored in the server or the database. In cloud computing, within the intranet there are some dedicated folders that are used for both monitoring and tracing illegal activities. This folder also records the visiting frequency of hackers, tracks that have been accessed by the hackers. After a careful analysis of the complete hacking information, enhancement of the design of IDS (Intrusion Detection Systems) and IPS is done and is used to fix the leakages and vulnerabilities in cloud computing [Tsai 2007].

1.3.2 Networking Security

To utilize the services that are offered by cloud computing, a kind of communication mechanism is required. In some scenarios, the service providers of cloud computing provide a separate leased line to communicate with the enterprise. It is the duty of the service provider, to guarantee both encryption and authentication of data in communication. Unless there is a physical leak in the dedicated lines, this mechanism provides guaranteed security in communication. The enterprise that utilizes the services provided by the cloud computing not only has the threat from the internet hacking, but also has implicit threats, such as data being stolen or forged by its employees. The information security that is guaranteed by the service provider plays a crucial role in the decision taken by the enterprise in utilizing the services offered by cloud computing. In order to achieve better security, the service provider and the enterprise has to reach an agreement called SLA (Service Level Agreement). In a service
level agreement, quality of service, information assurance and service security are clearly defined. This SLA prevents leaking and spoofing of confidential business information. The agreement must follow certain terms before implementation [Tsai 2007]:

1) Before utilizing the services offered by cloud computing, the enterprise has to be aware of the service requirement.

2) The cost and price associated with the service must be flexible and the service content must be easily accessible.

3) Ask the service provider to give the detailed physical implementation of system security and operating systems environment in the enterprise.

4) Evaluate the service provider based on problem management and handling information security events.

The enterprise/user must be satisfied with the terms that are mentioned in the SLA. If the enterprise is satisfied with the terms laid in SLA, then guaranteed information security can be promoted and enhanced [Tsai 2007]. In order to provide security in small size and medium size enterprises, VPN (Virtual Private Networks) are used by many service providers. In recent emerging applications in wireless communication, the concern on Information security management and policies has dramatically increased. The restriction on communication media has been lowered. There is no restriction that the communication media must be wired, pair-wise, coaxial cable etc. There are many advantages associated with wireless networks such as lower costs, lower power consumption, and higher flexibility. Despite the advantages, it is vulnerable to spoofing, cracking and interception. The information security is more of a concern in wireless systems compared to wired systems. In 802.11 ‘n’ wireless networks the data rate in communication is 300 Mbps. In 802.11 ‘n’ wireless networks, the data rate has increased five times to that of 802.11g [Tsai 2007]. Due to this high data transfer rates, the access points with memory can be used as a server for
wireless networking. These kinds of network policies attract or lure hackers to attack the enterprise network without any notice. In 802.16 WiMAX, the employee of an organization can easily access the desired server through networking and download his intended files [Tsai 2007]. In wireless networks, the signal is transmitted through air, thus the information can be easily spoofed, intercepted and sniffed. If an enterprise is using wireless networking, the security aspect of this network can be suspected. A lot of research is now being focused on capturing the transmitted packets and trying to crack them. This is the best way to find out vulnerabilities in wireless networks. This helps in formulating policies for information security [Tsai 2007].

1.3.3 User Authentication

The management of user accounts and their corresponding privileges play a key role in cloud computing. Some enterprises use Single Sign on (SSO) to access systems. In some Enterprises, each user will be given different accounts to access different systems. This multi-authentication is often confronted in an enterprise. The accounts associated with the individuals can be similar or different. It depends on how the administrator sets privileges to that user. Single Sign on (SSO), which was adopted by many companies, has now become a single point of risk. It all depends on how the administrator sets privileges on the users to access the system resources. The main goal is to provide information security without any leakage of information and loss of confidential and sensitive information. Using IAM (Identity Access Management), enterprise can formulate management mechanisms for handling identification, authentication and authorization simultaneously. IAM is now more focused on security and availability. The benefits of using IAM include reducing IT costs, authentication, access control, authorization, increasing productivity and decreasing the complexity in user identification. The enterprise uses consolidate foundation of user authentication to provide and enhance authentication in wired equipments. A better
authentication can be established in wireless communication using hashing and registration to achieve non-repudiation and data integrity. In Open authorization, every user can access the networking system by entering the username and password provided by the previous or present Internet Service Provider (ISP). It has many advantages which include authorization for third parties to access the network by typing user name and password. Thus, individual users can authenticate their pictures or graphics to print using the printing service web server via networking [Tsai 2007].

1.3.4 Data Security on Cloud Side

Starting with IaaS at the bottom, PaaS at the middle and SaaS at the top, the cloud storage always play a key role in implementing cloud computing application. A large size cloud computing must support dynamic requirements and also added functionality that is requested by the enterprise. In Micro Blogging, such as Twitter, it allows to store millions of users’ information on S3 (Simple Storage Service). For a general user of a cloud computing service, it is easy to find out the possible storage [Tsai 2007].

The most common protocols used to achieve the services of cloud computing are HTTP (Hyper Text Transfer Protocol), HTTPS (Hyper Text Transfer Protocol Secure) to achieve information security and data integrity, and Secure Shell. The data security at the cloud side is not only focused on data transmission, but also on the system protection and data protection on the data that is stored in the cloud. If there are many users at the cloud side, the service providers must mainly focus on the database and file management. The service provider at the cloud side must provide all assurances regarding the storage and system protection for those users accessing the cloud computing service. The service providers should be cautious of system crash or storage loss. The data stored at the cloud side should be protected from unauthorized users or intruders or even the employees of the enterprise. The service provider gives assurance of system protection and data integrity. The
enterprise evaluates the storage loss, data loss and networking problems at the cloud side. The service provider presents the purchase procedure, abolishment procedure, and management of storage for the third party that plays the role of supervisory for auditing. The user of cloud computing adheres to some physical specifications in retrieval of data in the storage at the cloud side. If there is any abolishment at the cloud side, recording the location, demagnetizing, verifying and recycling provides necessary evidence or reference. Data at Rest (adapting encryption, authorization and authentication) is adapted for data security at cloud side. The enterprise performs encryption and authentication before uploading the file on the server. After performing encryption the file is stored in the location designated by the service provider through a secure channel. IaaS only offers this mechanism. If security is the major concern, the IaaS (Information as a Service) is the best choice [Tsai 2007].
2. NARRATIVE

Cloud computing is emerging as a major step change of IT strategic development and implementation. The major adoption of cloud computing is creating vast challenges to digital forensic investigators. In traditional forensic investigations, the investigation is carried out on a particular domain where the components suspected to be involved in crime, are within a range or boundary which is well defined. But, in cloud environment the scenario is different. Consistently configured infrastructure is less available, which poses a serious challenge for investigators. The forensic analysis in the cloud environment can be defined as an art of applying digital forensic techniques to gather evidence or digital artifacts from the cloud, for the purpose of preservation and presentation of evidences in the court for legal process [Zimmerman 2011]. The forensic analysis in clouds applies to the traditional forensic process which is divided into four steps [Zimmerman 2011]:

1. Collection: The evidences which may be digital or necessary supporting documents are acquired using forensic tools.

2. Preservation: Preserving the collected artifacts in a way that they are accurate, verifiable, complete and reliable.

3. Filtering: Analyzing the acquired artifacts and involving or removing data based on their importance in case.

4. Presentation: Presenting the accurate and complete acquired data to the law court for the legal process.

But the major challenge to apply this traditional approach for analysis in the cloud is combining the locations which are physically and logically located. The locations in the cloud computing environment are distinguished as client side, provider side and combined side. The basic challenge involved is to provide accurate and complete forensic data from the cloud to prove misuse of service. Bit by bit, copy of the image is not possible in cloud. So, the
snapshots of the cloud data should be taken and cloud logs access should be recreated. Proving that presented data denotes the event occurred accurately is also a crucial challenge in cloud forensics [Zimmerman 2011].

2.1 Technical Constraints Challenging Cloud Forensics

The key constraints of cloud computing which pose a serious challenge to traditional forensic approach are location and time [Zimmerman 2011].

2.1.1 Location

The first step of forensic investigation is locating the suspected device. In case of cloud computing, only traces of device would be of virtual machine as there exists, no physical device involved. This VM can reside anywhere dispersed over several physical locations and also the disk unit which stores the data, may be emptied or particular data may be deleted from it. And access to particular cloud storage would require judicial orders etc based on the location of the cloud vendor organization [Zimmerman 2011].

2.1.2 Time

In cloud environment there always exists dilemma in terms of timestamps. Once after the source for data is identified, testing and matching the timestamps of all entities acquired during investigation is a major challenge for the investigators. Synchronization of clocks using the network timing protocol is not adopted by most of the cloud vendors, which is why forensic investigators have difficulty in presenting timestamps of the evidence [Zimmerman 2011].

These technical constraints of cloud environment limit the traditional forensic analysis capabilities in cloud. The traditional forensic analysis is categorized as static analysis and live analysis. It is not accurate or complete in cloud, as finding the data location is impossible when asked for and without acquisition analysis it is of no use. So, there is a need for hybrid analysis technique for forensic analysis in cloud environment. The hybrid tool must be
capable of predicting artifacts based on forensic heuristic. It differs from traditional tool in the way of collecting the data. The tool must be able to visualize the logical and physical locations where acquisition is a challenge. Visualization must include both obtainable and unobtainable evidences, such that it eases the collection and presentation. The hybrid tool should be capable of using cloud as a discovery engine for forensic analysis and heuristics. Signature based and heuristic based analysis should be carried out for unobtainable artifacts. The proposed prototype would address the technical challenges of traditional forensic tools to an extent but there exists many other forensic analysis challenges that should be addressed [Zimmerman 2011].

2.2 Forensic Analysis Challenges in Cloud Computing

Performing forensics investigations on the evolving computing platform is a major challenge. Also challenging is keeping pace with the best methods of investigation and standards of evidence. Following are the research challenges most of the investigators have to face [Wolthusen 2009].

2.2.1 Identifying the Structure of the Computing Environment

In situations where the evidence resides on a specific location, identifying the computing environment and analyzing a single computer is time saving. But when the environment comprises of distributed systems, the evidence cannot be found with certainty, as memory is distributed among several computing systems. The first and foremost task of an investigator is to determine the structure of the distributed systems that need to be investigated [Wolthusen 2009].

An alternative is to duplicate the entire storage area of the distributed systems. But, this would result in extraneous volumes of memory [Wolthusen 2009]. These systems cannot be seized leading to loss of productivity and company policy violations. The appropriate choice is to interpret the data by introducing methodologies to describe the range of services,
computations and the documents using temporal extent and semantic context.

2.2.1.1 Temporal Extent

The snapshot of the state of data and the services which need to be investigated should be established to safeguard the reliability of the methods of investigation. At all times data is subjected to changes or restricted access due to the hierarchy of storage levels. Consequently, the events on the computing environment must be captured in entirety before they are changed. In order to capture data events should be associated with partial ordering. The consistent state is established before the inter-dependant events affect the volatile and transitory processes resulting in modified structure of the distributed systems [Wolthusen 2009].

2.2.1.2 Spatial Extent

In situations where the evidence needs to be seized or is subjected to changes, determining the location where the evidence resides is significant. It is challenging to determine the location when data is managed by an authority. In Distributed systems the details of the location are made unknown to the users [Wolthusen 2009]. Adversaries can make good use of this advantage. To determine the conditional data of the evidence, the information used to reduce latency and increase bandwidth of the location forms the conditional information. This information can be made available to determine direct evidence and locations [Wolthusen 2009].

2.2.1.3 Dependency Analysis

In the cloud environment, the dependencies of processes and the way they are distributed among systems need to be analyzed in addition to the temporal extent of the data. If the investigation requires capturing the semantic dependencies of the data, the data responsible to create the process and the semantics information at the time of an event which includes information related to ontology, analysis structures and data dictionaries must be
considered [Wolthusen 2009].

2.2.2 Attribution of Data

It is important to obtain attributions of the data in cases where digital signatures are used to protect the documents while maintaining the practices of public key framework. But if the certificates or the chains of certificates become outdated the attributions also become conditional. This leads to differences in the time frame of the data obtained and its signatures. Due to the limitations of attribution more conditional information of the data must be captured which is the log files with least protection levels, the public key service which is the communication information obtained through the usage of the data, name services and the methods that reveal the web services used [Wolthusen 2009]. The major challenge is obtaining the communication services and the interaction information among the entities for cryptographically protected and unprotected communication. The ordering of the events significantly affects the process behavior which is why attributions and orderings must be established. The reliability of the attributions also depends on their quality.

2.2.3 Semantic Integrity

Although the data and the data structures may be concealed, overwritten or deleted, the snapshot of data is trustworthy in digital forensics where the environment has a single system. In distributed systems the evidence is documented and stored. The limitations in the scope of semantics of the snapshot of data have reliability levels similar to the data. For instance, in databases the information of dynamic structures is not available but the related structural information is available in the relational databases which may not be sufficient [Wolthusen 2009].

The evidence is stored in the form of data and the development of the data model of the target machine continues, as the semantic information and the data do not match completely. Developing methods to obtain semantic information is extremely important to
confidently infer the data. When this inferred data is used analysis and reasoning must be performed visibly as the collection, analysis and the presentation of data is limited [Wolthusen 2009].

2.2.4 Stability of Evidence

To preserve the stability of evidence in the long run along with obtaining or inferring the data is a key challenge. To retain the semantic information for a long time is more important as data can become invalid even when it is protected cryptographically. The instantiations of operational specifications of files and data objects provide complete understanding of data while specifications of revision and type information cannot be complete. It may be a complex task to obtain the operational information or specifications of data on distributed systems [Wolthusen 2009]. The best solution is to capture and determine the complete extensional information and methods to describe semantic information while preserving the data sets in the long run.

Streaming videos or system data flow which constitute to the short term data also encounters the stability of evidence problem. The semantic information of the data is interpreted by the process nodes which require obtaining the system state. Collection of evidence must be performed on the end-point devices to determine the evidence during retention of data on remote end points [Wolthusen 2009].

2.2.5 Presentation and Visualization of Evidence

The aspects considered to face the challenges of production of evidence in the distributed systems are intricacy of the data and limits of trustworthiness on single data sets and their interpretation. The examination of the data can be performed by interactive presentation of the data and visualization of the environment without causing reinvestigations of data and jeopardy of questions involving documents related to the data. But, the temporal extent, semantics and specifications of the data cause multiple formats and presentation
methods of the data. Moreover, to investigate and document relational databases, data work flow and process efficiency, presentation and methods of visualization must be considered. Along with the real data, limitations of aggregation methods, interpreting and producing semantics of data with certainty and gaps in the data must be measured. To resolve these issues the uncertainties and results of investigations (including assumptions) must be documented evidently in situations where presentation and visualization methods are used to analyze statistically, validate and form interactive hypothesis [Wolthusen 2009]. Presentation methods along with the pattern matching and tools that statistically analyze data sets and their actions must be used in cases where complex data such as media files are meant to be united, synchronized and reconstructed while reconstruction of complex data cannot be performed due to gaps and exclusion of raw data [Wolthusen 2009].

2.2.6 Cross-Jurisdictional Aspects

During the investigations and storage of data, the theories of data processing in distributed systems are prone to exceed the national borders. The legal connotations of these theories must be considered whether the study of forensics deals with criminal, compliance or civil cases. The European and International Interpol strive to co-ordinate the aggregation and management of the digital evidence [Wolthusen 2009]. In the process of avoiding the investigation risk, discovering the location and the jurisdiction of the data is more challenging. The accessibility or the ability to aggregate the data is limited by the various standards of collection, type of events and retention of data. If the limitation is not recognized, the accessibility of the overall data is at risk even when the technical issues are resolved [Wolthusen 2009].

2.3 Proposed Solution to the Challenges

When a company decides to outsource its data storage and services to an outside cloud provider, then its landscape becomes a little bit simpler. The information that is present in the
cloud is not limited like in documents and ESI (Electronically Stored Information). The data of a particular company now is not only stored on the servers that is owned by that company, but is also stored on different servers on many networks, hosted across many countries. The cloud computing in this way provides many advantages to the individual forensics investigators and also to the entire team. There are many risks and obstacles involved in moving the entire applications to the cloud environment. This makes the enterprise that is involved in moving the applications to cloud environment, to carefully examine the risks involved, the security infrastructure, oversight ability and contractual obligations [Barbara 2010]. The enterprise must present to the vendor involved in data management, with legal and security requirements, based on the information or data that is being stored or transacted. The enterprise must take every step to protect the property and also secure its information. There are legal departments that get involved in this process in helping the enterprise to secure its information. The legal requirements are made a part of the contact by the enterprise. The business in any event must make sure that the vendor is meeting up with the requirements [Barbara 2010].

A forensics server can be used for a dedicated purpose in the company cloud. This dedicated forensics server is placed offline and can be made available whenever necessary. This gives a cost-effective solution because the company does not face the logistical challenges that are involved. In an enterprise, distribution of workload is done by giving a copy of virtual machines to different incident responders. This occurs when new sources of evidence arise, and then a need for analysis at enterprise level occurs. To reduce the evidence acquisition time, whenever it is known that a particular cloud is compromised, then cloning is performed on that server at an instance of click of mouse. In this way this cloned disk is available to the forensic server for the investigation purpose. If the hardware is being abstracted from the datacenter, then the process of forensics investigation might further get
slowed down. If the system has to be slowed down for a slight time period when search for data is going on, then the hardware has to be abstracted from the datacenters [Barbara 2010].

Cloud computing avoids the operations disruptions and service downtime. There are some cloud implementations that try to expose the cryptographic checksum or hash, such as the MD-5 hash and Amazon S3 generation. These are exposed whenever an object is stored. Due to this exposure, the need to perform the MD-5 checksum using the other available external tools is eliminated. As the checksums are already present, the forensics image verification time is reduced in the forensic investigation [Barbara 2010]. The customer who uses cloud services has to only pay as long as they are using the services like the storage and so on. Bit by bit copies are now made fast with the advancement in the file systems, replication and distribution. Due to the increase in the speed of the CPU in the cloud computing process, the forensics investigators can now test a wide range of passwords. This is made possible because accessing the documents has now become very much quick with the advancements in the technologies [Barbara 2010].

By performing the Forensic Readiness and synchronization of data inside the cloud, the challenges can be overcome [Ahmed 2010]. With proper planning and use of IMS (Identity Management Systems), handling of the evidence data of the customer, without going into the customer personnel data can be done. In such systems, the encryption procedures, Key management procedures and IDS (Intrusion Detection Systems) will prevent the problem from going into reality. Instead of using all these mentioned procedures, standardizing the Metadata can be dealt with. All the applications that reside in the cloud have the standard API that supports the forensics tool composure. A standard procedure must be adapted for the signature metrics and FMD (File Meta Data) to test the validity of the application profiles [Barbara 2010].

Much Research have to be yet focused on developing the Language independent
disks, byte stream object processing and Disks, IP packets, sectors etc. Identification procedures and File reorganization procedures have to be improvised. There should be many improvements in stream based forensics, which can be used for analyzing the hard drive without reorganizing the files on the disk. There should be a standard mechanism in which a standard representation for the email addresses, their names and time stamps, should be included. To speed the partial analysis much research has to be yet focused on stochastic analysis and random sampling. The major challenges lie in improvising the live analysis feature [Zimmerman 2010]. Improving the logging feature, their generation and analysis is also a must. Different departments in Forensics analysis have come together and formulate the common laws.
3. SYSTEM DESIGN

Location and time are two major forensic constraints in cloud environment [Zimmerman 2011]. Based on the location constraint the project was divided into two phases. In the first phase a prototype called trust monitoring system was deployed on the provider server. In the second phase, some freeware cloud tools were analyzed for evidences using conventional forensic tools at the client side. At the provider side, as a precaution before cure, a forensic server which acts like a trusted monitoring system was deployed.

The system logs and audits cloud activity periodically to provide solutions to the non-existent data in the cloud. The forensic server provides proof of compliance to vendors or court jury when a crime is committed in the cloud. At the client side, the forensic analysis of some freeware cloud computing tools like QT Web browser, Cloudatag and Amazon Cloud Drive is performed with the conventional forensic tool FTK.

3.1 Implementation at Cloud Provider Side

The implementation of the project at the provider side is based on trusted computing. A trust monitoring system is installed on the provider side application which handles the media files. The trusted monitoring system based on security policies of the application, logs and audits user violated rules. Trusted monitoring system acts as a forensic server when there is need for forensic analysis in the cloud environment. The deployment of the monitoring system on application server could provide proof of compliance to the owner of the application or to the court jury when certain access or security policies are violated.

The project is mainly about developing a prototype trusted monitoring system for a cloud computing application called Media Manager. The complete test scenario is developed using PHP and MySQL database is used to maintain data. The media application is hosted on cloudsystem.co.cc domain.
3.1.1 Media Manager Application:

Media Manager application is simple server software that provides simple user friendly interface to upload and download images. The service is a simple image hosting service where the clients register and start store media files. This application is similar in functionality to the existing Cloudatag [Cloudatag 2011] media tool.

In order to provide security assurance to media being stored, the application uses data protection measures like authentication and authorization of users accessing the data. Each user is allocated account credentials using which he can upload and download images to the server. There exist terms of usage of the service and a mutual contract between the provider and client. Every client in order to access the application has to agree upon it. Any violation of the terms included in the agreement policy are logged and audited by the trust monitoring system. After certain attempts of violation the user account is deactivated. Thus, the project aims at providing precaution before cure and later provides necessary evidence in terms of log documents during forensic analysis. The Media Manager application on which the trusted monitoring system is deployed has the following functionalities:

1. The user is authenticated to access the application based on his account credentials.
2. The user can upload media to his cloud account and store them in cloud for later use.
3. The user can download the images from his account using download option.

These are the basic activities that a user can do in this image manager application. But, before a user registers for an account in the application, he has to agree upon “Terms of Usage” which includes the trusted monitoring system logging the violated activity. The terms of usage of the service in this application include four rules:

1. The maximum size of the image that can be uploaded is 50 KB.
2. The client can upload a maximum of 10 images per minute. If this limit is violated the server will refuse to accept any more images. If this term is violated more than 10 times then the account will be cancelled.

3. When downloading images a maximum of 15 images per minute, if this limit is exceeded the server allows it, but the monitoring tool detects it in order to raise a flag for the account, as downloading more than 15 images in less than one minute indicates high traffic.

4. Sharing individual credentials is forbidden. IP addresses are recorded, and accessing the server with too many different addresses is recorded as violation.

The application is registered as cloudsystems.co.cc and provided with the user and admin modules.

**User module:** The user module handles the functionalities like user login, upload, download, password change and logout as shown in Figure 1 through Figure 6.

![User Login Page](image.png)

**Figure 1: User Login Page**
Figure 2: New User Register Form

Figure 3: User Home Screen
Figure 4: Upload Image

Figure 5: User Photo Gallery
Admin Module: The Admin module is for the administrator of the application who can view the registered user records, images uploaded, downloaded, add new users and password reset as illustrated in Figure 7 through Figure 11.
Figure 8: Registered Users

Figure 9: Images Uploaded Record
Figure 10: Users Download Activity
3.1.2 Trusted Monitoring System

The prototype trusted monitoring system, called TMA in the project, is deployed on the Media Manager application server. The trusted monitoring system is based on terms of usage mentioned in section 3.1.1, logs and audits user violated rules. The system actively monitors Media Manager application activity and records the four rules violations. The four rules considered as violation are:

1. Image size greater than 50KB.
2. Uploading more than ten images per minute.
3. Downloading more fifteen images per min.
4. Ip Block

The number of uploads and downloads are exceeding the maximum limit is considered a violation, so as to prevent high traffic and attempt to denial of service attacks on the application server. Similarly, Ip Block rule is implemented to provide data protection and
to guarantee cloud clients high data security. Ip Block rule implementation will prevent access to the application or data by unauthorized users like previous employees of an enterprise or remote access. Thus, the deployment of trust monitoring system on cloud application provides proof of compliance to the cloud provider.

All the violation rules are logged in the form of tables. Each rule is associated with a table in the system. Violated over limit upload criterion logs rule 2, described above. Similarly, violated max size logs rule 1 violation. Violated over download logs rule 3 and forbidden IP rule 4. On any violation, the system logs basic details of the incident like time of violation, username, ip address. In case of upload-download limits, the system logs the number of over the limit images count. For forbidden ip address rule, the forbidden ip address from which unauthorized access was attempted is logged. Each rule violation is illustrated in Figure 12 through Figure 15.

![Figure 12: Violated Image Size Upload (Rule 1)]
**Figure 13: Over Limit Upload Record (Rule 2)**

<table>
<thead>
<tr>
<th>User</th>
<th>Ip Address</th>
<th>Total Image Violated</th>
<th>Image Upload Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>68.206.115.196</td>
<td>12</td>
<td>2011-06-25 23:36:43</td>
</tr>
<tr>
<td>david</td>
<td>68.206.115.196</td>
<td>10</td>
<td>2011-06-25 03:40:13</td>
</tr>
<tr>
<td>dhris</td>
<td>68.206.115.196</td>
<td>14</td>
<td>2011-06-25 14:34:12</td>
</tr>
<tr>
<td>war</td>
<td>68.206.115.196</td>
<td>13</td>
<td>2011-06-25 00:24:52</td>
</tr>
</tbody>
</table>

**Figure 14: Over Limit Download Record (Rule 3)**

<table>
<thead>
<tr>
<th>User</th>
<th>Ip Address</th>
<th>Total Downloaded Image</th>
<th>Total Downloaded Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhris</td>
<td>68.206.115.196</td>
<td>5</td>
<td>2011-06-25 08:04:21</td>
</tr>
<tr>
<td>war</td>
<td>68.206.115.196</td>
<td>22</td>
<td>2011-06-25 03:38:14</td>
</tr>
</tbody>
</table>
3.2 Forensic Analysis at Client Side:

The second phase of project involves forensic analysis of some freeware cloud tools like QT web browser [QT 2010], Cloudatag [Cloudatag 2011] and Amazon Cloud Drive [Amazon 2011] using the conventional forensic tool FTK. This phase mainly focuses on acquiring evidences and data on client side. The freeware cloud tools are analyzed for evidences like incase of QT web browser, the browsing history and cache, media information in case of Cloudatag and Amazon cloud drive.

3.2.1 Cloudatag Media Manager

Cloudatag is a simple, flexible and open source cloud media application facilitating the user to upload and store pictures in the cloud. Cloudatag is used to optimize storage service and improve efficiency. It provides 1GB free space for photos and videos. To start using Cloudatag, an account is to be created by the user and then the desktop application is downloaded and installed. As soon as the application is installed, the user can login and start importing media onto cloud [Cloudatag 2011].
3.2.2 Amazon Cloud Drive

Amazon cloud drive is a new cloud storage device launched by Amazon. It provides
storage space to user files, media etc on Amazon’s servers. It offers 5GB of free online storage space. Any extra space would cost the user one dollar per gigabyte for a particular year. Any type of data can be stored on Amazon cloud drive due to its storage capacity. Media like music can be uploaded to cloud through Amazon mp3 desktop software provided by Amazon [Amazon 2011].

![Figure 18](image) [Amazon 2011]: Home screen of Amazon MP3 Uploader

### 3.2.3 QT Web Internet Browser

QT web browser application is a lightweight, secure, portable web browser with a simple interface that helps user to implement it in a simple way. It is an open source cloud browser which is based on Nokia's "Qt Framework" and Apple's "WebKit". The latest version that has been upgraded is Version 4.7.2. It provides various privacy and security features are also available which enhances secured access. This browser provides full reset feature which can clear all stored caches. Ad Block is yet another important security feature of QT Web browser which is used to hide most disturbing advertisements, and block web counters. It is a
single portable EXE file that can be copied to USB, and can be executed anywhere which makes it user friendly [QT 2011].

Figure 19 [QT 2011]: QT Web Browser
4. Testing and Evaluation

4.1 Testing Methodology

Testing in this project involves two phases: Testing the trust monitoring system functionality and forensic analysis of cloud tools (Cloudatag, Amazon cloud drive and QT web browser) with the conventional forensic tool FTK. The forensic analysis was performed with administrative privileges on a Windows 7 system with sufficient RAM. Testing of prototype trust monitoring system deployed over Media Manager application is performed by considering 4 test cases. Test cases for each violated rule were designed and tested.

4.2 Forensic Tool Used: FTK

The forensic toolkit by AccessData [AccessData 2011] is considered to be the standard conventional forensic tool. FTK is a well recognized computer forensic tool available to licensed users. Analysis and evidences acquired using FTK can be directly provided to the court as proof of compliance i.e. it is a court validated computer forensic tool. FTK provides reliable and cutting edge analysis with customizable user-friendly interface. Its implementation provides flexible search indexes and effective data reporting. To analyze deleted documents, images or media files sophisticated approaches are implemented [Garfinkel 2007].

4.3 Testing at Provider side

Testing at cloud provider side involved testing for violation of the four rules mentioned in section 3.1.2. Proper logging and auditing of these violations in the TMA server is a major testing constraint considered. For each violation rule, a test case was built to verify proper working of the trust monitoring system. For testing, user account David is considered for the media manager application. Through his account, all the rules will be violated for testing the trusted monitoring system functionality. Following are the test cases that use detailed procedures to test the functionality of the deployed prototype trusted monitoring
System.

Test Case 1:

Tests whether upload of an image greater than 50KB in size is violating the terms of usage.

Input: Through David account uploading an 826KB image is shown in Figure 20.

Figure 20: Uploading 826KB Image

Output: TMA system logs the violation rule attempted by David in the Violated Max Size Upload table as shown in Figure 21.

Figure 21: Log Entry for Rule 1 Violation
**Test Case 2:**

Testing whether ten per min upload rule violation is working as per design.

Input: From *David* account uploaded 12 images of mixed sizes.

Output: TMA system logs the violation rule 2 attempted by *David* in the Violated over limit upload table as shown in Figure 22. Here the numbers of images uploaded over the limit are presented as Total Images which is two in this case.

![Figure 22: Log Entry for Rule 2 Violation](image)

**Test Case 3:**

Testing whether download of more than 15 images per min is violating the terms of usage as per design.

Input: From *David* account downloading 21 images and expecting an entry of six violated image count in Violated over download image table.

Output: TMA system logs the violation rule 3 attempted by *David* in the Violated download table as shown in Figure 23. Here the numbers of images downloaded over the limit are presented as total downloaded images. In this case the count is 6.
Figure 23: Log entry for rule 3 violation

**Test Case 4:**

Tests working of IP block on user account *David*. The user was initially registered from the ip address 68.206.115.196. In order to test the forbidden ip rule the account is accessed from the ip address 64.71.89.23.

Output: This violation is logged in Forbidden Ip table as shown in Figure 24. The entry shows the Ip address used to gain unauthorized access along with authenticated Ip address.
Figure 24: Log Entry for Rule 4 Violation
4.4 Forensic Analysis at Client Side

4.4.1 Forensic Analysis of Amazon Cloud Drive using FTK

Step 1: Starting a new case in FTK Forensic Toolkit.

![Image of FTK Forensic Toolkit interface]

**Figure 25: Start a New Case Dialog Box**

Step 2: Filling up Investigation Details:

**Investigator Name:** Druha

**Case Number:** 1

**Case Path:** c:\amazonclouddriveanalysis
Step 3: Checking case log options

Figure 27 shows the different logs options that can be checked for logging the case into the default FTK.log test file. In this project all the options are checked as the data that will be analyzed is not known.
Step 4: Refining the data

Figure 28 shows the different options that can be selected for refining and eliminating unwanted data analysis. In this project all file types are selected because Amazon cloud drive supports storage of documents, music and video.

Step 5: Adding the evidence for forensic analysis
Figure 29: Adding evidence from image of drive

Figure 29 shows the location of evidence from which the evidence for analysis is imported. In this case the C:\ disk image is taken for locating Amazon mp3 up loader activity log.

Step 6: Analysis of Evidence

In this step the evidence imported in add evidence step is analyzed and the data present in the evidence is displayed in the right most dialog box.
Figure 30: Analyzing evidence of Amazon MP3 Uploader

Figure 30 shows the information present in the evidence folder amulog.txt. This data retrieved from the amulog.txt file is very informative for investigation, as it provides session start timestamp, operating system used, Air version and when scrolled down the files uploaded, their location and many other significant details.
Figure 31: Music files uploading details retrieved

Figure 31 shows the mp3 music album details uploaded onto the cloud. It clearly provides complete source path for the music album updated. The timestamp of upload, album display name and track of complete process of upload is highlighted.

4.4.2 Forensic Analysis of Cloudata
g

Similar testing procedure to that of Amazon cloud drive has been followed to carryout forensic analysis in cloudata application. Forensic analysis of Cloudata using FTK acquired the media that was uploaded from local account to cloud account.

The forensic analysis snapshots are as follows:
Figure 32: Cloudata Analysis Case

Figure 32 shows the start of cloudata analysis case. In this the investigator name, case number and case folder where the analysis results will be stored are entered.

Figure 33: Adding the cloudata evidence for analysis

Figure 33 shows the path of the cloudata evidence folder which is used for data analysis. In this case the evidence is extracted from program files where the cloudata desktop
application is stored.

Figure 34: Hex format view of cl2.jpg image

Figure 34 shows all the different type of images that ever uploaded from local machine to cloud. The Hex format view of image cl2.jpg is presented in the data analysis pane.
Figure 35: Native view of the Lighthouse.jpg image.

Figure 35 shows the lighthouse.jpg image in its native format i.e. the image format in cloud. This format provides investigators the cloud storage view of the image.
Figure 36: Filtered Text format view of Lighthouse.jpg image

Figure 36 shows filtered text view of the graphic image lighthouse.jpg. This view filters and displays the basic information about the data in this case about the .jpg image.

4.4.3 Forensic analysis of QT Web browser using FTK:

Similar forensic analysis procedure to that of Cloudatag, Amazon cloud drive is followed. The only difference will be the type of evidence being analyzed. As QT web browser tool is a browser, the main concern of investigators will be to analyze the cookies, browsing history, passwords etc.
Figure 37: QT web browser forensic case start

Figure 37 shows the first step of the QT browser case. The basic details like investigator name, case number and analyzed data path is entered.
Figure 38: Adding the evidence

Figure 38 shows the path of the evidence to be analyzed for acquiring cookies and history data of the browser. In this case the evidence is retrieved from Program Files/QTweb.
Figure 39 shows the list of files retrieved when FTK tool is run on QTweb. The files retrieved are cookies, history and icon. The list of files clearly serves the purpose of investigation, as cookies data, browser history exists.
Figure 40: Data extracted from cookies file

Figure 40 shows the data extracted from the cookies file. The important cookie information like timestamp, domain name, path, pref id etc is retrieved from this data.
Figure 41: Extracting browsing history from history file

Figure 41 shows the browsing history of the QT web browser. It is automatically listing all the URL’s visited. In this snapshot all the wiki and Google links visited are listed.
4.5 Evaluation of Results

Table 1 shows the different test cases considered and results obtained with forensic analysis. The initial four test cases are performed on the provider side to test the working of trusted monitoring system in logging and auditing the violation rules. These test case outputs confirmed the correctness of the monitoring system. The last three test cases were mainly designed to carry out forensic analysis using FTK and to retrieve necessary information. The analysis retrieved crucial information like media file path, cookies, browsing history, media files, and URL visited etc. The experimentation met the expected results thus making the forensic analysis testing positive.

**Table 1: Forensic Analysis Test cases and Results**

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Tool/Prototype</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>826KB image upload</td>
<td>Trusted Monitoring System</td>
<td>Max size update rule violated&lt;br&gt;Log entry for rule 1 violation is updated in TMA.</td>
</tr>
<tr>
<td>12 images upload in one min</td>
<td>Trusted Monitoring System</td>
<td>Over the limit upload rule violated&lt;br&gt;Log entry for rule 2 violation is updated in TMA.</td>
</tr>
<tr>
<td>21 images download in one min</td>
<td>Trusted Monitoring System</td>
<td>Over the limit download rule violated&lt;br&gt;Log entry for rule 3 violation is updated.</td>
</tr>
<tr>
<td>User account <em>David</em> forbidden access</td>
<td>Trusted Monitoring System</td>
<td>Forbidden Ip address rule violated&lt;br&gt;Log entry of forbidden ip</td>
</tr>
<tr>
<td>Analysis of Amazon cloud drive</td>
<td>FTK</td>
<td>Information like path of media file, OS, AIR version, album display name, process status, time of upload retrieved.</td>
</tr>
<tr>
<td>Analysis of Cloudatag</td>
<td>FTK</td>
<td>Retrieved media file data such as all formats of images uploaded to cloud. Presented different views of evidence like Hex view, native and filtered view.</td>
</tr>
<tr>
<td>Analysis of QT web browser</td>
<td>FTK</td>
<td>Retrieved cookies, browsing history, URL’s visited.</td>
</tr>
</tbody>
</table>
5. CONCLUSION AND FUTURE WORK

The project contributes to the practice of forensic analysis in cloud by providing a prototype trust monitoring system which could become capable of providing proof of compliance to criminal court jury and by analyzing some freeware cloud tools with conventional forensic tool FTK. This project highlighted several forensic challenges in cloud environment and addressed some of the challenges like data non-existence by providing the prototype trusted monitoring system. The forensic analysis of cloud tools using FTK extracted major evidences like cookie information, timestamp of media files uploaded to cloud etc. Forensic analysis at both provider and client sides enhance understanding of the cloud system from a forensic perspective. Future work could be the customization and implementation of the trusted monitoring system prototype by both small and big scale cloud providers. As location is the major constraint in cloud, there is a need for a hybrid tool that could perform both static and live analysis. There still exist many technical challenges associated with forensic analysis in cloud environment that need to be well researched and effectively addressed.
BIBLIOGRAPHY AND REFERENCES


APPENDIX A. Partial Code of Prototype Trust Monitoring System

// Violation of max size image upload and upload limit

if(move_uploaded_file($_FILES['uploaded']['tmp_name'], $target))
{
    "The file ", basename( $_FILES['uploadedfile']['name']). " has been uploaded"
;

    $query="INSERT INTO
    upload(username,title,description,name,type,ip_address,image_upload_time,login_id)
    VALUES
    (".$username."",".$title."",".$dis."",".$fileName."",".$fileSize."",".$ip."",".$date."",".$id.");"
    mysql_query($query) or die("error");

    $event_time =mysql_query("SELECT min(image_upload_time) as image_upload_time
    FROM upload
    WHERE image_upload_time>(SELECT login_time FROM user_login where
    user_name=""."$_SESSION['sess_user'].""");
    $row=mysql_fetch_array($event_time);

    $min_time=$row['image_upload_time'];

    $t=mysql_query("SELECT count(login_id) as id,type FROM upload WHERE
    image_upload_time BETWEEN ".".$min_time."" AND ".".$min_time."" + INTERVAL 10
    MINUTE");
    $check=mysql_fetch_array($t);

    $idd=$check['id'];
    $setip=mysql_query("SELECT DISTINCT (ip_address) FROM upload WHERE
    image_upload_time
    BETWEEN ".".$min_time."" AND ".".$min_time."" + INTERVAL 10 MINUTE
    LIMIT 2 , 30");
    $ipaddress=mysql_fetch_array($setip);
    $ipd=$ipaddress['ip_address'];
    //echo $ipd;
    $insip=mysql_query("INSERT INTO
    violation_ip(user_name,title,description,name,image_upload_time,ip_address)(SELECT
    user_name, title, desc
    ription, name, ip_addreee, image_upload_time
    FROM user_login l, upload u
    WHERE l.id = u.login_id AND ip_address IN($ipd) LIMIT 2, 30");
    if($ip==$ipaddress)
    {
        if($idd<=10 && $fileSize<=50000)
        {

    59
$fu="INSERT INTO finalupload
(username,title,description,name,type,image_upload_time,login_id,ip_address)VALUES(".$username",".".$title",".".$dis",".".$fileName",".".$fileSize",".".$date",".".$id",".".$ip"))";

mysql_query($fu);

$_SESSION['sess_mg']='OK, Image Uploaded:--'.Sidd;
}
else{
$result="INSERT INTO finalvioletedupload
(title,description,name,image_upload_time,login_id,ip_address)VALUES(".$title",".".$dis",".".$fileName",".".$date",".".$id",".".$ip")";

mysql_query($result);

$_SESSION['sess_mg']='Uploaded image size violation';
}
else{
$iv="INSERT INTO violation_ip(user_name,name,image_upload_time,ip_address,fip)
VALUES(".$username",".".$fileName",".".$date",".".$ip",".".$ipaddress")";
mysql_query($iv);
$_SESSION['sess_mg']='prashant';
}
}

// Violation of download limit
$query="INSERT INTO download(name,login_id,ip_address,download_time) VALUES
(".$fname",".".$id",".".$ip",".".$date")";

mysql_query($query);

$event_time =mysql_query("SELECT min(download_time) as download_time FROM download
WHERE download_time>(SELECT login_time FROM user_login where user_name="'.$_SESSION['sess_user']."')");

$row=mysql_fetch_array($event_time);
$min_time=$row['download_time'];

60
$t=mysql_query("SELECT name,count(login_id) as id FROM download WHERE
download_time BETWEEN ".".$min_time." AND ".".$min_time." + INTERVAL 1
MINUTE");

$check=mysql_fetch_array($t);

$idd=$check['id'];

if($idd<=15)
{

    $fu="INSERT INTO finaldownload
(name,download_time,login_id,ip_address)VALUES( ".".$fname."","".$date."","".$id."","".$ip.""")"
;

    mysql_query($fu);

    $_SESSION['sess_msgg']='Ok,Download Image';

}

else{

    $result="INSERT INTO finalvioleteddownload
(name,download_time,login_id,ip_address)VALUES( ".".$fname."","".$date."","".$id."","".$ip.""")"
;

    mysql_query($result);

    $_SESSION['sess_msgg']='Download Limit Violated';

}

//Forbidden Ip address rule

if($ip==$ipv)
{
    if($idd<=10 & & $fileSize<=50000)
    {

        $fu="INSERT INTO finalupload
(username,title,description,name,type,image_upload_time,login_id,ip_address)VALUES( ".".$username."","".$title."","".$dis."","".$fileName."","".$fileSize."","".$date."","".$id."","".$ip.""")"
;

        mysql_query($fu);

        $_SESSION['sess_mg']='OK, Image Uploaded:--'.+$idd;

    }

}
else{
    $result="INSERT INTO finalvioletedupload
    (title,description,name,image_upload_time,login_id,ip_address)VALUES(".$title."",".$dis.",".
    $fileName."",".$date.",".$id.",".$ip.");"
    mysql_query($result);

    $_SESSION['sess_mg']="Uploaded image size violation';
}
}
else{
    $iv="INSERT INTO violation_ip(user_name,name,image_upload_time,ip_address,fip)
    VALUES (".$username."",".$fileName."",".$date."",".$ipv."",".$ip.");"
    //echo $iv;
    mysql_query($iv);

    $_SESSION['sess_mg']="Forbidden Access';
}
}