Private Virtual Infrastructure for Security of Electronic Health Records in a Cloud Computing Environment

Emmanuel Achampong
University of Cape Coast
25 PUBLICATIONS **69** CITATIONS

ISSN: 2458 – 7419

International Journal of Business Innovation and Technology (IJBIT), Volume 3, No. 1, March 2016, pp.1-7

Private Virtual Infrastructure for Security of Electronic Health Records in a Cloud Computing Environment

Emmanuel Kusi Achampong[1] and Clement Dzidonu[2]
[1]*University of Cape Coast, Cape Coast*
[2]*Accra Institute of Technology, Accra, Ghana*

Abstract

This study focuses on the use of Private Virtual Infrastructure (PVI) to enhance the security of Electronic Health Records (EHR) in a Cloud Computing Environment (CCE). Electronic health records stored in a cloud computing environment place the sensitive data in the control of third parties. Healthcare institutions want to have control over the computing infrastructure that stores their sensitive data. But current cloud computing systems does not guarantee such access to the datacentre infrastructure. Customers are sometimes not aware of where the datacentre keeping their data is even located. This study discusses a security model of cloud computing known as PVI whose core responsibility is to share the security of cloud computing between the Cloud Service Provider (CSP) and the customer. The PVI also seeks to remove the risk exposure between the CSP and the customer. The PVI datacentre is under the control of customer whereas the cloud datacentre infrastructure comes under the control of CSP. A software device called Locater Bot (LoBot) pre-measures the security properties of the cloud infrastructure. The LoBot performs security provisions and offers situational awareness. LoBot also performs continuous monitoring of the cloud computing security. PVI and LoBot offer the tools that organisations need to maintain control over their information in the cloud and retain the benefits of cloud computing. PVI and LoBot have the capacity to satisfy the security requirements of EHR within the CCE.

Keywords: Private Virtual Infrastructure, Electronic Health Records, Cloud Computing

1. Introduction

Electronic health record (EHR) is a patient record which is shared across various health workers and environments, by computing networks that connect the different departments within healthcare organization. (Zhang, Liu, & Xue, 2010). Electronic health records (EHR) in a cloud computing environment has the potential to make healthcare cheaper, safer, and more convenient by ensuring complete health history, avoiding repeated tests, and allowing authorised users to have timely access to EHRs anytime and anywhere (Morton, 2008).

Cloud computing is an online processing and storage system where resources, information and software are shared and provided to computing devices over the Internet (Nayyar, 2011). The advantages of cloud computing makes it attractive to healthcare providers who operate with sensitive data (health records). Cloud computing has the potential to deliver dynamic computing resources. Cloud computing creates a new approach to doing business but also comes with new challenges. These challenges mainly border on privacy and security of the information that is stored on the cloud computing servers (Armbrust et al., 2009).

A major risk in the use of cloud computing services is where an information owner loses control of their information after it is uploaded to cloud servers for storage and processing. The lack of physical control of data centre by data owners compromises the security of sensitive data.

This research article presents a better way in managing the security of EHR in a cloud computing environment by using Private Virtual Infrastructure (PVI). PVI would allow healthcare institutions to make use of cloud resources with an assurance to meet all the security issues. PVI minimises the security risks of cloud computing by a shared responsibility between the cloud service provider (CSP) and the health institution (customer).

1.1 *Cloud computing security*

Cloud Computing security demands total awareness of the risks to information, network and infrastructure. Abstraction is the major security weakness and at the same time an advantage to the provision of cloud computing services. Abstraction eliminates knowledge of the core structure of storage, processors and networking and it makes the cloud computing environment to be pervasive (Reddy & Reddy, 2011). Nevertheless, without knowledge of the core structure, customers (healthcare organisations) understanding to the process to secure information and applications become very complex. Generally, networks and datacentres depend on routers, servers, intrusion detection devices and firewalls to know sources and types of attacks. Knowledge of the source and type of attack would help in safeguarding the information stored by either separating pieces of the structure under attack or totally shutting down access to other resources (Nurmi et al., 2008).

Traditional information security methodologies cannot be applied over the cloud computing infrastructure because information owners are unable to manipulate the security settings. When information owners are allowed to directly manipulate the security settings, they may tamper with the security settings of other customers. But to ensure trust between the CSP and the customer, the information owner should have some knowledge of the security posture of where their information is being stored and processed.

Therefore, cloud computing requires a new security model for ensuring trust between CSPs and clients. Shared security arrangement between CSPs and clients is the way to go now. Cloud service providers (CSPs) must clearly show clients the security position of the cloud infrastructure so that customers can be assured that they have full control over the confidentiality and privacy of their data/information. Customers must be assured that they can have access to their information all the time and can also destroy, remove or manipulate their data. This process of giving customers control over the security of their applications and information provides an interdependent security posture that can be useful provided both parties fulfils their side of the agreement.

1.2 Private Virtual Infrastructure (PVI) cloud security model

Private Virtual Infrastructure (PVI) satisfies the objectives of a shared security position where all the necessary resources for a virtual datacentre are isolated from the physical cloud. The PVI provides secure provisioning of cloud computing resources that separate the customer datacentre to operate on its own virtual domain. The virtual datacentre is fully controlled by the customer while the cloud infrastructure is under the complete control of the CSP. The CSP and the customer agree to share security information among themselves. This would help achieve situational awareness of the security positions at all times.

Before any provisioning is done for the PVI, the cloud server security has to be verified in order to report security properties of the cloud resources. These securities properties should be cryptographically bound and signed so that only authorised users would be able to verify the properties. Trusted computing methods are selected to verify the security settings and report the configuration of the cloud infrastructure in the PVI. Communications within the PVI should be done through a virtual private network (VPN) and through encryption with Internet protocol security (IPSec) or secure sockets layer (SSL) tunnels which offers confidentiality on the networks and averts eavesdropping and spoofing in PVI.

1.3 Trusted computing

Trusted Computing offers security to computer systems through the enforcement of security policies through hardware and software controls. With trusted computing technology, health institutions can easily verify the posture of security within the cloud computing environment (Berger et al., 2009).

The Trusted Platform Module (TPM) is the main component in trusted computing. The TPM is a cryptographic unit that offers root of trust for constructing a trusted computing base (Berger et al., 2009). Cryptographic keys are stored in the TPM’s Platform Configuration Registers (PCRs) and they are used to measure and confirm the state of operation of the platform. The attestation process gives customers the opportunity to demand the PCRs of the TPM and also verify that the platform meet their configuration and policy requirements (Berger et al., 2009).

However, TPM is only useful in non-virtualised environments. Therefore TPM needs to be virtualised if it can be used in a virtual environment. Specifications for virtual TPM (VTPM) have already been developed. The VTPM is implemented by offering software instances of TPMs for a virtual machine (VM) on a trusted platform. The VTPMs are connected to physical TPMs and are used to protect virtual machines (VMs) in the cloud. Locator Bot (LoBot) secures each VM cryptographically by tightly linking a VTPM in its own stub-domain. LoBot as an agent lets each VM to be verified by its owner and offers secure provisioning and relocation of the VM in the cloud computing environment (Schwarzkopf, Schmidt, Strack, Martin, & Freisleben, 2012).

2. Methodology

Information system research methodology is classified into two major groups. These are behavioural research and design science research (DSR). Design Science Research becomes useful when a study involves the design of artefacts in the form of methods, models, constructs and instantiations. This study used the DSR method. The design research process from Peffers et al (2008) was used. The research process followed the following format: problem identification, requirement analysis, design and evaluation.

The outcome of the research process was the design of the artefact in figure 1.

3. PVI cloud security architecture

The PVI architecture is made up of two layers which shares the security responsibility between the CSP and the customer. The PVI layer offers a virtual datacentre which is managed by the customer. The CSP accepts the responsibility of providing both physical and logical security of the platform needed for PVI Layer.

The customer is responsible for equipping their virtual infrastructure with correctly configured intrusion detection systems, firewalls, monitoring and logging systems to ensure that data/information is kept confidential. The PVI allows the customers to build virtual infrastructure that satisfy these requirements.

3.1 *Trusted cloud computing services platform*

The main focus of PVI security model is for the customer to confirm the security settings of the datacentre infrastructure. The CSP is responsible for the provision of security services which would secure and monitor the datacentre infrastructure. These security services are reported through an identity certificate given to the virtual environment that confirms these services. The PVI depends on components of trusted computing to attain the trusted cloud platform.

Many research projects are being undertaken to make it easy for PVI to be applied. An example is the IBM's Trusted Virtual Datacentre (TVD) which offers several features in cloud computing environment for appropriate security of datacentre servers and VM isolation through a secure Hypervisor called sHype (Nurmi et al., 2008).

3.2 *Private Virtual Infrastructure Factory (PVIF)*

The PVI factory (PVIF) stores all the various components of PVI. It is considered as the source authority for provisioning, management and certificate generation and VTPM key generation within PVI (Nayyar, 2011). The PVIF is responsible for preserving master images for application servers. It is also responsible for managing data transfers to PVI through VPN configuration and management.
The PVIF must be under complete control of the customer on the customer's website. It must not be virtualised and must be isolated from other systems on the cloud platform. The PVIF implementation for the customer can either be a hardware or software. For the purposes of this research, it is going to be a software-only implementation.

The PVIF operates as the main controller and a decision point for policy for the PVI (Krautheim, 2010). It is responsible for safeguarding the integrity of the PVI and managing incidents of any security breach. The PVIF shutdown the PVI if problems are detected. It recalls and inspects all images for any tampering, and also generates alarms and reports.

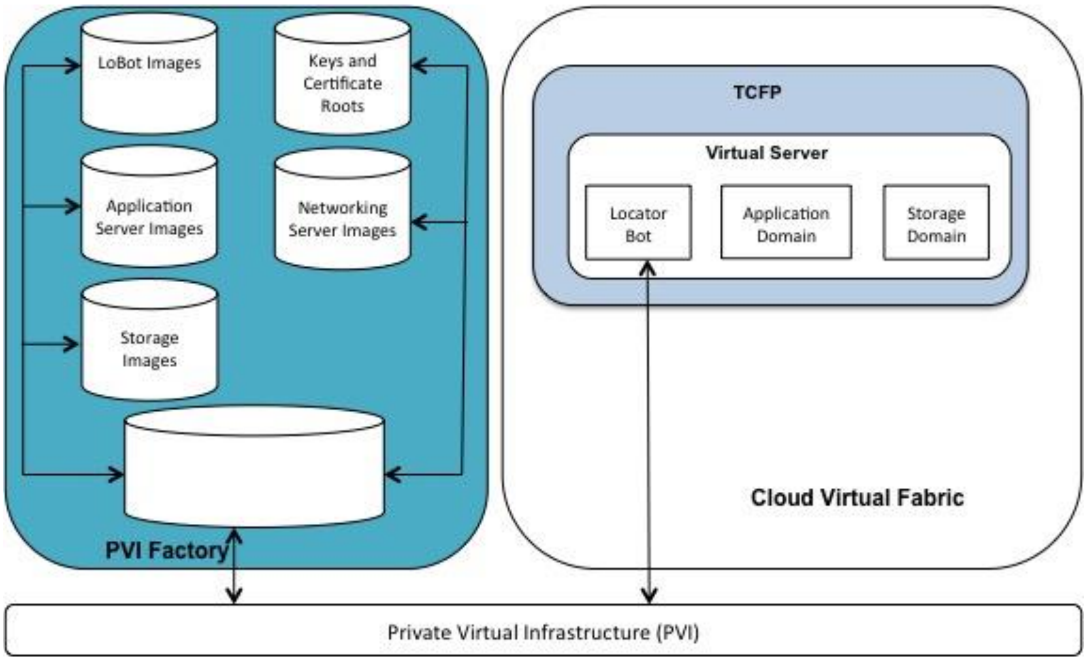

Figure 1: Enhanced Private Virtual Infrastructure Architecture

Figure 1 displays the enhanced PVI architecture where PVIF behave like the management structure that is outside of the CVF. The PVIF has a responsibility to ensure the PVI's integrity and also manage incidents whenever security is compromised. The PVIF has the power to close the PVI when problems are seen. The PVIF can recall and check all images for any tampering, and create alarms and reports (Krautheim, 2010).

The PVIF serves as the most sensitive aspect of the PVI. The PVIF as root of trust for PVI and the management controller provides virtual machine provisioning, endorsement key (EK) certificate authority (Virtual Trusted Platform Module (VTPM) Entity), VTPM key generation, and VTPM NVRAM storage. All components of the PVI are provisioned at the PVIF and it is the main root authority for provisioning, certificate generation and VTPM key generation. Virtual TPMs do not have valid EKs, and therefore an EK must be produced for each VTPM. This is used within the PVI in order to trust the operations of the VTPM. The PVI factory also keeps master images for application servers, LoBots, and is in charge of data transfers within the PVI using the VPN management and configuration (Krautheim, 2010).

The PVIF operate on a dedicated trusted server and is a software-based application. As the root authority, when the PVIF is compromised, all PVI components may also be at risk of compromise and may threaten components that are provisioned in future and therefore cannot be trusted. Since the PVI is under the control of the health authority, the PVIF automatically falls under the complete control of the health authority and must be secured from other systems and applications within the cloud computing setting. The PVIF must be physically isolated in an access-controlled area (Krautheim, 2010).

3.2.1 Virtual Server Domain

Specific virtual server domain (VSD) is a mixture of an application domain (AD), which is unprivileged, and a closely coupled LoBot. The LoBot is executed as a stub driver domain, which is unprivileged to offer protection and isolation for the VTPM. The virtual server domains (VSD) are provisioned, controlled and managed by the Health Authority, to guarantee that the health authority ensure control of the EHR in the application server (Krautheim, 2010).

3.2.2 Application Domain (AD)

The application domain (AD) is a VM that is used by clients to run application in a cloud computing environment. The application domain is the location where all-important processing is done and confidential data are processed and stored. Hence, the domain has to be safeguarded at the maximum level possible. PVI and LoBot have the responsibility to protect the application domain. The primary goal of PVI is to protect the application domain. Any compromise of the application domain would grant a malicious user access to the running application and destroy the EHR that is being processed within the application server (Krautheim, 2010).

3.2.3 Storage Domain

The storage domain is a virtual device where software and data (EHR) are stored within the cloud computing environment. It is therefore important that the domain is protected from malicious users. The PVI has the responsibility of ensuring that data kept with the storage domain are secured through proper encryption. The storage domain is a sensitive storage device that is monitored and protected by the PVI and LoBot.

3.2.4 LoBot Domain

LoBot is a virtual device used to guard application and storage servers in PVI. A LoBot is an independent virtual machine image that possesses no external storage requirements and as a result letting it move and reproduce within a cloud computing environment efficiently. The primary responsibility of LoBot domain is to act as a protection for the application and storage domains (ASD). LoBot defends the application and storage domains with these primary functions:

- imitate a physical TPM and offer a root of trust for the application and storage
- domains serve as an enquiry to measure target platforms
- offer safe provisioning and live and quick migration services. The investigative function certifies that the destination platform offers adequate security properties to safeguard information of both the application and storage domains.
- offer continuous monitoring of the application server, application domain, storage domain and virtual servers.

The LoBot architecture is a driver-stub domain dedicated to a particular application domain and storage domain generating a virtual server domain. The LoBot offers TPM services by employing a VTPM to the application domain. The VTPM is central to the LoBot architecture offering equal level of trust for the virtual platform as the TPM performs on the physical infrastructure. The LoBot’s VTPM is fixed to the physical TPM of the TCFP closely linking the LoBot and application domain to the main host. The PVI owns the VTPM whilst CVF owns the TPM (Krautheim, 2010). Placing the VTPM in the LoBot has several advantages over operating the VTPM in the host domain including isolation of the VTPM process and reducing the burden of VTPM migration. All the necessary information that must be saved by LoBot and VTPM, such as non-volatile storage and keys are encrypted in a blob. The information is stored in the PVIF. The PVIF controls storage of data for each LoBot rejecting the need for local storage (Krautheim, 2010).

When LoBot launches, the VTPM fixes itself to the target TPM. The probe application studies the configuration of the platform from the TPM’s Platform Configuration Registers (PCRs) target and acquires information about the platform. Information on identity is offered in cryptographic certificates. The information is combined with VTPM’s PCR, which is sealed cryptographically in a blob that is transmitted to the PVIF. The blob is decrypted by PVIF and the information received is examined to help in making a trust decision. If the target environment is determined to be trustworthy by the PVIF, the application domain image is configured and securely transferred to the target environment in a blob, which is encrypted in such a way that the target platform only may implement source environment(Krautheim, Phatak, & Sherman, 2009).

The LoBot probe application obtains and opens the application domain image at the target environment. During the decryption phase, it will be detected if the image was tampered with during transfer. To ensure everything is secured, the source environment is measured by the probe again to certify its integrity and to make sure that the launch was successful in the target environment.

After successful provisioning, the LoBot continues to monitor the VTPM, application and storage domains for changes and any malicious activity. LoBot therefore runs at the background to report any policy breaches to ensure that the EHR in a cloud computing environment is secured.

3.3 Secured Storage

Secured storage is essential for customers to be satisfied that their EHR is protected from motivated workers and malicious users. Every application domain in PVI needs a virtual storage device to act as the system disk and to store the software and data. The EHR application within the cloud computing environment both process and stores health data. The EHR have to be kept in a secured storage domain and in a location that is accessible to the source and destination nodes throughout all migrations. Physical management of the storage devices lies within the confines of the CSP and customers through the PVI must be assured that their EHR is secured. LoBot is employed to continuously monitor the data storage VM to ensure a secured storage VM so as to avoid malicious users exploiting the system.

3.4 Networking

Private Virtual Infrastructure (PVI) runs on a fast local area network within CVF, which is secluded from the Internet by network address translation, firewalls, and other security devices. This is handled by the CSP. Encrypted VPNs and virtual LAN partitioning are employed to separate PVI from the other CVF network traffic in order to guarantee private networking within PVI (Krautheim, 2010). Private networking for PVI would guarantee secured transmission of EHR within the cloud environment.

For the EHR in the cloud computing environment, it is important that the network is secured for guarded transmission of sensitive data/information from one location to the other. Apart from avoiding man-in-the-middle attack through encryption methods, the addition of firewalls and network address translation would protect data transmission within the cloud infrastructure.

3.5 Secure Provisioning and Monitoring

The removal of the abstraction of the datacentre infrastructure is a trade off in order to take to enhance the security of the virtual datacentre (Nayyar, 2011). This means that CSPs need to allow customers access to evaluate the security posture of the datacentre infrastructures. This would create a synergistic relationship between CSPs and customers and therefore enhancing the security framework and capacity of both the customer and the CSP.

Pre-measurement of the datacentre infrastructure permits PVI to share the responsibilities of security management between the CSP and customer (Krautheim, 2010). LoBot performs the pre-measurement, which tests the datacentre infrastructure’s security posture before provisioning is done. This allows the customer to determine the security of the datacentre infrastructure before the PVI is deployed.

LoBot is a secure transfer protocol based on VTPMs and VM architecture (Krautheim, 2010). When LoBot finish probing target platforms for security properties, they can then tightly provision VMs on the platforms. A LoBot is a self-reliant VM with a VTPM and probe application. Whenever there is a start-up, the VTPM fixes itself to the target’s TPM. The probe application then studies the platform configuration which is on the target TPM’s PCR and gets identifying information about the platform (Nayyar, 2011). Identity information is delivered in the form of credentials. These credentials are combined with the VTPM’s PCR which is sealed cryptographically in a blob that is moved to the PVIF (Krautheim, 2010).

The blob is decrypted by the PVIF. The PVIF also studies the information received to establish whether the environment is secure. Once the target environment is confirmed to be safe, the PVIF then configures the VM and also securely transfers it to the target environment. This transfer of the VM is done using the LoBot protocol, encrypted in a blob to ensure that the target platform only execute the source environment (Krautheim, 2010).

The LoBot probe application obtains and opens the source environment at the target environment. The decryption phase would detect any tampering of the source environment during the transfer. The probe application measures the source environment again to validate its integrity and to make sure that the launch within the target environment was effective and successful (Nayyar, 2011).

3.6 Secure shutdown and data disposition

Current virtual machine monitors do not have secure shutdown and data disposition properties. Vulnerability may therefore arise when a

VM with health data is closed down and a fresh VM is deployed the place of the previous VM.

The new VM could just read its whole memory space searching for any data left behind by the former VM. The privacy and security implications of such a risk can be very serious as health information can be stolen and used for health insurance fraud and blackmail. LoBot has the capacity to wipe a VM’s memory space securely after shutdown and thus removing any health data that could have been left behind by the VM.

3.7 Monitoring and auditing

LoBot deliver continuous monitoring of the cloud computing environment. It monitors the cloud computing environment and communicate with PVIF to get the situation of cloud computing environment (Nayyar, 2011).

Auditing enhances the ability to manage security incidents. Auditing responsibilities must be shared between CSPs and customers for an improved productive cloud computing performance. Monitoring and logging must be performed within PVI whilst the CSP does the security monitoring and services delivered by the datacentre infrastructure. This enhances the capability to investigate security incidents at both the PVI and datacentre infrastructure. Reconciliation of the PVI and datacentre infrastructure logs can improve the capability and pace of tracking down incidents (Nayyar, 2011).

LoBot has the capacity to perform monitoring of the PVI continuously and record the daily activities on the platform. This additional responsibility of the LoBot would ensure the early detection of any malicious users trying to misuse and abuse the EHR within the cloud computing environment.

4. Conclusion

This research paper recommends a new revolution for ensuring a secured EHR in a cloud computing environment. This enhanced security is based on an improved relationship between the CSP and health authority (customer) and it offers a better security posture when setting security controls needed to protect the EHR in the cloud environment, datacentre infrastructure and the virtual datacentre.

The CSPs has the capability to offer a transparent view of their datacentre infrastructure to their customers through the use of PVIs. This builds the customer’s trust in the CSP. Cooperation between the CSPs and clients will result in an improved security.

The CSP is responsible for preserving a secure datacentre infrastructure. The PVI offers customers the flexibility to manage and control their data while enjoying the benefits of cloud computing. It is recommended that data destruction and secure shutdown capabilities be added into future virtual machine monitors.

Reference

[1] Armbrust, M., Armbrust, M., Fox, a, Fox, a, Griffith, R., Griffith, R., … Rh. (2009). Above the clouds: A Berkeley view of cloud computing. *University of California, Berkeley, Tech. Rep. UCB* , 07–013. doi:10.1145/1721654.1721672

[2] Berger, S., Caceres, R., Goldman, K., Pendarakis, D., Perez, R., Rao, J. R., … Valdez, E. (2009). Security for the cloud infrastructure: Trusted virtual data center implementation. *IBM Journal of Research and Development*, *53*(4), 6:1–6:12. doi:10.1147/JRD.2009.5429060

[3] Krautheim, F. J. (2010). *Building trust into utility cloud computing*. *ProQuest Dissertations and Theses*. Retrieved from https://login.ctu.idm/oclc.org/?url=http://search.proquest.com/docview/757888543?accountid=26967 LA - English

[4] Krautheim, F., Phatak, D. S., & Sherman, A. T. (2009). *Private Virtual Infrastructure : A Model for Trustworthy Utility Cloud Computing UMBC Computer Science Technical Report Number TR-CS-10-04. Program*.

[5] Morton, M. E. (2008). Use and acceptance of an electronic health record: factors affecting physician attitudes, (August), 153.

[6] Nayyar, P. A. (2011). Private Virtual Infrastructure (PVI) Model for Cloud Computing. *International Journal of Software Engineering Research and Practices*, *1*(1), 10–14.

[7] Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2008). *Eucalyptus : A Technical Report on an Elastic Utility Computing Archietcture Linking Your Programs to Useful Systems UCSB Computer Science Technical Report Number 2008-10*.

[8] Reddy, V. K., & Reddy, L. S. S. (2011). Security Architecture of Cloud Computing. *International Journal of Engineering Science and Technology*, *3*(9), 7149–7155. Retrieved from http://lit.summon.serialssolutions.com/link/0/eLvHCXMwTV27CsJAEDwkhXVAr_UHEnLPXOpgTCESxIjaXW73SkGN_-8aFayWqaYZZliWYRlboQlWOwwetNFBlhaMAAhIcaFkOZWEu77qjmqzV-2fmzcpm-F1wfpmfajb7PsMIAOKdJFB6ZGcM4ISOhowRbTDoL1F6ZwnNln5AeL7kFhE0hUCKAfehUAoChnEkiW0UCNnyXh_0iCv5

[9] Schwarzkopf, R., Schmidt, M., Strack, C., Martin, S., & Freisleben, B. (2012). Increasing

virtual machine security in cloud environments. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*, 12. doi:10.1186/2192-113X-1-12

[10] Zhang, R., Liu, L., & Xue, R. (2010). Role-Based and Time-Bound Access and Management of EHR Data. *Security and Communication Networks*, 1–21. doi:10.1002/sec