Open Access Library Journal
2023, Volume 10, e9699
ISSN Online: 2333-9721
ISSN Print: 2333-9705

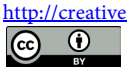
An Enhanced Healthcare Integration System Based on Cloud Computing during the Coronavirus Crisis

Samah A. Massadeh, Rose M. Al-Qasem, Nawal A. Al-Zabin, Sara I. Al-Issa

Department of Electrical Engineering, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan
Email: smassadeh@bau.edu.jo, rose_alqasem@bau.edu.jo, nawal_alzabin@bau.edu.jo, 32215333103@std.bau.edu.jo

How to cite this paper: Massadeh, S.A., Al-Qasem, R.M., Al-Zabin, N.A. and Al-Issa, S.I. (2023) An Enhanced Healthcare Integration System Based on Cloud Computing during the Coronavirus Crisis. *Open Access Library Journal*, **10**: e9699.
https://doi.org/10.4236/oalib.1109699

Received: December 21, 2022
Accepted: February 10, 2023
Published: February 13, 2023



Abstract

Coronavirus had some healthcare organizations embrace cloud hosting without proper investigation or review. This raises challenges concerning security and privacy aspects and could lead to lasting risks and vulnerabilities in the system. Our project's main objectives include separating medical information from other data, such as billing and accounting information, and integrating e-health cards into the system. The TVD infrastructure isolates and protects the TVD from adversaries from the outside. In this paper, we examined security and privacy issues in E-health systems, and then we proposed a secure e-health infrastructure based on Trusted Virtual Domains (TVDs) to ensure fundamental security and privacy properties.

Subject Areas

Cloud Computing

Keywords

Cloud Computing, Coronavirus, Trusted Virtual Domains, Electronic Health Records

1. Introduction

Healthcare is defined as the service delivered to individuals or populations by healthcare service providers to promote, maintain, monitor, or restore health [1].

In healthcare, the volume and complexity of digital healthcare data grow exponentially each year, factors driving this big-data scenario include changes within the payer environment, the use of electronic health records (EHRs) and a

shift toward value-based payments. Technology changes are also driving data increases as patients employ the newest in mobile digital devices, including activity monitors and chronic disease monitoring applications like blood sugar trackers for diabetics, the growth within the use of Internet of Things (IoT) applications and therefore the use of patient genomic information is increasing healthcare providers' data-storage and data-analytics needs.

Using of information technology in healthcare (healthcare IT) has become increasingly important in many countries in recent years. Cloud computing aims to incorporate many existing computing approaches and technologies such as distributed services, applications, information, and infrastructure consisting of pools of computers, networks, information, and storage resources [2], but the healthcare industry has been slow to embrace technologies-like using the cloud for analytics, that would help them leverage their growing information assets.

Due to the Coronavirus pandemic a lot of healthcare organizations embraced cloud adoption without making sure that the transition is secure and without prior knowledge of cloud services, the speed and scale at which healthcare organizations have had to embrace cloud hosting, this sudden and rapid shift could lead to lasting risks and vulnerabilities for a way bigger attack surface.

Since the healthcare industry requires higher security and privacy standards that have to be managed carefully. The hasty rush to cloud hosting during the Coronavirus crisis could set the stage for a "cyber pandemic", which would leave healthcare security teams during a reactive mode as they struggle to spot new vulnerabilities and stop new threats and staying proactive of potential attacks.

The healthcare attack surface of unmanaged medical IoT devices is now compounded with an attack of unmanaged cloud services; this is often incredibly risky and represents a future cyber pandemic just waiting to happen.

In the Coronavirus crisis, the necessity for immediate response outweighed the traditional policy for secure data handling. But even when the Coronavirus crisis emergency hopefully ends, the healthcare security teams will likely struggle with managing the necessity for the availability of patient information with the policy and controls required for securing and protecting that data within the cloud.

To help solve this problem we propose a secure e-health infrastructure based on Trusted Virtual Domains (TVDs) to ensure fundamental security and privacy properties.

2. Methods

Trusted Virtual Domains (TVDs) represent a new model for achieving IT and business security. TVDs address critical heterogeneity and complexity issues in existing models, they provide quantifiable security and operational management for business and IT services, and they simplify overall containment and trust management in large distributed systems [3].

In a virtualized environment, virtual machines (VMs) that share the same

physical infrastructure execute operating systems with different applications and services, each virtual machine is controlled by an underlying security kernel that serves as a virtual machine monitor and executes in a logically isolated execution environment (which we refer to as a compartment).

The user's work environment is now handled by a virtual machine hosted by the safety kernel, which runs alongside other architectural components on the physical platform.

A TVD could be a group of virtual machines that trust each other, share a common security policy, and enforce it regardless of the platform they're running on, the user's work environment is handled by a virtual machine hosted by the safety kernel, which runs alongside other architectural components on the physical platform, virtual machines belonging to the same TVD are connected by a virtual network that spans many platforms and is completely isolated from the virtual networks of other TVDs.

TVDs use cutting-edge security technologies to give these features: During system operation, the safety kernel must ensure that multiple domains are kept completely separate, when data leaves a website, such as during network transmission or disk storage, security services encrypt it with a cryptographic key that is only available within the related TVD.

TVDs help to prevent malware attacks by preventing unintentional information leakage, protect data from assaults and verify the integrity of platforms before they're permitted to hitch a ride on a TVD.

The automatic management of the TVD infrastructure is a key aspect, users have total visibility into the creation of TVDs, key management, and policy enforcement. Once a client platform joins a TVD, the infrastructure verifies its integrity and distributes keys and policies. Policy enforcement and encoding are performed by a security kernel on the client platform with no user interaction.

In our implementation, we deploy an IP secured virtual private network to secure the communication between multiple platforms during a TVD.

Since achieving security and privacy in e-Health is very vital in achieving the objectives of using this modern technology [4]. This is crucial because sharing and digitizing health-related data could result in various types of attacks. Many government health institutions have therefore developed a framework to ensure a high level of security and privacy.

Cloud computing has a lot of potential for facilitating quick access to healthcare data in the industry, cloud computing can help patients to gain access to their medical data from anywhere in the world via the Internet. The healthcare industry requires higher security and privacy standards. Cloud computing technology needs to be more carefully managed to meet this goal, this issue is more ethical and legal than technological.

On the international basis the ISO (Technical Committee 215) [5] and the Health Level consortium (HL7) [6] define standards for e-health infrastructures.

These are presented in **Table 1**.

Table 1. Security and privacy requirements as recommended by HIPAA7.

Requirement	Description
Patient's understanding	This implies that patients have an exclusive right to know and understand how their sensitive and private health information are kept and utilized by any healthcare provider.
Patient's control	This allows patients to be given permission to determine who can access his/her health data.
Confidentiality	Health information should be kept away from people who should not access it. The sanctity of the information should be maintained.
Data integrity	This ensures that manipulation and omission of health information is totally prohibited. Hence, health information being shared should be a true representation of original information without any form of amendment or alteration.
Consent exception	This stipulates that patient's information could be accessed without his consent only in emergency cases.
Non-repudiation	Healthcare practitioner should deny the fact that it has performed a certain activity on the sensitive data of patient. Such activity should be supported with evidence to avoid dispute or suspicion.
Auditing	This is a requirement that health data should be well monitored frequently along with any form of activity to ensure that data is well secured and protected. This will assist user to know the confidential status of his data.

3. Securing the E-Health Cloud

3.1. Model of the E-Health Cloud

In this section we will provide an overview of common e-health infrastructures as products or as proposed deployments in national healthcare information technology projects. We will present an abstract model of the resulting e-health clouds.

In the past, medical professionals (such the family doctor) kept local copies of their patients' medical records on paper. This made it possible to maintain a controlled environment with simple data privacy and security management: the paper records were kept in a closed cabin at the doctor's office. Even the growing usage of personal computers and contemporary information technology in healthcare facilities allowed for a modest effort to manage patient privacy and confidentiality. This was a result of each institution's infrastructure being locally and decentralized handled.

However, today's outsourcing of IT infrastructure (such as cloud computing) and other services (such as billing and accounting for medical practices) results in a complex system where privacy-sensitive data are stored and processed across numerous locations. Hence, it becomes attractive to store and process healthcare data in the cloud (at outsourced data providers that can be accessed via the Internet). Although such e-health systems promise a more affordable

service and improved service quality, managing data security and privacy also becomes more difficult.

We first present a basic model of the e-health cloud, and then we extend it to a more complex model in order to identify and discuss the various problem areas. We identify the involved parties and main components that are relevant for the focus of our paper.

3.2. Simple E-Health Cloud Infrastructure

We first consider a simple model that underlies commercial systems like Google Health1, Microsoft HealthVault2, and ICW LifeSensor3. In these systems patients store their own health-related data on certain web servers: Personal Health Record (PHR). In this model, patients track, collect, and manage the information about their health at online web sites. They can add their doctor's appointments, their illness dates and durations, and any other health-related information. Additionally, patients can import information into their PHRs from healthcare providers, such as x-ray images or laboratory results from their primary care physician or dentist. Figure 1 demonstrates this model and the parties involved.

The PHRs are kept on a cloud-based server owned by a different entity, data protection is the responsibility of the PHR server provider. Typically, patients are able to choose role-based access rights for certain healthcare providers. For instance, customers may choose that their family doctor has complete access while their personal trainer or health coach only has limited access to certain data. The PHR may be accessed from anywhere with such a strategy due of the centralized management (IT outsourcing).

The patient can easily give one doctor access to data and test results that were determined by another doctor, when the data is stored in the PHR. This can help to avoid double examination.

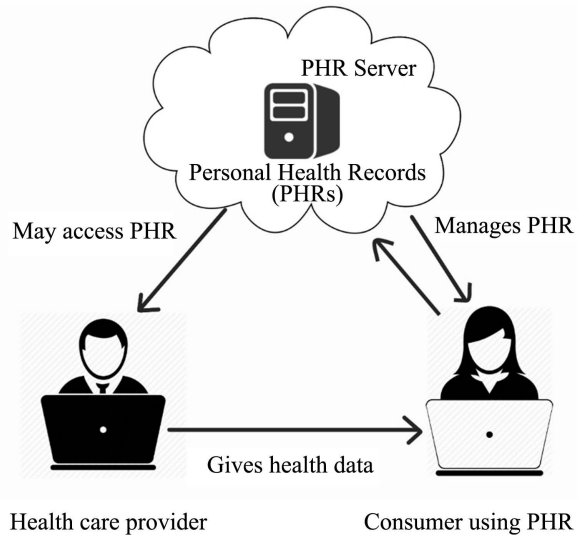


Figure 1. Simple e-health cloud model.

3.3. Advanced E-Health Cloud Infrastructure

In contrast to PHRs, which are managed by the patients, health professionals manage Electronic Health Records (EHR) only. In most countries, this involves different legal requirements and a clear distinction between PHRs and EHRs. As a result, infrastructures that involve EHRs are usually more complex than our simple e-health cloud model. Figure 2 shows the advanced model, which not only involves more parties (e.g., health insurances), but also includes some technical means to enforce data security and privacy of EHRs.

The general requirement in this model is still the functional and semantic interoperability of the data stored in EHRs. The EHRs are created, maintained, and managed by health care providers, and can be shared (via the central EHR server in the cloud) with other health professionals.

However, storing and processing EHRs is not the only service that can be outsourced to the cloud. The health care providers can use billing services that manage their billing and accounting with the health insurances of the patients. This is a typical scenario that can be found in practice, many doctors outsource the billing to third party providers, and those billing services accumulate the billing of several patients for different health insurances, but also for various health care providers at the same time. Therefore, privacy becomes an even more important aspect in this model because health insurances or billing services should not be able to access private details of EHRs.

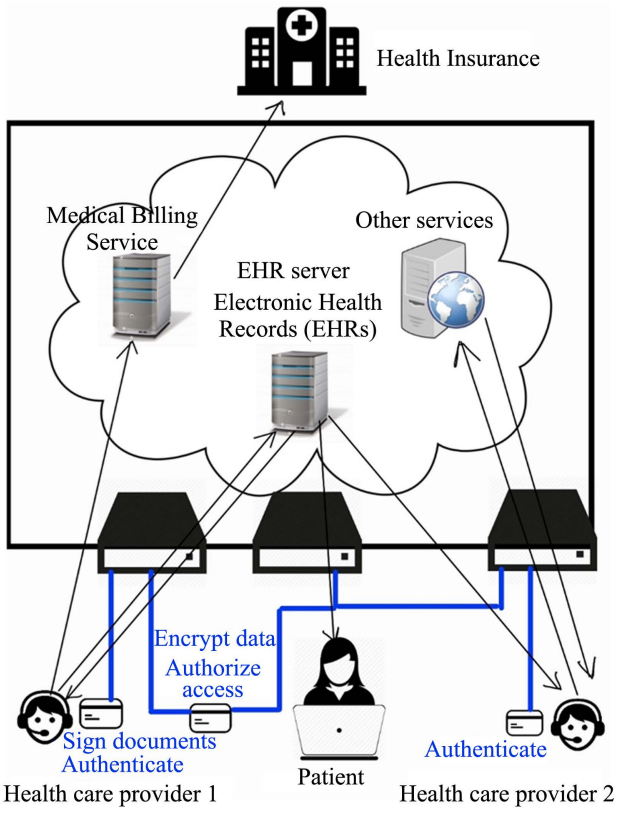


Figure 2. Advanced e-health cloud model.

Smartcards are commonly used to: 1) authenticate health professionals and patients; 2) sign EHR documents to ensure authenticity; 3) encrypt EHR data before it is saved in the cloud; 4) authorize access to EHR data in order to protect EHR data. Only unique interface connections to the telematics infrastructure border can access the e-health cloud's data and services. This interface connection is usually a specific hardware device that establishes secure network connections to the e-health data centers via a Virtual Private Network (VPN). Many countries create standards and specifications for national e-health infrastructures that incorporate technical means for security and privacy because of rising privacy concerns.

Existing e-health security ideas, on the other hand, focus on data access control (for example, smartcard-based access control to web-based PHRs and EHRs), data transfer security (encryption for secrecy, digital signatures for integrity and authenticity), and network security (firewalls, VPNs). The latter focuses on the separation of separate networks, such as health insurance administrative networks from EHR servers and other applications.

However, little consideration is given to what happens once data access is granted, namely, how data is processed and stored on end-user client systems. Viruses and Trojan Horse programs can corrupt data and listen in on patient records, infringing on both legal and personal privacy rights.

3.4. Management of E-Health Infrastructure

The security of health data is threatened by a number of risks that affect the entire infrastructure of an e-health cloud on a larger scale. The e-health cloud processes patients' medical and administrative data at various locations, and using smartcards and access control mechanisms alone does not provide the necessary protection.

3.4.1. Cryptographic Key Management

The use of encryption for additional security and privacy necessitates the management of cryptographic keys, and users must be issued personalized smartcards, the patient controls the cryptographic keys, this means that no other entity is permitted to get around the patient's access rights and privacy decisions about their EHR data.

However, the card issuer the EHR server providers should keep a copy of the cryptographic keys in a backup location for the purpose of issuing backup smartcards in the event of theft or loss.

To ensure the legitimacy of key holders, certificates must be managed, just like in any public key infrastructure. This includes updating revocation lists and issuing and disseminating certificates.

3.4.2. Hardware/Software Components Management

In addition to the cryptographic infrastructure, additional elements also need to be handled and maintained. This covers the hardware and software elements

employed by EHR servers, billing servers, and healthcare providers' computing equipment. Smartcard readers and connectors to secured networks are examples of security-critical components that need to be properly certified and tested. A secure distribution system is necessary for software component installation and updating.

On one hand, it must be possible to allow adjustments in software configuration brought on by legal updates, on the other hand, unauthorized and malicious changes (such as those brought on by malware attacks) must be detectable in order to stop further use or to remove the affected components from the e-health infrastructure.

3.5. Privacy Domains for E-Health

We propose a secure e-health infrastructure based on Trusted Virtual Domains (TVDs) to ensure fundamental security and privacy properties. Initially we will discuss privacy domains for healthcare systems. Next, we will talk about our realization, which is built on a security kernel and TVDs.

As a technical solution to facilitate the implementation of privacy and data protection regulations, we suggest creating privacy domains for the medical data of the patients: Applications' execution environments must be able to be divided into distinct domains that are isolated from one another by systems (like a client PC).

A privacy domain is used to store data, and its infrastructure makes sure that only authorized parties are allowed to join. Additionally, the domain infrastructure and security architecture both work to prevent data leaking from the domain. The privacy domains used in our e-health cloud concept are shown in Figure 3.

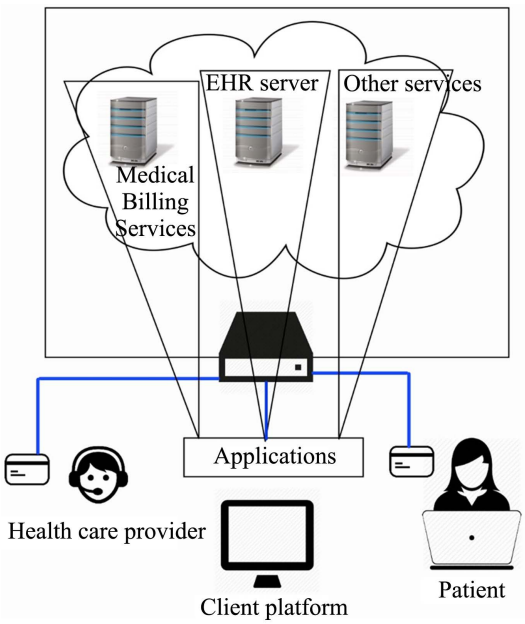


Figure 3. Privacy domains in the e-health.

The implementation of any new infrastructure in practice requires the integration of legacy systems as a crucial step. It is possible to utilize current applications that are already running on a legacy operating system inside a privacy domain with the support of our privacy domain idea. Furthermore, the privacy domain architecture can be connected to older systems and data can be imported into the domain using gateways and filters.

4. Trusted Virtual Domains Implemmentation

4.1. Client Platform Security Implementation

For each domain, Figure 4 shows the organization of a TVD, which includes a client platform and a TVD master (a server that manages the TVD infrastructure). On the client platform, a security kernel runs on top of the hardware, allowing applications and regular operating systems to execute in isolated virtual machines. Furthermore, for each TVD, there is a TVD proxy that manages the TVD on the client and configures the safety kernel in accordance with the TVD policy. Input and output are handled using a secure graphical interface (secure GUI), which ensures that users can always tell which compartment they're dealing with, the secure GUI prevents other compartments from reading user input if they aren't authorized.

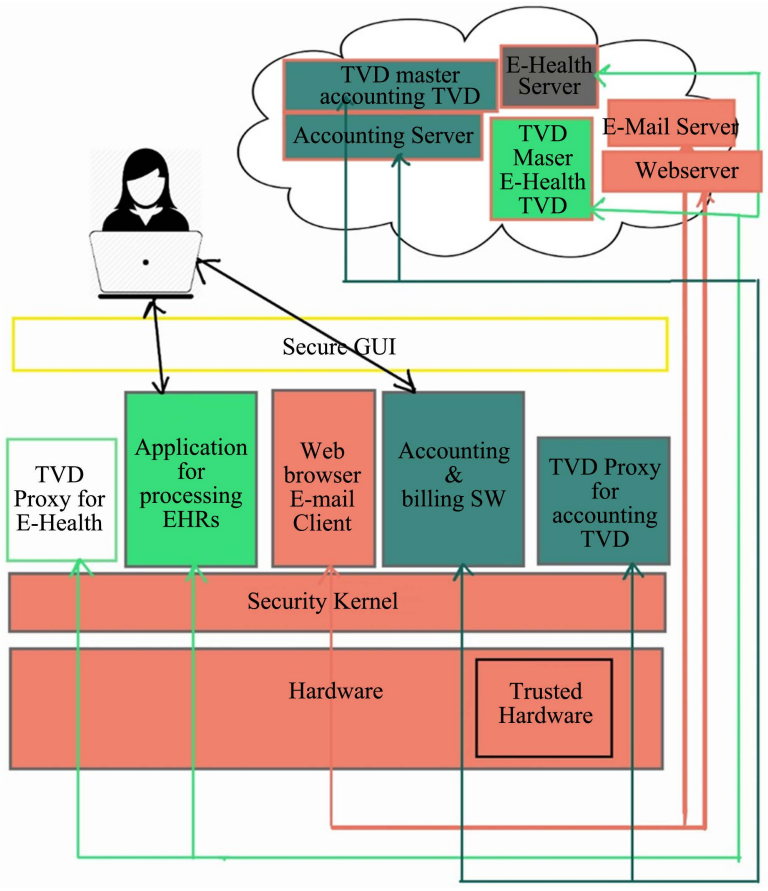


Figure 4. TVDs with client platform, servers and TVD masters.

Furthermore, the client platform includes a trusted hardware component that may be used to verify the software integrity on the client (in particular, the safety kernel). The Trusted Platform Module (TPM) [7] is the most widely used trusted hardware component. Currently, it's commonly implemented as a separate chip on the computer's mainboard. TPMs are found in many computers (including the majority of business laptops sold today), however they are rarely publicized.

TPMs offer a variety of security and cryptography features, such as public key encryption, digital signatures, secure key storage, and non-volatile memory, among others.

Three capabilities are particularly crucial for TVDs:

*Authenticated boot [8]: When the system boots up, the platform computes cryptographic hash values (which are commonly referred to as a "secure fingerprint" of the loaded and executed components) (e.g., firmware, boot loader, OS kernel). These values are safely kept in the TPM's platform configuration registers, which are special-purpose registers (PCRs).

*Trusted storage [9]: The use of TPM-generated cryptographic keys is frequently limited to specified PCR values. This implies that these keys can only be utilized once the appropriate system has been launched.

*Attestation [10] [11]: To sign the current PCR values, the TPM can employ special-purpose cryptographic keys known as attestation identity keys. This authentication technique is frequently used in cryptographic protocols to report the contents of the PCRs and hence the "fingerprint" of the system to a third party.

When a client wants to join a TVD, the TVD master first verifies the integrity of the client's security kernel using the trusted hardware component's security features. To accomplish this, an interactive protocol is run between the security kernel, trusted hardware, and the TVD master to verify that only clients who comply with the TVD policy are permitted into the TVD (for details see [5] [12]). The TVD master then delivers the TVD policy and appropriate cryptographic keys to the TVD proxy, which is then started on the client. The proxy configures the security kernel (for example, a virtual network is built for VMs that join the TVD) and controls which VMs are allowed to join the TVD.

A secure channel is provided for communication between the connector and the client platform, but it is not enforced in most electronic health systems. The transmission is not encrypted by default, and the devices are not authenticated. In contrast, with our suggested architecture and use of TVD technology, all client platforms and software components running on them are authenticated using trusted computing technology's attestation feature. Only components and platforms that have successfully authenticated will be able to create a trusted channel to the central e-health infrastructure and access data from the associated privacy domain.

4.2. TVD Implementations

Our project's main objectives include separating medical information from other

data, such as billing and accounting information, and integrating e-health cards into the system.

In the following, we describe the basic technology of our proposal. Our realization is based on Trusted Virtual Domains.

A security kernel that supports virtualization and Trusted Computing is required to implement a TVD. We've built TVDs as research prototypes, and a Common Criteria protection profile 6 for a security kernel with Trusted Computing capability has been certified. Operating systems that have been assessed and certified in accordance with this protective profile would be a good starting point for industry-grade TVDs.

Because of the TPM's availability, we integrated Trusted Computing functionality. For the TVD master, we employ the TPM's authenticated boot process and attestation functionality to validate client platform integrity and preserve cryptographic keys.

In conclusion, TVDs have been proved to be useful in a variety of situations. Various implementations based on different security kernels exist, supporting all kinds of operating systems, even though some are research prototypes rather than production-ready systems.

4.3. Protection of External Storage

The secure integration and use of external storage in TVDs, such as USB disks, pen drives, or cloud storage like Amazon S3, increases users' flexibility in their work, but also necessitates careful security architecture design. Mobile storage devices are commonly used to store copies of documents that the user (for example, a doctor) can take home or to another office, as well as data that needs to be processed on other systems. USB disks, in particular, are frequently utilized offline, that is, when plugged into any platform that is not linked to the domain network (For example, a laptop on a train or an airline). Backups could be stored in the cloud, which is a very convenient and very inexpensive option:

Regular backups can be conveniently stored using external cloud services that provide the user with potentially unlimited storage capacity. While local storage devices or file servers provide quick access to data and are available regardless of a working Internet connection, regular backups can be conveniently stored using external cloud services that provide the user with potentially unlimited storage capacity. Only the amount of storage currently in use must be paid, and the amount of storage accessible increases as needed. In the same way, file servers that aren't part of a TVD can be used as external storage within one. Storage devices and services should be considered as passive components that do not provide security properties.

As a result, the computer to which the storage is linked is solely responsible for enforcing security regulations. As long as storage is used inside the TVD borders, we can assume the policy is correctly enforced. When external storage is used outside of its domain, such as when it is connected to another computer, this assumption is no longer valid.

We enhanced the TVD model by including the advantages of mobile storage devices, allowing for the transparent binding of devices to a specific TVD so that only platforms belonging to the same TVD may access the data. Other external storage, such as cloud Computing storage, can be incorporated into TVDs in the same way. The storage service, like a mobile storage device, provides a container for data in terms of the TVD architecture.

4.4. Considerations for External Storage Security

Adding external storage to a system can introduce additional security concerns. Physical possession of external devices may be easier for attackers than physical possession of an internal hard disk. Outside attackers who are not part of the TVD infrastructure, on the other hand, are unable to access the data due to the visible encryption of all external storage by the TVD infrastructure.

Viruses or Trojan horse programs could also be stored on USB sticks inserted into a computer. This is a serious threat on commodity operating systems like Windows because programs from USB storage are automatically executed when the device is connected, and even if automatic execution of programs from USB storage is disabled, users can manually start malware-infected programs from USB sticks.

Because only data from a storage container belonging to the same TVD as a particular compartment will be connected to that compartment by the security kernel, we can prevent malware from accessing the TVD via USB sticks. The data in the compartment of the TVD is encrypted and decrypted transparently, and it cannot be viewed from outside the TVD. External storage, such as a USB disk, is treated as a passive storage device by the security kernel. There will be no automated execution of programs from it, neither in the security kernel nor in any TVD.

Malware installed on USB sticks in one TVD compartment cannot be stopped from being read or executed in another TVD compartment (which might be on a different computer system). The TVD architecture only separates and protects the TVD from external threats, not from dangerous software already installed on the system. The TVD infrastructure, on the other hand, should help to ensure that only secure systems can join the TVD using processes such as platform integrity verification before joining.

5. Results and Discussion

The rapid shift to cloud computing during the corona virus pandemic introduces external storage to the healthcare system, which would lead to evident security risks, and it would be much easier for hackers to gain possession of external devices than to obtain an internal hard disk.

However, due to the transparent encryption presented for all external storage by the TVD infrastructure, hackers who are not part of the TVD cannot access the data saved on the external devices.

With the TVD architecture, we will stop malware from entering the TVD via USB sticks, as a result of solely knowledge from a storage instrumentation happiness to an equivalent TVD as a given compartment are going to be connected to it compartment by the security kernel. Coding and secret writing happens transparently for the compartment of the TVD, and therefore the data cannot be accessed from outside the TVD. For the security kernel, secondary storage similar to a USB disk is simply a passive storage device. No programs will be dead from it automatically, neither within the security kernel, nor in any TVD.

Malware that is stored on USB sticks from inside the TVD cannot be prevented from being read or executed in another compartment of identical TVD (which may be on a different computer system). The TVD infrastructure itself solely isolates and protects the TVD from adversaries from the outside, not from malicious software that is already part of the TVD. However, the TVD infrastructure should help to confirm that solely secure systems would become members of the TVD by mechanisms such as the integrity verification of all platforms before joining.

6. Conclusions

Since cloud hosting was adopted without proper investigation or review due to the Coronavirus crisis, which raised challenges concerning security and privacy aspects that could lead to long-term risks and vulnerabilities in the system, ensuring security and privacy is a major factor in the cloud computing environment.

In this paper, we examined security and privacy issues in E-health systems, and then we proposed a secure e-health infrastructure based on Trusted Virtual Domains (TVDs) to ensure fundamental security and privacy properties.

We discussed the importance of client platform security, which is often overlooked. We demonstrated how privacy domains can be utilized to improve the security of E-health systems beyond (current) network security solutions and into a more comprehensive infrastructure that includes the client.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] World Health Organization (2004) A Glossary of Terms for Community Health Care and Services for Older Persons. Who Centre for Health Development Ageing and Health Technical Report, Vol. 5, World Health Organization, Japan.

[2] Takabi, H. and Joshi, J.B.D. (2012) Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment. 2012 45*th Hawaii International Conference on System Sciences*, Maui, HI, USA, 4-07 January 2012, 5500-5508. https://doi.org/10.1109/HICSS.2012.475

[3] Leavitt, N. (2009) Is Cloud Computing Really Ready for Prime Time? *Computer*, **42**, 15-20. https://doi.org/10.1109/MC.2009.20

[4] AbuKhousa, E., Mohamed, N. and Al-Jaroodi, J. (2012) E-Health Cloud: Opportunities and Challenges. *Future Internet*, **4**, 621-645. https://doi.org/10.3390/fi4030621

[5] Cote, R.A. (1986) Architecture of SNOMED: Its Contribution to Medical Language Processing. *Proceedings of the Annual Symposium on Computer Applied Medical Care*, Washington, DC, USA, 25-26 October 1986, 74-80.

[6] Health Level Seven International (HL7). http://www.hl7.org

[7] Şen, A.F. (2021) Watchdog Journalism during the Coronavirus Crisis in Turkey. *Advances in Applied Sociology*, **11**, 500-512. https://doi.org/10.4236/aasoci.2021.1110044

[8] International Organization for Standardization (ISO) (2021) Technical Committee 215, Health Informatics. http://www.iso.org/iso/iso_technical_committee?commid=54960

[9] Bussani, A., Griffin, J.L., Jansenm, B., Julisch, K., Karjoth, G., Maruyama, H., Nakamura, M., Perez, R., Schunter, M., Tanner, A., van Doorn, L., Van Herreweghen, E.A., Waidner, M. and Yoshihama, S. (2005) IBM Research Report. Trusted Virtual Domains: Secure Foundations for Business and IT Services. https://www.researchgate.net/publication/228824533_Trusted_Virtual_Domains_Secure_foundations_for_business_and_IT_services

[10] Purbo, O.W. (2020) Internet-Offline Solution: Detail Description and Benchmarking. *TELKOMNIKA*, **18**, 1809-1818. https://doi.org/10.12928/telkomnika.v18i4.13309

[11] Pramukantoro, E.S., Luckies, M. and Bakhtiar, F.A. (2019) Bridging IoT infrastructure and Cloud Application Using Cellular-Based Internet Gateway Device. *TELKOMNIKA*, **17**, 1439-1446. https://doi.org/10.12928/telkomnika.v17i3.12229

[12] Mehraeen, E., Ghazisaeedi, M., Farzi, J. and Mirshekari, S. (2017) Security Challenges in Healthcare Cloud Computing: A Systematic Review. *Global Journal of Health Science*, **9**, 157-166. https://doi.org/10.5539/gjhs.v9n3p157