Journal of Computer Science

Original Research Paper

Integrated Security Framework for Private Cloud Computing On-Premise

Pedro Ramos Brandao

Advanced Computer Research Unit, Instituto Superior de Tecnologias Avancadas, Lisbon, Portugal

Article history
Received: 01-12-2020
Revised: 30-12-2020
Accepted: 30-12-2020

Email: pedro.brandao@istec.pt

Abstract: Development of a globally integrated framework, intended for implementation in a private on-premise cloud computing framework, structurally based on virtualization technologies, cloud computing, encryption, high availability and redundancy systems, data protection systems, governance, active steering, network monitoring systems, risk analysis and physical infrastructure protection.

Keywords: On-Premise Private Cloud Computing, Cybersecurity, Cybersecurity Framework, Cloud Computing Security, Authentication, Authorization, Encryption, Information Security, Data Protection System

Introduction

This study primary purpose is to design an integrated framework that will implement a high level of security in a private on-premise cloud computing (Hereafter referred to as CC). This on-premise private cloud will be one of a kind that stores critical and sensitive information, which requires concern regarding its access. In detail, the goal is to create a fully integrated solution that cumulatively implements several layers of protection, both physical and logical but thoroughly embedded in each other. To provide in a big level of identification control, authentication and authorization regarding users, the same type of controlling at level of physical access to facilities in which this private on-premise cloud is implemented.

It must be understood that the type of framework developed has very particular applicability in its possible implementation. This type of solution is primarily intended for organizations with an imperative need to have a private cloud in their facilities and protect the full information on their data servers, i.e., military, security and intelligence research related to the pharmaceutical industry. Physical access must be highly controlled. There must be a double authentication system (not to be confused with two-step authentication), a double authorization system and total data and information isolation from any other network, including the Internet.

Literature Review

The best-known framework for cloud computing systems was presented by the National Institute of Standards and Technology (NIST), it is an essential reference, however and as you would expect of a generalist model (NIST, 2020).

Its goal is to help organizations manage their cybersecurity risks in the country's critical infrastructure, such as power grids and bridges, etc. It contains a common vocabulary for the actions that need to be taken to identify, protect, detecting, responding to and recovering at the security threats.

They Include

> "*Identify: Developing an organizational understanding to manage cybersecurity risks to systems, people, assets, data and resources*
> *Protect: Develop and implement appropriate safeguards to guarantee the provision of critical services*
> *Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event*
> *Respond: Develop and implement appropriate activities to perform actions related to a detected cybersecurity incident*
> *Recover: Develop and implement appropriate activities to maintain resilience plans and restore any resources or services that have been impaired due to a cybersecurity incident*" (NIST, 2020)

This structure has been adopted on a large scale by many organizations in the US and other countries. This is applicable to both the private cloud and the public cloud.

Arijit Ukil, proposed a Framework for security in cloud computing in which it analyzes changes and security and questions about of cloud computing about differences innovates standard options. It proposes an architectural analysis to incorporate a distinguish cybersecurity's, approaches and standards for CC, mainly in Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) systems. This architecture-system is the usual, doesn't depend on the typology of deployment in the cloud, is independent of the application and is not associated with the underlying backbone.

It proposes a structure to satisfy the security of cloud computing, guaranteeing the main primitives: Confidentiality, integrity and authenticity (and total control). It integrates the individuals to made available integrated cybersecurity that can be like cybersecurity as service.

One solution is to do the analysis and processing of information in the company hiding the information of the customers. But encryption in these cases is difficult. To maintain confidentiality and extract services from the data by third-party applications, processing in the field of encryption is necessary. This is referred to as homomorphic encryption. Homomorphic encryption-technique provides accuracy calculate unusual functions on cipher information.

The biggest technique in the model is provides a single Internet identification, robust to different CC applications.

The CC services model are susceptible to not invasive the lateral channels attacks, such as software (hereafter referred to as SW) attacks (malware and viruses) and other like key assumption by the distributed kind. Best solution for solve the problems, according the author, is to provide a safe execution environment to guarantee the protected running SW and other active entities, like all kind of memory, that made available by securing hardware (hereinafter referred to as HW) platform. To make the CC infrastructure enable of handling with cybersecurity issues, strange components to combat not normal attacks is not easy to manage. Other important and specified configuration of CC cybersecurity is when cybersecurity is providing as-a-service, such as applications, platform or infrastructure-as-a-service. Cybersecurity-as-a-service has enormous potential for two issues, second or author, first, due to the continuous and rapid change in the IT security load and corporate security third companies and personalization; second, to scalability situations, cybersecurity problems need deal with the complex increase in process and adapt changing the paradigm of CC. The focus of this author's work was to describe the problems of information integrity and specially confidentiality, for authentication and the cybersecurity special issues are from about perspective of the users. In this study of the author, the perspectives of professionals are presented, addressing customer attention and raise aware-ness among stakeholders in cloud computing processes about the measures to be taken to guarantee the cybersecurity of users services software running in at CC (Ukil *et al*., 2013).

Shadi Aljawarneh presents us with a related framework that addresses essential questions about CC. This study, author presents perspectives of CC professionals, about to meet customer security implications and implement sensitizing information that must be taken to obtain the cybersecurity of customers services software, executed at CC.

This framework has 3 objectives:

a) A search for possible solutions to encounter software (hereinafter referred to as SW) cybersecurity problems, Analyze the risks of a CC system and is cybersecurity's boundaries
b) Several points of view from CC SW security professionals to try understanding the main CC SW cybersecurity problems at companies around the globe
c) An identification of the cybersecurity levels of cloud software, by research and other approaches

This study is an abstraction Framework with 3 components helping to identify the cybersecurity types of CC software that should be considered by scholars and professionals (Aljawarneh and Yassein, 2016).

Sang-Ho Na, publishes a paper in which he presents a Framework in which he analyzed threats and security requirements from previous research as well as proposed service models and cybersecurity framework, that include technology makes available high mobility possibilities of resources, presenting a conceptual and consensual solution, in his opinion.

Its structure aims to provide security in cloud computing. According to the author, this system works in individual CC, including a multivalent individual service-models, functional objects in several CC environments.

It presents as fundamental requirements for the Framework:

a) Users authorization and accessing to highest domain functions includes normal users, including request and customization of functions with CC authorizations for APIs, OS to access CC functions and administration services of monitorization
b) Implemented CC orchestration: This deals with a conjugation structure of cloud services, service providers can provide CC services, networking and storage services in an end user's consumers
c) Administration of virtualization resources: The domain of administration of virtualized resources describes the mobility of resources, automatically and dynamically made available

The framework model presented must include the following objects to be made available for the secure access of users: A certified browser client, a final portal for users, a configuration service, a gateway and broker service, security controls and a permanent security service monitoring.

Security structure proposed by the author, provides cyber secure data transactions and the possibilities to put APIs ON and exposed to user's access to the CC services, it considers CC administration environments, a single-one authentications by token and that turn possible a perfect user experience. In addition, he can provide systems for CC teamwork (Na *et al*., 2010).

Aman Kumar Sharma presents us with a study that lists concerns about data security problems. This study first explains several data security problems and possible solutions. The first is an authentication model that provides more secure access to data in the cloud, the second is encryption that encrypts data to make it more secure; the third is the structural method that breaks the data structurally to avoid its misuse; the fourth is a data security method that provides an alternative method that guarantees the security of the data to the user.

It prioritizes the following security issues: Data loss, data privacy, data theft, data integrity and data transfer.

In its Framework, in a generic way, it presents as solutions to the problems that the following states.

Data loss: To avoid data loss, there is a backup mechanism with all cloud service providers. Mirroring storage devices used with more sophisticated transmission media can reduce data loss. However, if the data is still lost, it is proposed that the data be guaranteed. In this model, all the care with the data is performed by the private organization, where the data must be stored, how the data must be transferred, availability and backup.

Data privacy: They propose to have a two-tier data security architecture. Identity and access management, which is a critical function for the entire organization and a fundamental expectation of customers, using the principle of least privilege in relation to access to their data. The theory that the least privileges should always be given by default establishes that the minimum access necessary to grant an operation must be granted and that access must be granted only for the minimum necessary period.

Data theft: One should always try to avoid data theft. This can be accomplished again by using the two-tier architecture. In addition, data encryption can be a solution to add to the integrated solution.

Data integrity: To solve problems related to data integrity, the data record can be structurally divided into parts. Different parts of the data can be saved on multiple systems.

In this Framework the author presents several solutions to specific problems and it is the combination of these solutions in an integrated way that creates the Framework (Sharma, 2019).

Ayesha Malik published a study in which he presented a proposal for a generic framework for cloud computing environments. The goal of work sits on state of and describe a system for CC to protect the user information and sensitive data.

The objectives of this investigation were to study the main threats that arise in the cloud environment, technologies used and problems that still need to be solved in terms of security.

The author identifies as main types of possible attacks in terms of security the following: Adulteration, interception/disclosure of information, repudiate users, increase privileges, Man in the Middle cyberattack, repetition at-tack, impersonation, threat of analysis differential, vi-ruses and worms. However, this type of attacks that the author lists is not specific to cloud computing environments.

It presents as integrated solutions, which embody or structure, as follows: Mirage image management system; customer-based privacy management; transparent cloud protection system; secure and efficient access to data outsourcing (Malik and Nazir, 2012).

Darshana Agrawal, propose a Framework based on a data migration mechanism between clouds that pro-vides greater security guarantees and shorter transfer intervals for giant-scale information files and migration in cloud computing administration systems.

On the issue of data migration in cloud computing systems, they propose a protocol in two phases. First, in contrast to most previous work, to ensure the integrity of remote data, the new Framework supports secure and economical dynamic operations on blocks of knowledge, including update, delete and attach. Second, an extensive security analysis to prevent malicious knowledge modification attacks and even server collusion attacks.

With this Framework, the author explains, that using distributed verification of encrypted information, whenever information corruption is detected during the correction of storage verification on distributed servers, the user can almost guarantee the simultaneous identification of the server as corrupted (Agrawal, 2016).

Arun Fera, present a reliable and special monitor system framework, that provides highly reliable cybersecurity automatically excluding domain areas where the environment is considered dangerous, in addition he propose the use of reliable technologically systems to guarantee the assurance of the environment monitorizations. He ca resolve the problem of liability, with a mechanism to monitoring the use of the data and information's in the CC system. The author's proposal assures the correct accessing by users, access that is managed by strong policies in conjunction with online monitoring, checking whether SLA agreements have been breached. It is a sophisticated framework based on a real-time analysis of the logs.

The author calls or its structure the Cloud Data Accountability framework (CDA), the main components consist of a system for making log records available and analyzing them. That log generator is to creating is responsible for in-depth analysis of these to detect errors and cybersecurity failures that can be analyzed through explicit errors, as well as automatically transmitting this information to the system administrator. The files are protecting with cypher system by a public key and the user logs have access to the files using a private key to achieve the integrity of data.

The user uses a package data file that includes the original cypher information, with authorization policies and logon strong strategies. These political systems help CDA to authenticate the user and to grant authorization to data information. These kinds of strong policies are automatically implemented based on the type of use they are automatically implemented based on the type of use, in relation to the data stored in the individual areas of a CC structure.

The authentication by the CC technologies and the request for accessing to user information on the access control rights indicated above based on the authorizations policies. Logon technology started in each information access and the log administration starts generating log files for all information accessed in the CC.

The hacker cannot change the contents of the log information after dismounting package. Integrity check engine for log files detect immediately changes to the log files, this technology auto-check automatically is log files match or not-match in the verification by the log file analyzer. Author proposes the use of Reed-Solomon encoding for the verification mechanism, so the log analyzer immediately identifies unusual changes to log files (Fera *et al*., 2015).

Threats, Attack Topology, Risks Underling Cloud Computing

- Threats (confidentiality field)

Inside cybersecurity dangerous:

- Dangers CC enterprises
- Dangers users at the CC client level
- Malicious users by third parties (e.g., companies outsourced by a cloud computing provider)

Characterization: The threat of privileged access to customer data held in the cloud is more significant, as each of the delivery models may introduce the need for multiple inside user:

- System-as-a-Service, CC clients and administration technicians
- Platform-as-a-Service, SW implementations and testing environment administrators
- Infrastructure-as-a-Service, outsider’s platform administrators and power users. Thus, an L language is a set of words. There are decidable languages and recognizable languages (Travassos, 2012)

External threats:

- Outside CC IaaS software attackers
- Remote attack to CC applications
- Remote cloud infrastructure software attack
- Outside hardware (hereinafter referred to as HW) cyberattack against the CC
- Outside cyberattack of software (hereinafter referred to as SW) and HW against CC enterprises and users, SW and end-user HW
- Social engineering by employees of CC enterprises and CC users

Characterization: The threat from the outside attacker can be seen as most applied to Internet-facing public CC; nevertheless, any type of CC available models can be changed by outsiders cyberattacks, mainly in private CC on what users' can be redirected. CC providers with big datacenters have, for example, credit card information’s, personal data and special intellectual and government information may be targeted by teams with sophisticated features, with the goal to steal information’s. Including HW cyberattack threats, social engineering and information DDOS attacks by organized hackers.

Information leaks:

- Cyber security authorizations failure in several systems
- Disaster of cybernetic and physical communications for CC information backups

Characterization: Widespread cyberthreat of information and information leakage among very potentially competing enterprises they use same CC enterprise services can be originated by human flaws or HW fail which may imply to failures in the protection of information (Sedgewick and Wayne, 2011):

- Threats (Integrity Area)

Data segregation:

- Incorrect definition of safety boundaries
- Inefficient configuration of Hypervisors and/or virtual machine (from now on referred to as VM)

Characterization: Data integrity in complex CC storage platforms, like Software-as-a-Service prepared to share resources among clients and users, can represent danger to the integrity of information if infrastructure of the data storage is not physically separated.

Users accessibility:

- Inadequate procedures in identification and authorization management

Characterization: Configuration of deficient authorizations to information can be the basis for successful cyberattacks, e.g., discontent from former employees of cloud provider organizations, who have outside capability to accessing the enterprise CC service administration may imply leakage of information and change of information without being detected. Information quality:

- Applications with issues or defective objects into infrastructure.

Characterization: The danger of an attack on information quality increases as CC enterprises store too much customer data and information. Implementation of a defective a system not properly configured and accessed by a customer can cause a very serious security breach and affect other cloud users' data integrity with whom the infrastructure is shared (Bruening and Treacy, 2009):

- Threats (availability area)

Change of management:

- One customer penetration tests impact other cloud customer
- Changes in the infrastructure of the CC enterprise, customer and third-party systems which affect CC clients

Characterization: As the CC enterprisers has an increasing attention in managing and modify in all CC delivery models-types, create a hypothetical danger that changes might input adverse effects. The origin of this is possibly come by SW or HW changes to default CC services (Chen *et al*., 2010):

- The threat of denial of service
- Distributed denial-of-network-bandwidth-service
- Denial of network DNS services
- Denial-of-Service for applications

Characterization: The threat-of-denial-of-service from computing systems in the CC is often an outside cyberthreat against public CC technologies. Nevertheless, the danger may impact all CC services and model-types, as outside and inside cyberthreat agents may introduce SW components and HW that trigger DOS cyberattack.

Physical security changes:

- Interruption of information technology systems by connection TCP/IP
- Interruption of the CC enterprises Information Technology services through physical access
- Interruption of services from this WAN enterprises

Characterization: Cyberthreat of shutdown some CC services and technologies originated by TCP-IP connections differs at big CC service and their clients. CC enterprises must have experience in cybersecurity extensive datacenter high technology for achieve resilience and sophisticate technologies to maintain de cybersecurity. Can exist a cyberthreat that the CC users may by physically attack easily, but usually is internal and external experts, in offices with low security and relocated from the main computing centers that suffer most from this type of professional attacks.

Weaknesses exploitation in data recovery procedures:

- Invoking an unsuitable cyberattack recovery and the continued availability of information
- Characterization: The danger of inappropriate incident recovery administration, once beginning, increases in the moment CC users consider recovering their internals alongside those administration by other outsider’s CC service enterprises. If the technologies are not analyzed, consequently the recovery uptime it will be very long

Framework Context

This chapter presents the whole conceptual part of the framework, from the fundamental principles underlying it, to the technological principles that can be integrated into each of the framework's components. Initially, a more summarized description is provided in a logical perspective of the framework and then all the features are described and conceptualized. A small comparison is made between the framework developed and the Frameworks referred to in state of the art, differentiating what it may have as innovative. The descriptive and conceptual development is carried out from a layer perspective; we refer to the security bed, as it is the articulated and homogeneous set of all these layers, which will allow us to achieve the goal: Information security in the private on-premise cloud.

Cybersecurity can no longer be a belated reflection on a set of measures to be implemented in a system; it must become an initial system design consideration that must be at the core of all cloud computing implementations. For most companies using public cloud structures, there is little ability to request modifications or additions to their provider's security architecture. Companies or organizations capable of creating a private cloud can develop an implementation of their security architecture and even innovate in terms of security. In terms of private cloud architecture implementations, it is not enough to consider information security exclusively as one of the three essential pillars: Confidentiality, integrity and availability. This basic theory are the main indicators of safety, cyber protection to give that 3 security pillars (confidentiality, integrity and availability) in a private CC, but in this case are more complex in technical terms compared to a traditional data center architecture.

In this framework, security controls need to be continuously monitored and take into consideration standardized tactics and methodologies in each of the following areas (VCE Company, 2015):

- Computing: Physical servers; operating system, CPU, memory, disk space and other hardware
- Network: Local virtual networks, demilitarized zone, segmentation, redundancy, connectivity
- Storage: Numbers of logical units, ports, partitions, backup and fail-safe technologies
- Virtualization: Hypervisor, geolocation, administration, authentication and data-authorization
- Applications: Multi-allocation, isolation, load balancing, authentication

Attack resilience helps protect the company's critical information's from inside and outside cyberattacks with implementation of healthy technology systems and good security practices. The issue of asset and data protection in a cloud dramatically differs depending on the implementation model; it's essential to distinguish between public and private clouds. With the protection of information in a public CC, usual Cyber Protection technologies are be enough in standard scenarios but will not be enough at enterprise or organizations they have not long access to the bases of infrastructure or OS. By creating a private CC platform, information users remain individual property and the responsibility for that information is the company that provides the services, which increases its responsibility in large data scenarios. Without a strong qualified and expertise information technology administrator highly qualified and support to technology CC platforms the enterprise cannot run, automate and monitor the systems, a potentially dangerous framework can be created.

Incident readiness is an essential component of the strategy that can help detect violations or cybersecurity attacks. With a cybersecurity breach, it is usual for the first thing is consultation of important data such as file log and packet capturing and obtaining forensic footprints. Suppose an enterprise didn't implement the required technology before a cybersecurity attack. In that case, usually all the information about the attackers is manually deleted for them and in many cases other information is provided by substitution during the breached. Technology to acquire event information's and security problems related to data, endpoint logging, in real-time action, with their storage at a secure point, will help to create the a scenario that allows to identify the origin of the attack and the consequences that the same impacted on the information, so in the future this type of attack can be remedied.

Developing a strong cybersecurity tool with an intelligence analyses, with a risk-based policy is a base required for mitigate cyberattacks. The constituent components of cybersecurity systems, which are considered in this framework, are specific security policies, a complete technique to mitigate cyberattack and a comprehensive and a safety training plan for all employees (Loeffer, 2013).

Safety in a private CC they impose that all the components of a normal system are subject to a well elaborated plan against cyber-attacks and that it contains a layer of redundancy in case the attack occurs. Aside from these recommended indications, we must consider context specific issues in Private CC, which are not considered in public CC. If the data in the Private CC has been cataloged as highly sensitive or classified higher than "Reserved", supplementary security measures must be considered, including reliable multi-allocation, data security and advanced identity management. The security of a private cloud, especially on-premise, becomes strong administration e online monitorization 24/24 by 7/7 of all operations and cybersecurity technically and methodologically so that no critical aspect is forgotten or easily exploited.

The developed framework, which applies to a private on-premise cloud structure, is designed to be used in an architectural system supported by the virtualization of servers and virtual access machines.

Thus, virtualization assumes a relevant role in this process; on the other hand, virtualization itself is a layer that can work as an addition of security if the architecture is well designed and well implemented.

The Framework

The framework is based on the basic principle that the private cloud system is on-premise. It is in the organization's physical facilities, thus requiring full control and administration of the entire infrastructure by the proprietary organization.

It is based on four primary pillars, which complement each other and interact in total synchrony and conformity; we have a graphic representation in Fig. 1.

A pillar related to governance, the responsibility of the organization's administrators and Information Technology Administrators, in which security policies, job assignment, user training and awareness and security training plans are established.

Another pillar specifically related to risk analysis, the responsibility of directors in which international standard standards are followed.

A third, entirely technical pillar under the responsibility of Information Technology Administrators, in which a model is developed and created allowing for a techno-logical implementation that enables the updating of the essential software of the private cloud structure (such as operating systems), without the systems integrating this private cloud being at any time in direct or indirect connection with the Internet. Maintaining a complete isolation policy but fulfilling another essential security requirement is the continuous software update.

A fourth pillar, totally of operations and technology, is inserted inside the security perimeter and within the facilities where the hardware is installed. This pillar comprises several layers, starting with one related to the physical security of the data center facilities, followed by another physical and logical protection, i.e., the first firewall, with a robust traffic management system, controlling access to the early logical domain. After the traffic passage through this first layer, the authentication and authorization for the first domain are done. Then there is the first layer of virtualization; the external user accesses a virtual computer allocated in the early domain. From this first domain and through a virtual computer, users access a second domain already inside the private cloud, where a double authentication and authorization is carried out and another firewall has scrutinized the traffic from the first to the second domain; also, this robust and with a physical base computing system, all traffic between the first and second do-main is encrypted. The dual-domain users have authorization to data information stored at private CC from the second domain's positive authorization.

The Private Cloud is equipped with several security technologies, including data protection, encryption, antivirus and malware, permanent monitoring, alerting system and an advanced redundancy system to prevent failure and preserve the continuity of deployment. All this can be represented by a set of abstract layers illustrated in Fig. 1.

The entire proposed framework that is graphically rep-resented in Fig. 2.

Its objectives are only achieved if there is an integration of all the components to be described.

Physical Security

Physical cybersecurity is a technical concept and art of protect system of no allow inclusion of normal and important information. This technique, involve procedures, equipment, specialized personnel and viewing everything that goes on in the perimeter, preserving the systems from stolen information or an unauthorized access.

Likewise, the term cybersecurity means protecting access to the property, equipment's, doors and information of all kind, including cyber-electronic, information and control vigilance.

Today, physical cybersecurity is an integrated set of techniques and synergies within physical and cybersecurity domains. The two are needed to give a robust general cybersecurity position and system.

We can think cybersecurity platform in simple way terms, like as a door with a lock, a cybersecurity guard doing around, or some other method used to protect assets, there are several.

The cybersecurity systems normally are a sum of a set safety-critical procedure experimented in the laboratory and analyzed in depth, so that they can be executed to achieve the safety objectives for which they were designed.

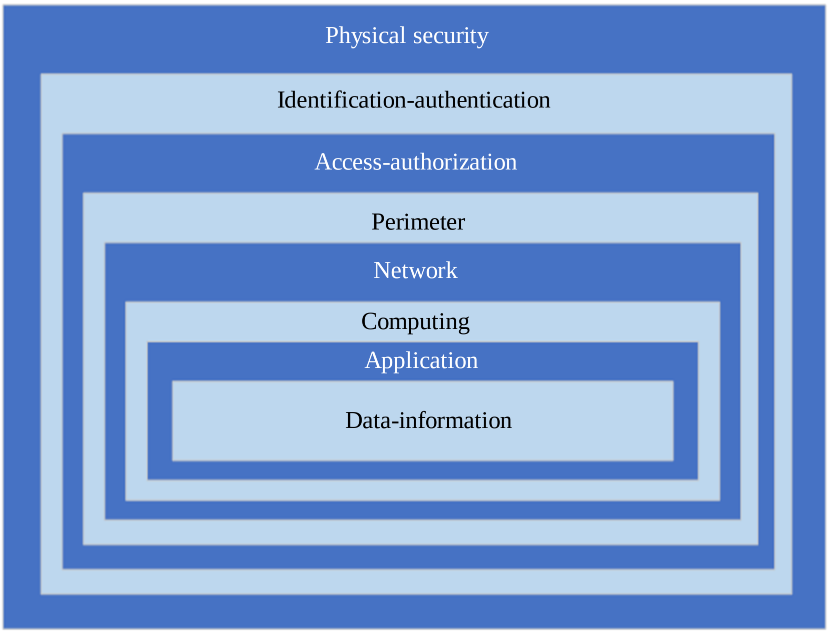

Fig. 1: Logical layers model of the framework security

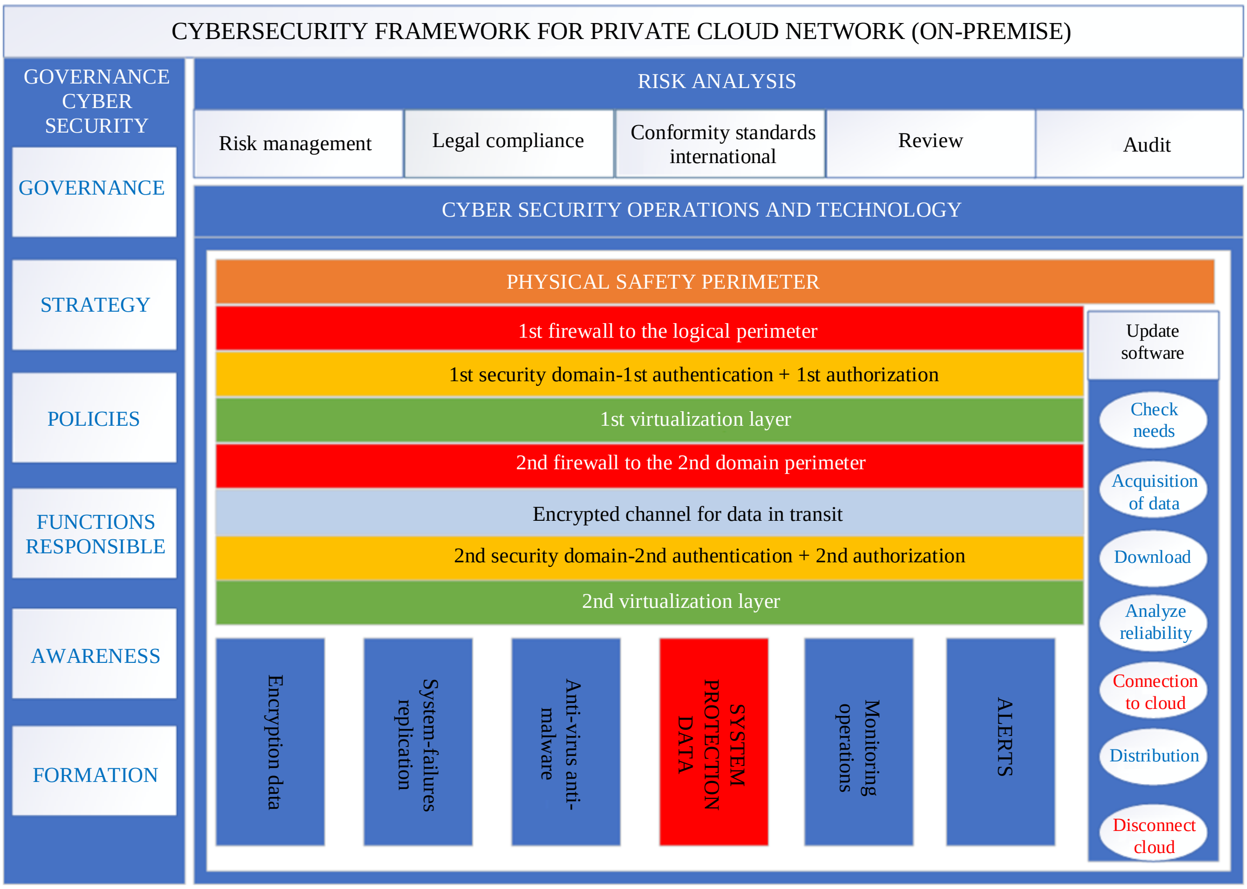
CYBERSECURITY FRAMEWORK FOR PRIVATE CLOUD NETWORK (ON-PREMISE)
GOVERNANCE CYBER SECURITY
GOVERNANCE
STRATEGY
POLICIES
FUNCTIONS RESPONSIBLE
AWARENESS
FORMATION
RISK ANALYSIS
Risk management
Legal compliance
Conformity standards international
Review
Audit
CYBER SECURITY OPERATIONS AND TECHNOLOGY
PHYSICAL SAFETY PERIMETER
1st firewall to the logical perimeter
1st security domain-1st authentication + 1st authorization
1st virtualization layer
2nd firewall to the 2nd domain perimeter
Encrypted channel for data in transit
2nd security domain-2nd authentication + 2nd authorization
2nd virtualization layer
Encryption data
System-failures replication
Anti-virus anti-malware
SYSTEM PROTECTION DATA
Monitoring operations
ALERTS
Update software
Check needs
Acquisition of data
Download
Analyze reliability
Connection to cloud
Distribution
Disconnect cloud

Fig. 2: Framework graphic representation

We have 3 usual layers to design and implement a strategy to protect CC platform information (an area, building, space around and technology): Outer Perimeter Protection, Building Protection and Interior Protection):

a) The External Perimeter: Protecting this space involves monitoring of all outside the perimeter and inside the perimeter, delimiting this perimeter. Examples of typical physical external boundaries can be property lines or outer fences of an enterprise
b) The Internal area: The perimeter usually involves special fences, special inside-doors and protected-windows-external or internal, depending on the context of the outer frame
c) The inside: We have most internal security high-level and consists is the office, storage, etc. that have special protection. The storage system to which our Framework fits must be in the most protected area of this layer
d) This security pillar should consider access control, physical security controls, security policies, gates with access control, authentication systems, remote access monitoring, video surveillance

Administration Specialized

In generals is the responsibility of the managers in a company or organization (for instance, the board and executive management of a corporation, the director of an organization) to provide strategic direction, ensure that objectives are obtained; verifying the cyber-risks are appropriately a guaranty the company is protected. We can associate cyber-risks and storage information can with different issues (e.g., computation, finances, legal, compliance, sensitive information, human resources) and other domains needing knowledge to deal with risks. Therefore, corporate administration is often structured by logical sectors.

Cybersecurity administration refers to the corporate governance component that deals with the company's dependency on information that must be protected from opponents. Therefore, cybersecurity governance covers, nowadays, it practically covers all areas of a company, in the physical and logical sense. The template presented and inserted in our framework is adaptable to any type of corporate governance. Yet, it is a crucial element of the framework.

It includes the following components: Cybersecurity governance; security strategy; cybersecurity policies; cybersecurity roles and responsibilities; cybersecurity awareness, cybersecurity training.

Management of Security Risks

Principle: A cybersecurity risk management process must be defined, approved, implemented and aligned with the organization's corporate risk management process.

Objective: To ensure that cybersecurity risks are appropriately managed and implement protections for information-confidentiality, information-integrity and information-availability and to ensure that the cybersecurity risk management process is aligned with the organization's corporate risk management process.

It includes the following components: Security risk management, legal compliance; compliance with international standards; monitoring, review and analysis of risk in cybersecurity; cybersecurity audit.

Logical Security Perimeters

At the level of identification, authentication, authorization, availability and group policies, the logical perimeters of the entire framework are managed by two active directory services (Mirosoft, 2016).

The first directory service creates a general perimeter of the organization's base network; the second directory service creates the security perimeter of the On-premise Private Cloud.

An accredited user of the organization, through a terminal registered in the first Active Directory, makes his identification and authentication in it; if the authentication is successful, the authorization policies that were previously configured for him will be implemented. In case this user is authorized to access the On-Premise Private Cloud, he accesses a virtual machine allocated in a Hypervisor which belongs to the network managed by this first Active Directory; from that virtual machine (which works as a virtual terminal), he accesses the second Active Directory, which manages identification, authentication, authorization and availability to On-Premise Private Cloud, if authentication is accepted, it will have access to the data and information contained in On-Premise Private Cloud, specifically to a virtual server that functions as a database. Active Directory has more functions than those described in the previous paragraph, even at the level of operation of this frame-work, it is responsible for implementing security policies, divided into groups, manages the logical process of all computers on the network, has incorporated DNS servers and also manages network encryption for data in transit. The servers responsible for managing every-thing described are called Domain Controllers.

Virtualization Layers

Two layers of virtualization are provided in the model, embodied by Hypervisors in the first logical perimeter, belonging to the first Active Directory and the second layer of virtualization that fully supports the private On-Premise cloud. The first layer of virtualization gives access to virtual computers, which allow internal access to private cloud servers On-Premise. The second layer of virtualization stores and allocates the private cloud servers. Both virtualization layers also work as increased security. The main security features provided by the two layers of virtualization are as follows.

Hyper-V VM with Securing Boot: In this day’s system-servers need the capacity to validating systems not only by operating system (hereafter referred to as OS) in the t boot case process onwards. Cybercriminals are increasingly intelligent and sophisticated in their use of invasive technologies and instantiate dangerous things much earlier in boot of OS itself. A system that assists in checking loyalty of a server-OS is the securing-booting system. This system is built on the *Unified Extensible Firmware Interface*. This is a better solution than normal BIOS initialized system. Both systems are responsible for running the HW devices before transferring the access of the HW devices to the OS. But, the BIOS running and the *Unified Extensible Firmware Interface*, both authorize the use of a securing system in the begin of the start system. Microsoft's Secure initiating running system, allows the OS detect cybersecurity issues, like rootkits, malware and memory virus, this kind of dangerous have the objective to compromise the OS at the early stages of a server startup process. This technology ensures the run booting, from the firmware to OS kernel loading securely, with reliability and has not been tampered with. A secure startup requires all startup codes and drivers to be properly identify. This technology decreases dramatically the danger of malware installation in this critical moment of startup systems. This technology appeared for the first time with the launch of OS Server in 2012 and the respective edition named after the year. With this 2012 R2 Editions, the technology of protection the initializations of the OS have been just for VM in the Microsoft Hypervisors. But, 2016 Server Edition, Microsoft implemented the possibility to be applied to VM with OP Linux executed in the Hypervisor Microsoft Server.

Hyper-V VM protection (vTPM): TPM increases the difficulty to attack on an encrypted drives and breaking the key this is because part of the key is stored in the HW system. Virtual TPM or "Virtual" Trusted Platform Module virtualizes the TPM module so virtual machines can use it. The Microsoft Servers Editions 2016/2019 Hypervisors, vTPM was implemented as a default base VN 2G, being possible BitLocker encrypt information’s in the booting system at the volume in the VM.

Hypervisor Shielded VMs: The cybersecurity issues described above are designed for maximum cybersecurity VM protection at the Hypervisor. At Server 2016/2019, this technology has been fully implemented and improved. Protected VM use this cybersecurity function provided to VMs by the vTPM system, allows to encrypt the booting running at volume and other cybersecurity-focused features.

Protected VM and take advantage of the already mentioned "*Host Guardian Service"* (HGS) is essential; however, protected VM force to deployed in running mode use a proper HGS used exclusively in a cluster of "at least" three nodes with Hypervisor-Server 2016 and in minimal 1 or 2 protected hypervisor-hosts running OS-Server 2016 or 2019 with respective hypervisor. With this we protected VM running within a protected framework.

Encryption

At the encryption level, the model must use two technologies: Data in transit from the private On-Premise cloud to the user and another for data and information at rest in the cloud servers.

In the case of data in transit, it is proposed to use IPsec for data at rest; it is suggested to use disk cipher. Bit-Locker is an information protecting system at OS made available for the first time in 2010, having been improved ever since, to allow the system more cybersecurity protection. BitLocker integrated into the OS protects against the danger to lose information and confidentiality, or unauthorized changes to information. When installing the optional BitLocker component on OS, we need to install Advanced Storage functionality to allow encryption of HW drives. On OS-servers, an additional part of Bit-Locker that can be implemented is the network unlocking of BitLocker.

Replication-Failure Remediation System

This is an anti-fault system. It ensures the availability of information to users in case of a server's failure that stores data and information. In practice, it ensures the constant availability of information. In the event of a failure in a server that stores the data, the second replica server is automatically activated to provide the same information. The Hyper-V Replica technology performs this function; however, other software also performs this function, such as Altaro Replica, which works integrated with Hyper-V or WM ware Hypervisor. The Microsoft Hypervisor 2016 and 2019 replica-system use a nonsynchronous technic to replicate information between 2 replica-Hypervisor using an TCP/IP network. This function to replicate the running information and services from one VM to other VM in a secondary Hypervisor-server, by that we obtain a disaster recovery system and the service continuity with protection for the virtual platform. Only one of the hypervisors is the virtual machines active. On the hypervisor, the virtual machines are inactive but receive 30 and 30 sec, all the changes occurring in the VM in production mode.

Operations Monitoring

The framework provides one server exclusively for global monitoring of all operating systems managed by the second Active Directory, i.e., global tracking of private On-Premise cloud systems.

The object is to detect anomalies before they occur or impact the network.

Namely and mainly in the following areas: Network, servers.

Software Updates

Updating private cloud operating systems is as essential as any operating system. However, the cloud is isolated from the Internet, so a process had to be developed to allow these operating systems to be updated without direct contact with the Internet.

The system proposed in the framework uses an update server linked to Microsoft's update server outside the two Active Directory's perimeters. This server directly downloads the necessary updates from Microsoft and stores them.

There will be on the perimeter managed by the Active Directory of the private cloud another update server that at scheduled times connects to the update server outside the frame and downloads the updates; these updates are verified and once authorized, update the operating systems of the machines belonging to the private cloud On-Premise.

The technology proposed for this solution is *Windows Server Update Service*s (WSUS). A WSUS server provides resources to manage and distribute updates through an administration console. A "WSUS-server" can be the data base of upgrading to second system in the network or outside de network. The "WSUS" operates data base origin of data like an upstream system. With WSUS installation, in the minimal 1 WSUS-server on the network will have to connect to the mother system at Microsoft to obtain available update information. Administrators can configure the system in very different ways depending on company policies and existing network segments, as well as the level of protection that each segment has.

Data Protection System

Entire set of systems, information and data in the private On-Premise cloud must have a security system for data protection and recovery in case of any incident, working in parallel with the replication system already mentioned above.

Unlike the replication system, this information and data protection system that you are proposing acts exclusively on information and not OS.

Microsoft "*System Center Data Protection Manager*" (SCDPM) can be used, as it is considered one of the best systems globally, or a system such as Altaro, which also protects data and simultaneously runs an integrated replication system.

The SCDPM's is a system for redundancy and recovery information. SCDPM makes available instantaneous protection for information in all systems, clients or servers. For datacenters, System Center Data Protection Manager it allows all administration in a global and totally remote way, obtaining an integrative vision in terms of cybersecurity of the entire system and the protection that is being implemented with this system. SCDPM functioning (Altaro's system has the same working orchestration).

This implement this level of protection, the DPM system generates and keeps a replica and an exact copy, of the information found at the of the machines that are being protected. This backup of information's is keeping in a logical group, consisting of a set of special storage at DPM-Server specially configured to store this redundant information. This function can run minute by minute depending on the configuration. This technology performs a highly consistent check block by block, on the disks, increasing the new information in the redundancy system.

The DPM system-agents control the changings protecting information and report the new information to the central unit of DPM. Besides, protection indicates on-running information even if a mitigation process is underway recovered from a problem. All computers to be protected must have an agent installed. This function can be done individually computer to computer or it can be through a centralized system.

Protection groups are used to better apply cybersecurity policies to each of the network segments or to sets of computers and servers with different functions.

Comparison to Other Frameworks

None of the analyzed frameworks are specifically designed for an on-premise private cloud computing framework situation. Consequently, none of them refers to issues of physical perimeter security. None of them is the issue of system upgrades safely addressed and no procedure or technological support is established for this to be implemented.

List of characteristics and components of the Frameworks, presented in Table 1:

a) Infrastructure physical security
b) Cybersecurity governance
c) Risk analysis
d) Superimposed safety logical perimeters
e) Double layers of virtualization
f) Encryption
g) Data permanent replication
h) Anti-fault system
i) Systems monitoring
j) Safe software updating
k) Physical data protection system
l) Double identification, authentication and authorization

The existence of an "X" in the chart's cell indicates that the component's presence in the framework.

In addition to references to encryption issues, no reference is made to data protection issues in transit within the inner perimeter of the private cloud relative to the organization's overall network structure.

None of them has specified technology or methodology for global data protection contemplating a simultaneous integrated solution of confidentiality, integrity and availability. Also, none of them addresses a solution to guarantee the functioning and availability in case of disaster or failure of a system in which services and data are being made available. The analyzed Frameworks do not mention failover clustering solutions for data or information storage. No solutions are presented regarding On-Premise security policies for creating redundant and duplicate authentication and authorization layers.

They have in common the analysis and enunciation of the need to safeguard the issues of Confidentiality, Integrity and availability, but separately and independently and never integrated. In short, none of the frameworks specifically addresses an on-premise private cloud solution with the unique features that they impose.

Table 1: Frameworks comparison

Framework	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)
Of this study	X	X	X	X	X	X	X	X	X	X	X	X
NIST		X	X			X	X	X	X	X	X	
Arijit Ukil			X			X						
Shadi Aljawareh		X	X									
Sang-Ho			X			X			X			
Aman Sharma					X	X	X				X	
Ayesha Malik							X					
Darshana Agrawal						X	X		X			
Arun Fera						X			X			X

Conclusion

This study main objective was to develop an integral and global framework to be applied in private on-premise cloud computing systems that need to be isolated in physical and logical terms from other networks. Specifically, in situations involving the need to protect highly sensitive and confidential information.

A Framework was developed, consisting of aggregated elements and a fully integrated operating logic. This framework comprehends: The physical security of facilities at various levels, governance in cybersecurity, risk management and analysis, duplicate logical perimeters, dual layers of virtualization as security elements, two encryption systems, replication system for operation in case of failures or catastrophes, monitoring of all processes in the cloud infrastructure, secure updating of software as well as an advanced data and information protection system.

A private on-premise cloud computing infrastructure was implemented in the laboratory and the framework was applied, with the technological contingency's mentioned in the corresponding chapter.

Finally, a comparison was made between the framework developed and other existing Frameworks. It was concluded that it was the most comprehensive of all, encompassing all the components that are currently considered vital in protecting systems from cybersecurity-ty problems.

Acknowledgement

We are grateful for the support given to research by the Higher Institute of Advanced Technologies (ISTEC). The guiding contribution made by Professor Miguel Nuno Dias Alves Pupo Correia, from IST, was fundamental and deserves thanks. I also thank you for contributing to my Research Center of scientific affiliation: CIDEHUS of the University of Évora.

Ethics

This article is original and contains unpublished material. The author has read and approved the manuscript and no ethical issues are involved.

References

Agrawal, D. (2016). A new Framework for Improving Security for Data Migration in Cloud Computing. International Journal of Innovative Computer Science & Engineering, 3(4).

Aljawarneh, S. A., & Yassein, M. O. B. (2016). A conceptual security framework for cloud computing issues. International Journal of Intelligent Information Technologies (IJIIT), 12(2), 12-24.

Bruening, P. J., & Treacy, B. C. (2009). Cloud computing: privacy, security challenges. Bureau of Nat'l Affairs.

Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.

Fera, M. A., Natarajan, I., Brinda, K., & Darathiprincy, R. (2015). Enhancing security in cloud using trusted monitoring framework. Procedia Computer Science, 48, 198-203.

Loeffer, B. (2013). "Private Cloud Principles, Concepts and Patterns," TechNet, https://social.technet.microsoft.com/wiki/contents/articles/4346.private-cloud-principles-concepts-and-patterns.aspx

Malik, A., & Nazir, M. M. (2012). Security framework for cloud computing environment: A review. Journal of Emerging Trends in Computing and Information Sciences, 3(3), 390-394.

Mirosoft. (2016). What's new in Active Directory Domain Services for Windows Server 2016. https://docs.microsoft.com/en-us/windows-server/identity/whats-new-active-directory-domain-services

Na, S. H., Park, J. Y., & Huh, E. N. (2010, December). Personal cloud computing security framework. In 2010 IEEE Asia-Pacific Services Computing Conference (pp. 671-675). IEEE.

NIST. (2020). NIST cybersecurity framework. NIST. https://www.nist.gov/cyberframework

Sedgewick, R., & Wayne, K. (2011). Algorithms. Addison-wesley professional..

Sharma, S. (2019). "Security and Data Storage Aspect in Cloud Computing," Studies in Big Data, 52, ISBN 978-981-13-6089-3, Springer.

Travassos, V. (2012). Virtualization Trends Trace Their Origins Back to the Mainframe. IBM Systems Magazine, 1(4), 2012.

Ukil, A., Jana, D., & De Sarkar, A. (2013). A security framework in cloud computing infrastructure. International Journal of Network Security & Its Applications, 5(5), 11.

VCE Company, L. (2015). "Enabling, Trusted Multi-Tenancy with Vblock Systems.," VCE Company, LLC: Richardson, TX. https://docplayer.net/3786368-Enabling-trusted-multi-tenancy-with-vblock-systems.html