FReadyPass: A Digital Forensic Ready Passport to Control Access to Data Across Jurisdictional Boundaries

Philip M. Trenwith[1] and H. S. Venter[2]

University of Pretoria

Department of Computer Science

Pretoria South Africa

Email: ptrenwith@gmail.com[1] Email: heinventer@gmail.com[2]

Abstract

Cloud computing offers users access to information from anywhere by duplicating and distributing information to multiple data centers around the globe. The distribution of information in such a manner presents a significant challenge if the need arises to locate a specific digital object. Such a need could stem from legislation put in place by governments or organization concerned with the protection of sensitive information, such as the European Union's Data Protection Directive, which states that sensitive information should not leave the jurisdiction of the European Union. In this article, the authors look at the requirements for securing sensitive information in the cloud and address many of the challenges associated with cloud forensics. The authors address a critical issue regarding sensitive information and the cloud, that of monitoring and controlling the flow of information across jurisdictional boundaries. The authors propose a model to control the access of information across jurisdictional boundaries, as well as capturing the necessary provenance data to report on the traveling history of a digital object and storing this information in a digital forensic ready manner. Should that object ever be required in a digital forensic investigation, it can easily be located.

Keywords: Digital Forensics, Digital Forensic Readiness, Cloud Computing, Data Provenance, Jurisdiction, Sensitive Information, Access Control

1. Introduction

Cloud computing has become a dominating force in the world of computing; offering many advantages for its users, but it also holds many challenges for digital forensic investigators. One such challenge is the inability to gain physical access to a device in the cloud [1]. Access to a device may be required during a digital forensic investigation (DFI). The physical location of a device in the cloud is most often unknown to investigators, and therefore the traditional DFI search and seizure approach does not scale well in the cloud. The location of an object in the cloud is important if an investigator needs to retrieve that object to present it as evidence in a court of law, especially when it is important to know the jurisdiction for legal purposes. Knowing the location of an object in the cloud can greatly aid the investigator's ability to gain access to that object and perform a live acquisition of the data if required. The history of an object's location constitutes the chain of custody, defined by the U.S. National Institute of Justice (NIJ) as “a process used to maintain and document the chronological history of the evidence” [2].

The research question asked in this paper is stated as follows: “How can a digital object be tracked through the cloud and how can digital space be anchored to physical space to control the access of information across jurisdictional boundaries?”

The goal of this research paper is to investigate how a digital object and its provenance data can be tracked through the cloud and provided to digital forensic investigators upon request. The authors investigate how provenance data can be stored in a digital forensic ready manner. The authors further investigate the design of a location-based access control mechanism to limit the access to information between different judicial areas.

The remainder of this paper is structured as follows. In section 2, the authors discuss cloud computing, digital forensics, data provenance and the data protection directive put in place by the European Union for the protection of sensitive information. The authors look at the requirements for data provenance. These are areas of interest to this research, and the authors require a thorough understanding of these domains to propose and implement a model addressing the research question. In section 3, the authors propose a model to store digital objects and its corresponding data provenance in a digital forensic ready manner. The model also provides location-based access control to limit the access to information between jurisdictions. Section 4 concludes the paper and discuss future work.

2. Background

To successfully determine a solution to the research question it is important to understand the digital forensic investigation process, as well as the known challenges with cloud forensics. Data provenance is discussed, and the authors explain why data provenance is necessary for cloud forensics. Lastly, the authors address the policies and procedures in place for the protection of personal and sensitive information. The policies and procedures are the driving force behind the development of systems aimed at the protection of personal information and, thus, is vital in the motivation leading to the undertaking of this research. In the next section, cloud computing is discussed.

2.1 Cloud Computing

The United States National Institute of Standards and Technology(NIST) defines cloud computing as: “a model for 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” [3]. In the cloud, data is no longer kept in a single location; it is distributed across multiple interconnected networks, making the protection of data much more difficult. Pearson discusses many of the challenges associated with cloud services and the protection of data in these services [4]. If a breach in security occurs, it is often not easily identified, and an investigation is often required. Such an investigation is referred to as a digital forensic investigation and is discussed in the next section.

2.2 Digital Forensics

Digital Forensic Science is defined by Palmer as, “the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” [5]. Digital Forensics consists of a collection of techniques that were originally developed to aid in data recovery. The application of these techniques is used to aid digital forensic investigators in answering questions relating to computer-based crimes. Barbara states that the biggest challenge investigators are faced with in the cloud is to determine the who, what, when, where, how, and why of cloud-based criminal activity [6].

Reilly et. el. refers that the inability to gain physical access to devices in the cloud, to investigate them, is one of the primary obstacles investigators need to overcome in cloud computing environments [1]. This obstacle may be overcome if a CSP follows a proactive approach to digital forensics, continuously collecting logs and keeping track of the history of data and events taking place in the cloud. Such a proactive approach is referred to as Digital Forensic Readiness (DFR) and is defined by Rowlingson as “the ability of an organization to maximise its potential to use digital evidence while minimizing the costs of an investigation” [7]. Birk supports this theory stating: “the history of a digital object, combined with a suitable authentication scheme is crucial information for a digital forensic investigation” [8]. Rowlingson defines a ten-step process to help organizations prepare for possible investigations by capturing potential evidence [7]. Muniswamy-Reddy defines the history of a digital object as data provenance, and this is discussed in the next section [9].

2.3 Data Provenance

Data Provenance reveals valuable information about a digital object, such as when the object was modified, who accessed it and sometimes how it was changed. This information is incredibly valuable in a digital forensic investigation. Lu states that the public will more widely accept cloud computing if data provenance is provided to report on the history of digital objects in the cloud [10]. This is because data provenance provides information that can be used to dispute changes to a digital object in case of a discrepancy.

Some researchers have investigated the use of data provenance in the cloud as a tool for aiding digital forensic investigations [9] [10] [11]. In previous work, the authors proposed a model that captures provenance data from protocols associated with the seven-layer ISO OSI model such as the TCP/IP protocol stack [11]. This data together with network logs from the CSP is used to identify the physical location of objects in the cloud. Muniswamy-Reddy proposed a system, designed to build provenance-aware network storage onto a Provenance-Aware Storage System (PASS) [12]. This system is directly aimed at capturing and storing provenance data but would not scale well to existing cloud services, as it requires the CSP's network to be installed and configured to capture the necessary provenance data. These systems do not provide the cross-platform capabilities and ease of use that the authors are looking for. Therefore, in the next section, the authors discuss what is required from data provenance in a cross-platform system to lead to successful implementation.

Lu identifies three requirements that a provenance record should have, similar to the CIA principles; they are listed as R1 to R3 below [10]. In the work of Shi [13] and Juels [14], a challenge was raised; a requirement exists to provide cryptographic proofs for verifying data integrity within the cloud. From what has been discussed in the article so far, Trenwith addresses the challenges digital forensics investigators are faced with in the cloud and these challenges are addressed as requirement R4 to R7 in the proposed model [11]. The requirements are listed below:

R1. A provenance record needs to be unforgeable.

R2. A provenance record needs to be kept confidential.

R3. The system should maintain the integrity of a provenance record.

R4. A provenance record should show who is responsible for a modification.

R5. A provenance record should show what was modified.

R6. A provenance record should indicate the time of a modification.

R7. A provenance record should show the object's location in the cloud at the time of a modification.

If all provenance records adhere to these requirements, it should contain sufficient information to answer the essential questions digital forensic investigators ask during the process of an investigation. It is essential that the integrity of the provenance data be maintained. To maintain the integrity of the provenance data the authors make use of digital signatures discussed next.

2.4 Digital Signatures

The RSA asymmetric encryption algorithm is used to digitally sign data [15] [16].

To digitally sign, a data object requires an RSA private key, as well as the data object's hash code, referred to as the original hash [17] [18]. The private key is used to encrypt the original hash code of the data object, producing the digital signature. To verify the integrity of a digital object, the digital signature is decrypted with the public key producing the original hash. The digital object is hashed again producing a verification hash code. The integrity of the digital object is verified by comparing the original hash with the verification hash.

In this work the RSA private key and certificate including the public key are stored in a PKCS#12 formatted keystore. The passphrase to access this file is hard-coded into the client-application’s source code. To protect the source code from reverse engineering it is obfuscated and converted to native code. The identity of the client remains secure as long as the keystore file remains secure. If the private key is compromised, the client can simply generate a new RSA key pair.

Apart from keeping track of the history and location of data in the cloud, there are sometimes limitations on who should have access to information and who should be restricted. In the next section, the authors briefly discuss some of the laws and legislation that prohibit the flow of information across jurisdictional boundaries.

2.5 Protection of sensitive data and information in the cloud

Government institutes and global organizations often need to protect sensitive information. To address these needs, laws, and legislation has been put in place to regulate the protection of personal and sensitive information. One of these legislative protocols is the European Union's Data Protection Directive 1995/46/EC. The Data Protection Directive (DPD) applies to the automated processing of personal data, by computer systems. This directive states that no sensitive data may leave the jurisdiction of the European Union. This directive defines sensitive data as any information that can identify a natural person. However, it does not apply to information regarding natural persons involved in illegal activities, security or defence.

The European Union's DPD requires sensitive data to stay within the jurisdiction of the European Union. This requires a method to determine the location of users concerning their jurisdiction. In the next section, the requirement that the proposed model should achieve are stated, and the authors discuss the design of the model. The design takes certain technical limitations and implementations into account.

From what has been discussed in this article so far it is clear that there exists a need to protect personal and sensitive information in the cloud. However, simple laws and legislation stating that data should be kept secure are not enough. Systems are required to enforce the law.

The authors develop such a system. The topics discussed in this section is necessary during the implementation of this system. Data provenance provides information that is often required during a digital forensic investigation, however, this information cannot be used in a court of law unless the integrity of the information is maintained and can be proven to be in-tact. Digital signatures provide the mechanism required to prove the integrity of potential evidence. All of these building blocks fit together in forming the foundation of the Digital Forensic Ready Passport the authors develop in the next section.

3. A Digital Forensic Ready Passport to Control Access to Data Across Jurisdictional Boundaries

In the physical world when a natural person is traveling from one country to another, that person requires a passport, and in some cases a Visa. A passport, issued by an individual's home country, indicates the home country's approval to allow the individual to leave the country. A Visa indicates the visiting country's willingness to allow an individual to enter its borders. The passport and Visa system provides the ability, to a certain extent to track a person's location to within a specific country. The author proposes the design of a forensic ready digital passport referred to as a FReadyPass to encapsulate user data and its provenance. The author further proposes the design of a software system to manage the creation of and access to FReadyPasses. This system, referred to as the FReadyPass system, aims to provide both an access control mechanism(ACM) for jurisdictional access, as well as a tracking system, using provenance data describing encapsulated digital data files to keep track of where the FReadyPass has been. The goal of the ACM is location-based access control referring to a user's physical location, and the granularity of the physical location is at the jurisdictional level. The ACM is discussed in more detail in the next section.

3.1 Location-based Access Control

An IP address identifies a device's location on a network in the same way a street address identifies a house on the street. An IP address assigned to a public service by an Internet Service Provider (ISP) is referred to as a public IP address. A reverse lookup of a public IP address against an IP address database can determine where in the world that IP address is assigned [19]. The Internet Assigned Numbers Authority (IANA) is responsible for the distribution of IP addresses to ISPs around the world [20]. IANA's IP address databases can suffice as a lookup database for the access control mechanism. The legislative requirement as discussed in section 2.5 only requires the determination of a digital object's physical location concerning a judicial area.

In the next section, the authors uses a scenario to define the access control rules that determine if access to content should be granted or denied.

3.1.1 Access Control Rules

Consider Figure 1. A South African CSP has a server S located in Cape Town. The CSP's policy allows only local access; meaning only requests originating from within South African jurisdiction be allowed access to data under the CSP's control. A computer within the borders of South Africa, referred to as local site L, should be granted access to S. However, a computer outside the borders of South Africa, referred to as remote site R, should not be allowed access to S.

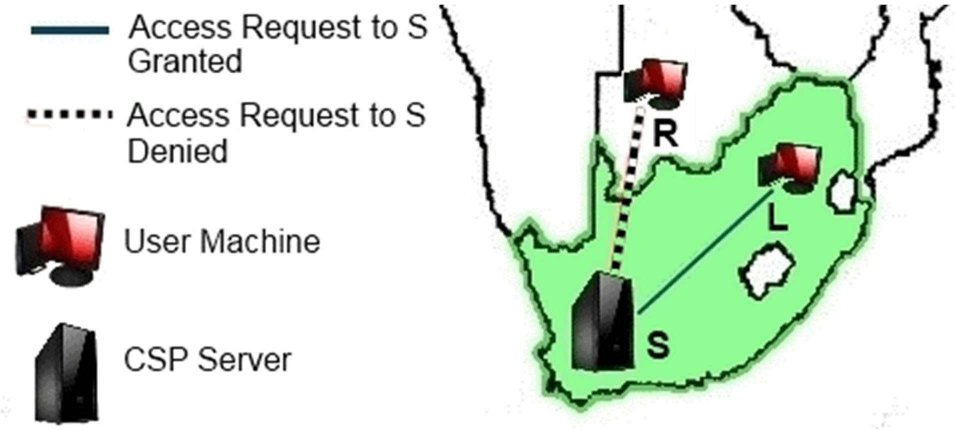


Figure 1: Location based access

From this scenario, it is possible for the author to establish a set of Access Control Rules (ACRs) for the ACM. The ACM requires a set of rules to determine which access requests to grant and which to deny. The list below is the rules the authors find necessary for the given scenario. The → indicates a connection from one machine to another. L → S means a connection to S is requested, originating from L. The server S determines which requests should be granted access (Allowed) or denied access (Not Allowed).

ACR1: L → S = Allowed

ACR2: R → S = Not Allowed

ACR3: R → L → S = Not Allowed

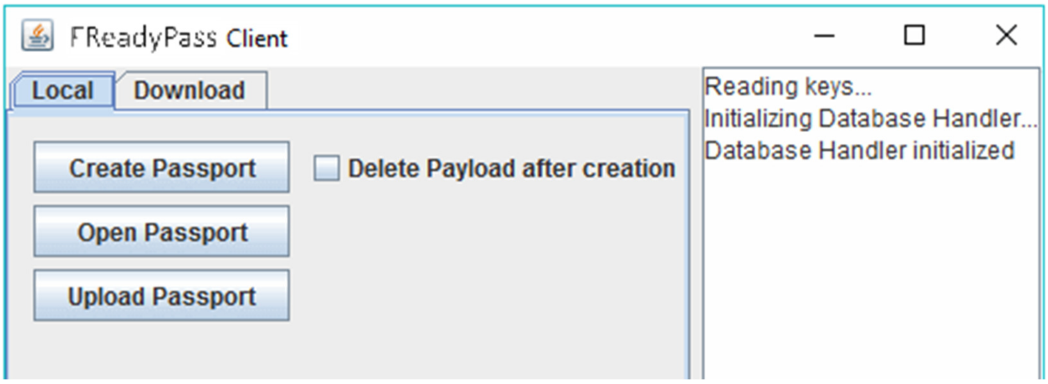
ACR4: L → R → S = Allowed

Any access request originating at a remote site, such as ACR2 and ACR3 should not be allowed because the policy of the CSP only allow access when the request originates from within South African jurisdiction. Therefore, an access request originating from a local site should be granted, even if it is routed through a remote site.

A reverse lookup of the user's IP address should point to the user's ISP. However, the user may be making use of a proxy server. A proxy hides the identity of the requester from the service provider. In the next section, the author proposes a technique to guard against proxies by implementing a 3-way handshake.

3.1.2 Counteracting proxies

When a client connects to a server belonging to a CSP, it is possible for the server to detect the IP address of the device connecting to the server. This may or may not be the public IP address assigned to the client. By establishing a 3-way handshake from the server to the client, it is possible to confirm if the detected IP address is the client's public IP address. For the client device to receive an incoming TCP connection requires a running application on the client able to receive TCP connection requests. The authors design such an application shown in Figure 2.



Reading keys...
Initializing Database Handler...
Database Handler initialized

Figure 2: Client Application

Figure 3 shows how the server initiates a 3-way handshake. The steps in the figure is numbered in the order in which it is executed.

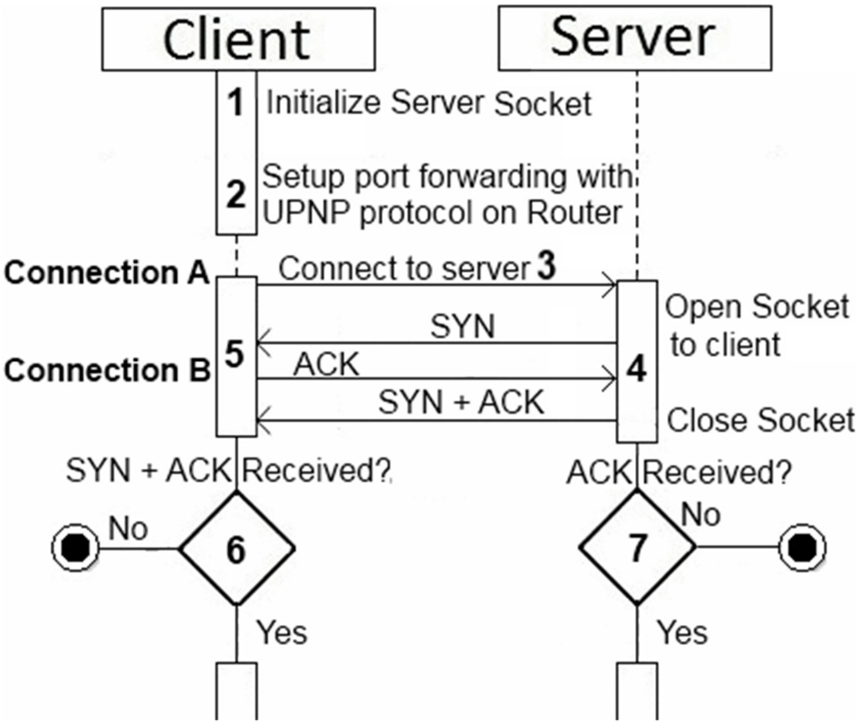


Figure 3: Authenticate a User Connection

Step 1: The client-side application opens a TCP server socket, awaiting a connection from the server.

Step 2: The client application utilizes the UPnP protocol to set up port forwarding on the public router visible from the internet to allow an incoming TCP socket connection to reach the client.

Step 3: The client connects to the server. This connection is Connection A.

Step 4: The server performs a reverse lookup of the IP address from connection A established by the client. The server initiates a 3-way handshake to the client on a predefined port establishing a new connection, referred to as Connection B. If the client is not making use of a proxy, the 3-way handshake will successfully reach the client. If the connection attempt fails, it is likely that the device connected to the server is not the same device that the user is connecting from.

Step 5: The server awaits the establishment of a 3-way handshake.

Step 6 and 7: If the 3-way handshake is unsuccessful, the client and server communication cease.

Connection B is routed through internet routers using routing tables outside the control of the client. It is for this reason that the establishment of a 3-way handshake can verify a client's public IP address.

Initiating Connection B from the server instead of the client grants more control to the CSP regarding the access to data. If a client is utilizing a proxy as shown in Figure 4, the IP address presented to the server during Connection A will not be the client's public IP address. Therefore, during the establishment of the 3-way handshake, the server's *SYN + ACK* will not be sent to the client but the proxy. Thus, the handshake will never be completed. Therefore, the client cannot make use of a proxy. If Connection B cannot be successfully established with the client, the access control mechanism cannot determine the client's location with reasonable certainty. Therefore, the request to access data is denied by the access control mechanism if Connection B fails.

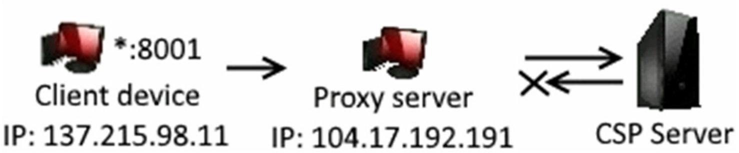


Figure 4: 3-way handshake initiated with a connection routed through a proxy

The use of a client-side application provides additional security benefits including, client-side authentication and the availability of a secure communication channel between the client and the server.

3.2 FReadyPass Architecture

The authors propose the design of FReadyPass containing three parts, shown in Figure 5. Part 1 of the FReadyPass contains the identifier for the FReadyPass. The FReadyPasses under the CSP's control may be legion; therefore, a unique ID is required to distinguish between FReadyPasses. The provenance data describing the history of the user data are stored in part 2 of the FReadyPass. The user data is stored in the payload section, which is part 3 of the FReadyPass. The payload can be any file. The FReadyPass is encrypted to protect the confidentiality and integrity of sensitive data. The FReadyPass also has a header, which indicates the length of the data contained in parts 1 to 3. The header of a FReadyPass is 32 bytes long and is shown in table 1.

Identifier	Provenance Length	Payload Length
16 bytes	8 bytes	8 bytes

Table 1: FReadyPass header architecture

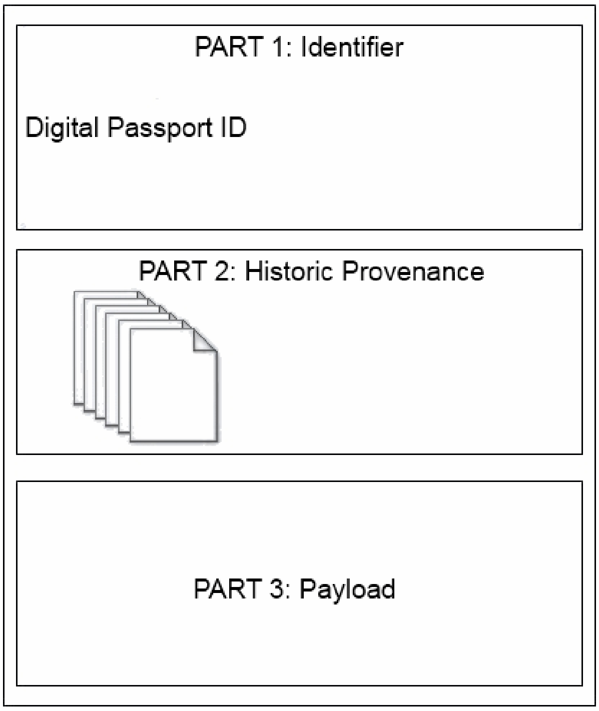


Figure 5: FReadyPass design

In the next section, the authors show how provenance data is stored in the FReadyPass.

3.3 Provenance Data

The provenance data contains information about the state of the user's data as well as its history. The design of the provenance record is shown in the next section.

3.3.1 Provenance Data

Listing 1 shows an example of the design of a provenance record. The XML-file structure is used to store provenance records. To maintain the integrity of the order in which provenance records are produced the provenance records are chained together by making use of the SHA-256 hash algorithm [21]. When a new provenance record numbered provenance record *n*, is produced, the SHA-256 hash code of provenance record *n-1* is included as the value of the Chain field of provenance record *n* as can be seen on line 4 of Listing 1. *n* is the number of the provenance record and is shown on line 6. Line 7 is the type of provenance record. There are three types of provenance records, modification, location-update and verification. The purpose of each type is briefly discussed shortly. Line 8 to 13 shows the identity of the user accessing the FReadyPass. This includes the domain and username of the operating system account as well as the user's CSP account name. The IP address and jurisdiction of the user is captured and shown on line 14 to 16. Line 18 shows the creation time of the provenance record. Line 19 to 21 is the hash code of the payload at the time of the creation of the provenance record. Line 23 to 31 is the digital signature of the ProvenanceData section of the provenance record.

```xml
<ProvenanceRecord>
    <ProvenanceData>
          <Chain>
    08861eb7321747b910570677b4de92da9181097059c370def97bca39f9f3bcfa
          </Chain>
          <Number>2</Number>
          <RecordType>Modification</RecordType>
          <Identity>
                <OSDomain></OSDomain>
                <OSUsername>John</OSUsername>
                <UserAccount>jdoe@gmail.com</UserAccount>
                <MachineName>JohnD-PC</MachineName>
          </Identity>
          <Location>
                <IPAddress>137.215.0.66</IPAddress>
                <Jurisdiction>ZA</Jurisdiction>
          </Location>
          <Timestamp>1430251065774</Timestamp>
          <HashCode>
    78c0c177eeaf438cccbda3aa3226fc4a18a98c2e672800a7ab781efb8e6c485
          </HashCode>
    </ProvenanceData>
    <DigitalSignature>
          B1i+WDjJtu5Bdu7XxOYGWCVPztyMHccvr0Nu8b0V0Y/mxBu68FJaTN
          mZBup4uVQ14pbGUruZvFHLk8VbHVHF+Ltc8sGguNWBOQFSn+buWG
          apNiqaWwtiWuc7nO8BcdQOElUqwH3xHslO500ZajoMETiw1qTqkpd7txZd
          cB+8vA1Lpi9riIAxaWe8Ka79h4iVLwsGjAV9pXicOEO4gy4rwT58MLn4V3
          TPQIwtXYghZsaOvP6E/DDtZbPKTy4GLCpTut94v4ZZZeDXCZpQwhJJ1
          TFFf3tZ8avM2Yp3krNWkEE6FzSI3MPS/OVai1oQhCsoSC/q824PxjYyWIB
          H7WEi1A==
    </DigitalSignature>
</ProvenanceRecord>
```

Listing 1: Provenance Record

Step 1 and 2: A location-update provenance record is created when the client application opens a FReadyPass.

Step 3 and 4: A modification provenance record is created when the client application saves a payload after a modification has been made.

Step 5: After a client has finished with a FReadyPass the client uploads the FReadyPass to the server.

Step 6: After a FReadyPass is uploaded to the server the server creates a location-update provenance record.

Step 7: Finally, after a FReadyPass is uploaded to the server and a location-update provenance record has been captured the server creates a verification provenance record.

The purpose of a location-update record is to show where a record is. The modification record indicates that a modification has been made to the payload. The verification record created by the server is done after the server verifies the digital signatures of the records produced by the client using the client's corresponding RSA public key.

3.3.2 Verify the integrity of provenance data

The process of verifying provenance data is quite simple. The digital signatures are used to confirm that the provenance records were not modified. There exist two concerns regarding the integrity of the provenance data.

C1. A provenance record may have been altered.

C2. A provenance record may have been deleted.

An attacker may alter or delete provenance records in an attempt to conceal access or modification to a FReadyPass payload.

To address concern C1, a provenance record is digitally signed to verify its integrity and either prove that the provenance record has not been altered, or detect if it was altered. The provenance record is signed by the entity that produces it. Thus, the client will sign provenance records it creates, and the server will sign provenance records that it creates. Formally stated:

DigitalSignature(n) $\rightarrow$ *Record(n)*

Meaning the signature of provenance record *n* denoted as: *DigitalSignature(n)* verifies provenance record *n* denoted as *Record(n)*.

To address concern C2, the system needs to provide cryptographic proof of the integrity of all provenance data. Provenance records are chained together to detect if a provenance record has been deleted. Chaining the provenance records together ensures that a forged provenance record cannot be inserted in the chain, a valid provenance record cannot be removed, and no provenance records can be modified without being detected. However, there is one risk that has not been addressed. The most recent provenance record, provenance record *n* can be deleted and will go undetected. If one deletes provenance record *n*, it becomes possible to delete provenance record *n-1* and again it will go undetected. To ensure that the most recent provenance record, provenance record *n* cannot be deleted without being detected, the author creates an index of the provenance chain. It is not necessary to create an index for the entire provenance records considering the provenance records is chained together. The index has merely to indicate how many provenance records there are, and what the value of *n* is.

4. Conclusion

This paper aims to investigate how a digital object can be tracked through the cloud and the history of the object stored in a forensic ready manner. The authors proposed the design of a model to accomplish this goal while providing an access control mechanism that relies on location information.

The research question asked in this paper is stated as follows: "How can a digital object be tracked through the cloud and how can digital space be anchored to physical space to control the access of information across jurisdictional boundaries?" This question is answered by relying on a reverse IP address lookup using the IANA registrar databases and verifying the IP address by making use of a TCP/IP 3-way handshake, thus ensuring that a client connecting to a CSP is, in fact, connecting from where they appear to be.

Applying the proposed model, the history of a digital object is captured and kept with that object in the form of a forensic ready passport, once the object comes under the control of the CSP. When the FReadyPass is requested for download an access control mechanism determines if the request is valid and should be allowed. If access to the FReadyPass is granted, the user may modify the payload of the FReadyPass. This model provides the ability to track data under the control of the CSP and to provide a detailed history of where the object has been and who accessed it.

Although this paper focus on the technical issues and implementation of tracking data through the cloud, there are also complex legislative and jurisdictional issues that arise when dealing with cross-jurisdictional investigations. It is essential to obtain collaboration between cross-jurisdictional organisations as well as to address legislative and jurisdictional issues in order to achieve maximum success in cross-jurisdictional investigations.

Some future work to be done includes a technique to successfully detect active remote control connections on a client. When the CSP intends to limit access to information based on the physical location of a user, a device that is being controlled remotely may provide access to information to users outside of the allowed locations, even if the user is only able to read that information.

5. Acknowledgements

The authors would like to thank the University of Pretoria, the South African National Research Foundation (NRF) and GEW Technologies that provided financial assistance for this research to be undertaken.

6. Bibliography

[1] D. Reilly, C. Wren and T. Berry, Cloud computing: Forensic challenges for law enforcement, IEEE, 2010, pp. 1-7.

[2] G. Giova, "Improving chain of custody in forensic investigation of electronic digital systems," *International Journal of Computer Science and Network Security,* vol. 11, no. 1, pp. 1-9, 2011.

[3] P. Mell and T. Grance, The NIST Definition of Cloud Computing, Information Technology Laboratory - Computer Security Division, 2011.

[4] S. Pearson and A. Benameur, Privacy, security and trust issues arising from cloud computing, IEEE, 2010, pp. 693-702.

[5] G. Palmer, "A Road Map for Digital Forensic Research," First Digital Forensic Research Workshop (DFRWS), 2001.

[6] J. J. Barbara, "Cloud Computing: Another Digital Forensic Challenge," *Digital Forensic Investigator News,* October 2009.

[7] R. Rowlingson, "A Ten Step Process for Forensic Readiness," *International Journal of Digital Evidence,* vol. 2, no. 3, 2004.

[8] D. Birk and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," *Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE),* pp. 1-10, 2011.

[9] K.-K. Muniswamy-Reddy and M. Seltzer, "Provenance as first class cloud data," *ACM SIGOPS Operating Systems Review,* vol. 43, no. 4, pp. 11-16, 2010.

[10] R. Lu, X. Lin, X. Liang and X. S. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, ACM, 2010, pp. 282-292.

[11] P. M. Trenwith and H. S. Venter, "A digital forensic model for providing better data provenance in the cloud," *Information Security for South Africa,* pp. 1-6, 2014.

[12] K.-K. Muniswamy-Reddy, U. Braun, D. A. Holland, P. Macko, D. Maclean, D. Margo, M. Seltzer and R. Smogor, "Layering in Provenance Systems," in *Proceedings of the 2009 USENIX Annual Technical Conference*, 2009.

[13] Y. Shi, K. Zhang and Q. Li, "A new data integrity verification mechanism for SaaS," in *Web Information Systems and Mining*, 2010, Springer, pp. 236-243.

[14] A. Juels and B. S. Kaliski Jr, "PORs: Proofs of retrievability for large files," *Proceedings of the 14th ACM conference on Computer and communications security,* pp. 584-597, 2007.

[15] P. Zimmermann, "A Proposed Standard Format for RSA Cryptosystems," vol. 19, no. 9, pp. 21-34, September 1986.

[16] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, no. 2, pp. 120-126, 1978.

[17] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM - Special 25th Anniversary Issue,* vol. 26, no. 1, pp. 96-99, 1983.

[18] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory,* vol. 31, no. 4, pp. 469-472, July 1985.

[19] K. R. Fall and W. R. Stevens, TCP/IP illustrated, volume 1: The protocols, Addison-Wesley, 2011.

[20] IANA, "IANA," 2015. [Online]. Available: www.iana.org.

[21] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *International workshop on selected areas in cryptography*, Springer, 2003, pp. 175-193.