CERIAS

The Center for Education and Research in Information Assurance and Security

Digital Forensics Evidence Acquisition In Cloud Storage Service: Examining and evaluating tools and techniques

Student: Gilchan Park / Advisor: Simuel Liles

Project overview

The purpose of this research is to provide an evaluation of proposed forensic acquisition methodologies and tools in cloud storage services and discuss the limits of those existing tools. As the number of users of cloud storage services such as Dropbox, Google Drive, Microsoft SkyDrive, etc rapidly increases, cloud storage has been identified as an emerging challenge to digital forensic researchers and practitioners. With the analysis of current forensic methodologies of cloud storage, it is expected that cloud storage should be enhanced at the aspect of security.

Techniques and Methods

1) INVESTIGATION INTO ARTIFACTS OF CLOUD STORAGE SERVICES [1]

Concept

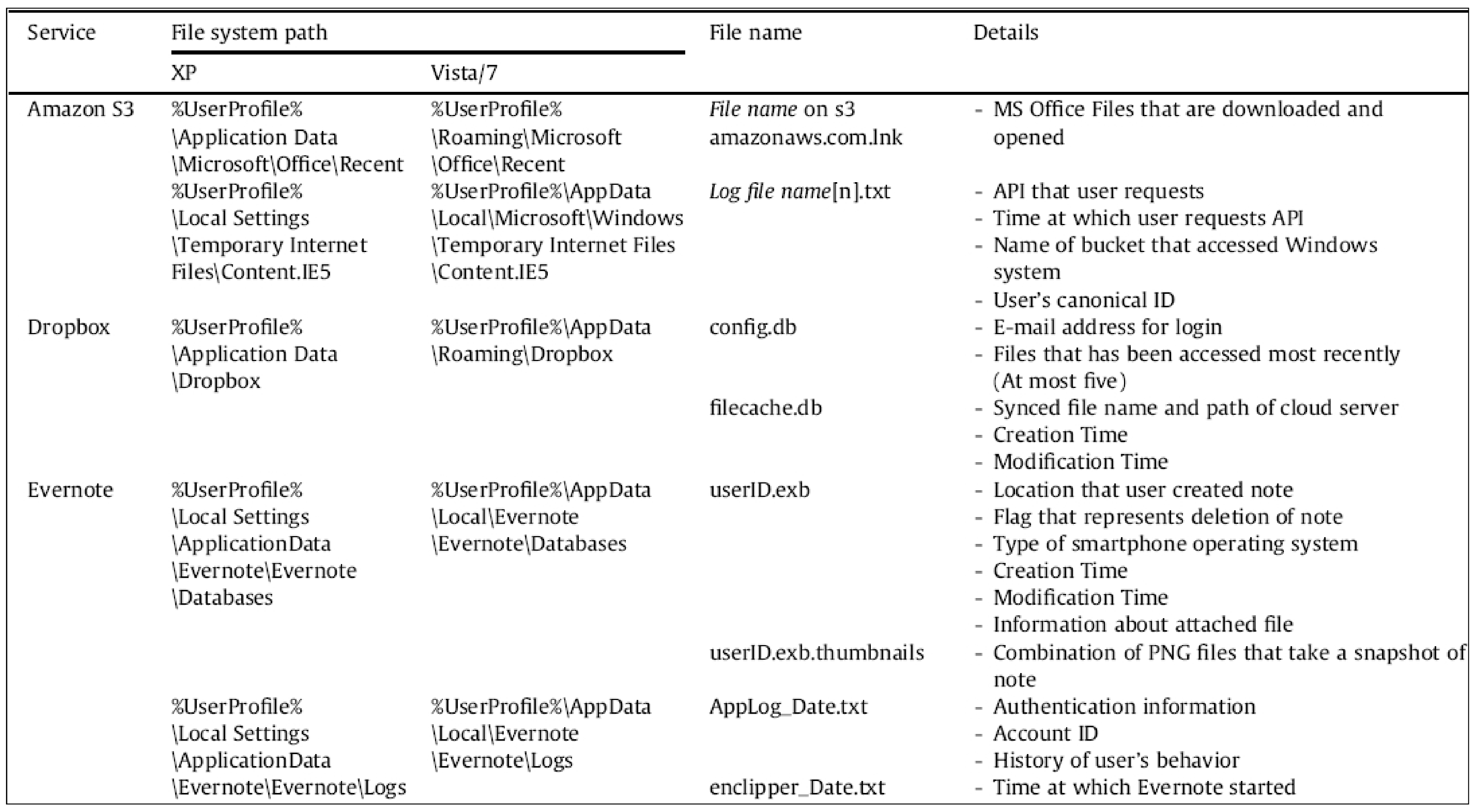
- The collection and analysis of the artifacts of all accessible devices which are log files and database files left by cloud storage applications.
- Examination of the artifacts that contain traces of use of a cloud storage service.

Limitations

- Heavily dependent on third party applications.

  E.g., If cloud service providers refuse providing the decryption key for encrypted artifacts, the forensic examiners cannot gather potential evidence on them.
- Malicious users can simply avoid leaving a trace by manipulating log files.

Artifacts of Cloud Storage Service (Windows)



Service	File system path		File name	Details
	XP	Vista/7		
Amazon S3	%UserProfile% \Application Data \Microsoft\Office\Recent	%UserProfile% \Roaming\Microsoft \Office\Recent	*File name* on s3 amazonaws.com.lnk	- MS Office Files that are downloaded and opened
	%UserProfile% \Local Settings \Temporary Internet Files\Content.IE5	%UserProfile%\AppData \Local\Microsoft\Windows \Temporary Internet Files \Content.IE5	*Log file name*[n].txt	- API that user requests - Time at which user requests API - Name of bucket that accessed Windows system - User's canonical ID
Dropbox	%UserProfile% \Application Data \Dropbox	%UserProfile%\AppData \Roaming\Dropbox	config.db	- E-mail address for login - Files that has been accessed most recently (At most five)
			filecache.db	- Synced file name and path of cloud server - Creation Time - Modification Time
Evernote	%UserProfile% \Local Settings \ApplicationData \Evernote\Evernote \Databases	%UserProfile%\AppData \Local\Evernote \Evernote\Databases	userID.exb	- Location that user created note - Flag that represents deletion of note - Type of smartphone operating system - Creation Time - Modification Time - Information about attached file
			userID.exb.thumbnails	- Combination of PNG files that take a snapshot of note
	%UserProfile% \Local Settings \ApplicationData \Evernote\Evernote\Logs	%UserProfile%\AppData \Local\Evernote \Evernote\Logs	AppLog_Date.txt	- Authentication information - Account ID - History of user's behavior
			enclipper_Date.txt	- Time at which Evernote started

2) DIGITAL FORENSIC SOFTWARE AS A SERVICE (DFSaaS) [2]

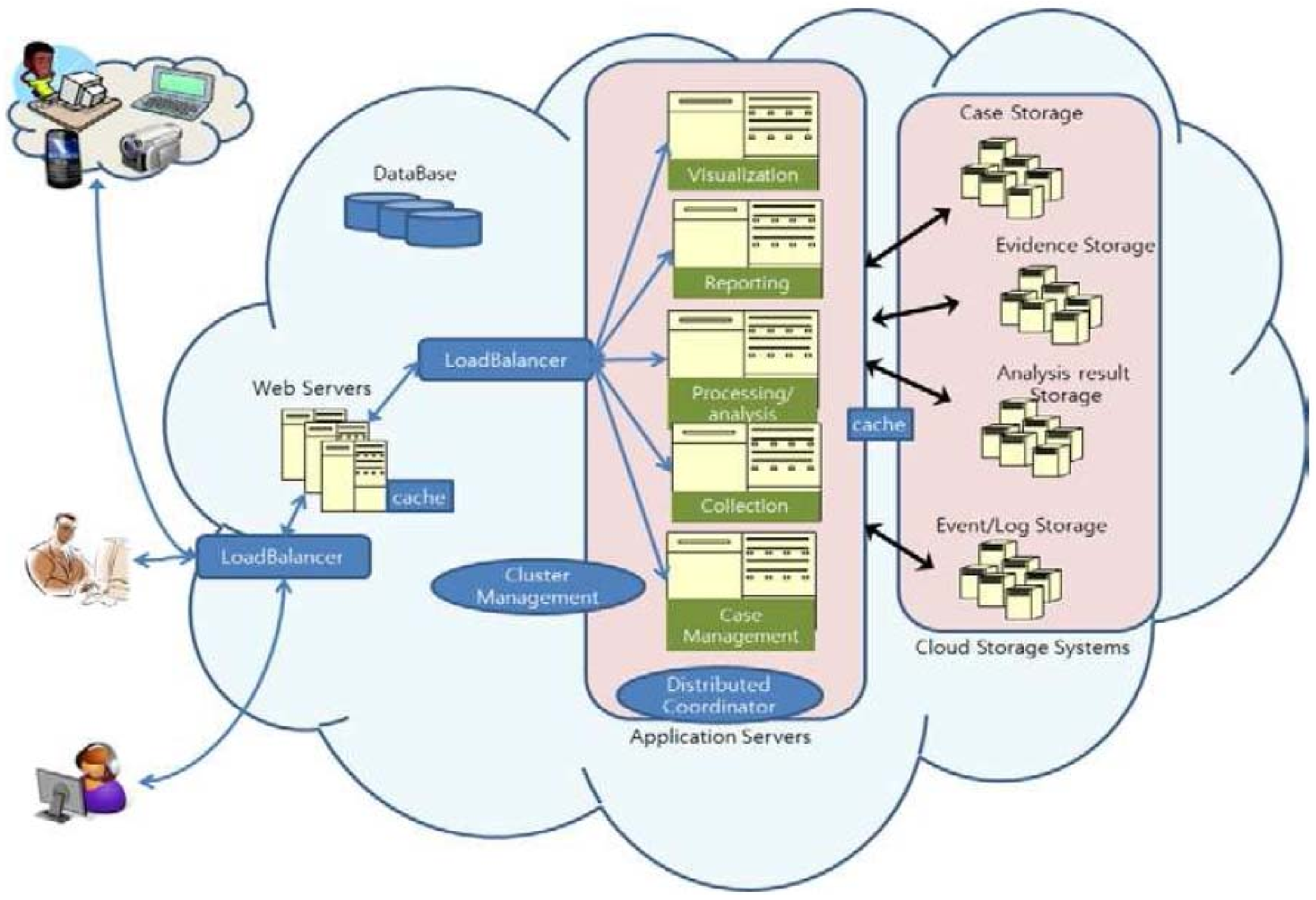
Concept

- The cloud based forensic tool.
- All forensic examiners can analyze collected evidence at the same time provided network connection.
- Fast performance by massive and distributed data processing in cloud computing.

Limitations

- A user authentication has a potential threat to be hacked.
- Uncertainties arising in chain of custody of evidence by allowing multiple analysts to simultaneously access to log files.

DFSaaS architecture



References

- [1] Chung, H., Park, J., Lee, S., & Kang, C. (2012). Digital forensic investigation of cloud storage services. Digital Investigation.
- [2] Koo, B. M., Lee, T. R., Kim, H., & Shin, S. U. (2012). A Study on Digital Forensic Software as a Service on Cloud Computing.

CERIAS

PURDUE UNIVERSITY