Journal of Computer Science 10 (2): 240-250, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.240.250 Published Online 10 (2) 2014 (http://www.thescipub.com/jcs.toc)

TRUSTED CLOUD COMPUTING FRAMEWORK FOR HEALTHCARE SECTOR

[1]Mervat Adib Bamiah, [1]Sarfraz Nawaz Brohi, [1]Suriayati Chuprat and [2]Jamalul-lail Ab Manan

[1]Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
[2]Strategic Advanced Research Cluster, MIMOS Berhad, Kuala Lumpur, Malaysia

Received 2013-10-04, Revised 2013-10-22; Accepted 2013-11-13

ABSTRACT

Cloud computing is rapidly evolving due to its efficient characteristics such as cost-effectiveness, availability and elasticity. Healthcare organizations and consumers lose control when they outsource their sensitive data and computing resources to a third party Cloud Service Provider (CSP), which may raise security and privacy concerns related to data loss and misuse appealing threats. Lack of consumers' knowledge about their data storage location may lead to violating rules and regulations of Health Insurance Portability and Accountability Act (HIPAA) that can cost them huge penalty. Fear of data breach by internal or external hackers may decrease consumers' trust in adopting cloud computing and benefiting from its promising features. We designed a HealthcareTrusted Cloud Computing (HTCC) framework that maintains security, privacy and considers HIPAA regulations. HTCC framework deploys Trusted Computing Group (TCG) technologies such as Trusted Platform Module (TPM), Trusted Software Stack (TSS), virtual Trusted Platform Module (vTPM), Trusted Network Connect (TNC) and Self Encrypting Drives (SEDs). We emphasize on using strong multi-factor authentication access control mechanisms and strict security controls, as well as encryption for data at storage, in-transit and while process. We contributed in customizing a cloud Service Level Agreement (SLA) by considering healthcare requirements. HTCC was evaluated by comparing with previous researchers' work and conducting survey from experts. Results were satisfactory and showed acceptance of the framework. We aim that our proposed framework will assist in optimizing trust on cloud computing to be adopted in healthcare sector.

Keywords: Cloud Computing, HIPAA, Security, Privacy, Trust

1. INTRODUCTION

Healthcare users are now demanding higher level of IT interaction such as instant online access to information, products and services through their mobile devices. Healthcare organizations are struggling to manage the complexity, cost and effort when upgrading their IT infrastructure, purchasing new hardware and software, as well as licencing and maintenance of their existing devices and applications. Cloud computing offers significant benefits for healthcare sector such as scalability, resiliency, adaptability, connectivity and virtualization and optimized performance. Cloud has high potential to maximize the efficiency and quality of healthcare services through its various service delivery and deployment models (Wu *et al*., 2012), (Zhang and Liu, 2010). Despite the advantages of cloud computing for healthcare, still there are several obstacles related to security, privacy and trust that restricts its full adoption (Servos, 2012), (Mori, 2011), (Khatua *et al*., 2011). Consumers lose control when they outsource their data and computing resources to cloud with no knowledge of data storage location and accessing person from the CSP side which may alternatively lead to HIPAA violation (Popovic and Hocenski, 2010). Moreover, multi-tenancy feature of cloud can raise the probability of one healthcare organization's data can be stored at the same server as their competitors. This requires strong isolation techniques beside robust authentication and authorization methods to preserve privacy and prevent any illegal access to their data (Takahashi *et al*., 2012).

Corresponding Author: Mervat Adib Bamiah, Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

2. RELATED WORK

Several researches have been proposed to deploy cloud computing in healthcare sector. Some of these proposals did not implement any security mechanisms such as (Vazhenin, 2012), (Zhou *et al*., 2011), (Ratnam and Dominic, 2012) which can open the way for internal and external threats and may cause severe damage to organizations reputation besides misuse of data. While, researchers such as (Narayan *et al*., 2010), (Narayanan and Gunes, 2011) implemented strong access controls but did not apply any trusted secure hardware mechanisms. Some researchers such as (Li *et al*., 2013), (Alshehri *et al*., 2012) provided only data encryption techniques to preserve privacy but their techniques was not adequate enough to secure cloud infrastructure.

Other researchers relied on trusted middleware to achieve integrity and confidentiality i.e., (Abbadi *et al*., 2011) but did not provide any security for physical cloud infrastructure. Lohr *et al*. (2010) proposed secure E-Health Cloud which provides a security architecture based on Trusted Virtual Domains (TVDs) for privacy as well as the usage of TPM for creating chain of trust. However, E-Health Cloud architecture did not provide data encryption or any security technique for middleware. After conducting in- depth literature review we found out that there are security and privacy issues that are not well covered by the current solutions. These issues will be considered in research framework design.

3. FRAMEWORK DESIGN

Healthcare sectors' trust can be achieved when they are confident that their data is secured, available and under their control with known data storage location (Fan, 2012), (Ko *et al*., 2011).

Cloud computing facilitates healthcare organizations and indeviduals three service delivery models in form Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) according to National Institute of Standards and Technology (NIST) (Mell and Grance, 2011).

Cloud infrastructure is composed of physical, virtual, applications and data resources that have to be secured against internal and external threats to protect them from unauthorized access to the servers, storage and Virtual Machines (VMs) (Metri and Sarote, 2011). By considering healthcare requirements, we propose secure by design layered architecture as shown in **Fig. 1.**

3.1. Physical Layer

Physical layer consists of servers, storage, network components and their interaction (Abbadi *et al*., 2011). Its resources are consolidated to serve the virtual layer. For securing this layer we designed Trusted Platform (TP) a computing platform that has trusted hardware and software components which are used to create a foundation of trust for software processes based on TCG specifications that includes its operation and storage rules (Basit, 2009). Physical layer security can be achieved by securing its components as follows:

3.1.1. Server Security

To secure cloud servers from unauthorized access and tampering, we use TPM a microcontroller hardware root of trust that is capable of secure key management, storage and reporting of platform configuration measurements. It allows the identification of users and devices which facilitate dual-level authentication for more optimized security (Berger, 2012). TPM ensures that the system is booted into a Trusted Operating System (TOS) which adheres to specified security policies and strong isolation to protect the system from being compromised after it has been booted and to prevent applications from tampering with each other.

TPM is installed inside each processing platform in the cloud. It facilitates remote attestation to certify the authenticity of hardware and software being run by a remote party (Celesti *et al*., 2011). TPM and its software TSS checks what is installed on each dsevice and verifies the device's health and proper performance. By using TPM capabilities such as authentication, encryption and attestation ensures that cloud servers are secured against tampering (Achemlal *et al*., 2011).

3.1.2. Network Security

Secure communication requires both the identity and state of the remote system to be identified and accepted on the same server (Harris and Hill, 2011). In HTCC, network is secured by TNC that detects malicious attack and acts by restricting access to a device or server. It enables Cloud Service Administrators (CSAs) to control the network access based on user identity and device health while observing the performance on the network and responding immediately to issues as they occur. TNC provides strong user authentication and blocks any unauthorized or malicious access. It can include various devices such as IP phones and printers as well as coordinating security devices across the organization.

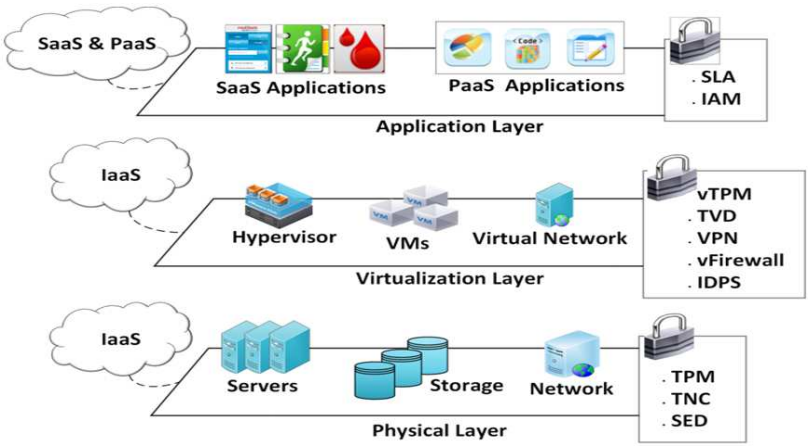

Fig. 1. Healthcare trusted cloud computing framework

By implementing TNC on CSP network, strong security will be added which will protect the communication channel and end points. This will facilitate healthcare sector to use smart devices such as mobiles and sensors for collecting and sharing information between healthcare professionals and patients via SaaS model (TCG, 2012).

3.1.3. Storage Security

CSPs must ensure that healthcare data are encrypted and stored in safe storage to maintain security and privacy. In HTCC, cloud storages are secured by SEDs full-disk encryption hardware that moves the processing overhead of decryption and encryption to the Central Processing Unit (CPU) providing encryption protection without impacting performance. SEDs have all data, applications and drivers encrypted internally, also key management is an integral part of the design. SEDs have unified, standards-based key management within the drive controller. Encryption algorithms are based on the NIST FIPS 197- AES standards including AES-128 and AES-256 that secures against side channel leak vulnerabilities and associated exploits. For providing data availability to healthcare, backup servers are also secured by TPM and SEDs (TCG, 2013).

3.2.Virtual Layer

In HTCC, virtual layer represents the virtual resources that host consumer's applications. It consists of VMs, hypervisor, virtual network and virtual storage (Abbadi *et al*., 2011). In order to secure this layer we utilized vTPM which simulates the interface and functionality of TPM and enables it's related TSS and other applications functionality for VMs. The integration of TCG technologies into virtualized cloud environments enables the hardware-based protection of critical data and the detection of malicious software. For mitigating the security concerns of virtualization techniques, we base our solution on NIST SP 800-125 guidelines (Scarfone *et al*., 2011) that recommends securing all elements of full virtualization.

Optional secure virtualization techniques also is provided in HTCC such as Trusted Virtual Domains (TVDs) over an encrypted Virtual Private Network (VPN) that provides an IPSec point-to-point secure encrypted communication channel between the consumers network and cloud datacenter and is decrypted upon receipt at either end points (Jones, 2012).

VPN is established in cloud environment for the consumer account as shown in **Fig. 2**. A single private Virtual Local Area Networks (VLAN) is allocated for the account that provides an additional layer of network isolation for VMs that are assigned to it (Vernier and Jones, 2011). The VMs are not visible from the Internet but can only be accessed either via the VPN or via another VM on the VLAN.

3.2.1. Virtual Machine Security

In HTCC, TPM provides hardware-based verification of hypervisor and VM integrity. Every vTPM is associated with its VM and is provisioned with IP network addresses that are accessible through the Internet. This will allow the applications in the VM to use the vTPM for secure storage and reporting platform integrity. VMs and cloud servers use the same OSs and web applications as physical servers.

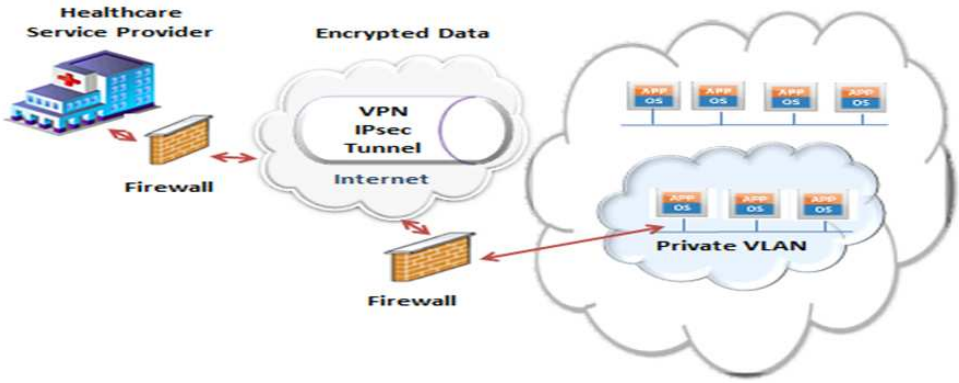

Fig. 2. Isolating healthcare data via VPN

By deploying vTPM on VMs shields newly discovered vulnerabilities in their applications and OSs to protect against VMs exploits (Buecker *et al*., 2013). We implement stringent security controls such Intrusion Detection and Prevention Systems (IDPS), next generation firewalls, integrity monitoring, log inspection, malware protection, encryption and data control on VMs to increase the safety, protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environments (Mell and Scarfone, 2012).

3.2.2. Hypervisor Security

Hypervisor manages and control the VMs, if attackers managed to take control over the hypervisor, they will gain full control over VMs and consumers data within the hypervisor's territory. Virtual infrastructure relies on the security of the virtualization management system that controls the hypervisor and allows the VMs administrator to start and create new VMs, besides performing other actions which may lead to insider threats that can access VMs and exploit the data.

We implemented resilient security controls on the hypervisor by restricting the accessibility only to authorized administrators with least privileges. More over, we deployed virtual Firewall (vFirewall), anti-viruses and virtualization aware malware protection that leverages hypervisor introspection APIs to secure both active and inactive VMs by performing full system scans from separate scanning VMs and defending against viruses, spyware, Trojans. In addition to incorporating clean up capabilities to remove malicious code and repair any system damage caused by the malware (Micro, 2010).

3.3. Application Layer

This layer consists of cloud consumer's applications, which are hosted using resources in the virtual layer (Abbadi *et al*., 2011). The CSP must ensure that these applications are free from bugs and cannot be used as a tool to launch attacks. Securing the application layer is about ensuring that healthcare security and privacy requirements are maintained by the environment surrounding the application which includes robust security controls described as follows: Applications are free from bugs and cannot be used as a tool to launch attacks. Securing the application layer is about ensuring that healthcare security and privacy requirements are maintained by the environment surrounding the application which includes robust security controls described as follows:

- Implementing strong security password technique that will make it hard for the attacker to access the consumer's account as discussed in 3.3.1
- Securing the access to the cloud application with robust least privilege access control methods as discussed in 3.3.2
- Encrypting and securing consumer's data during its life cycle besides securing it in safe storage by using TCG-SED technology as discussed in 3.3.3
- Securing the communication channel between the cloud server and the consumer by using SSL/TLS over HTTPS that ensures all communications are encrypted and protected from interception. HTTPS guaranties a lightweight security for interfacing with several numbers of medical software and EHRs

- Deploying security controls such as, firewall, antivirus protection and the latest OSs and Web browser updates
- Securing the cloud physical infrastructure with TPM and TNC as discussed in 3.1
- Securing the cloud virtual infrastructure with vTPM and related security controls as discussed in 3.2
- Guaranteeing disaster recovery plan and secure encrypted data backup under the regulations and compliance of the consumer's location
- Ensuring that the applications are running and data is stored at pre-agreed geographical location
- Ensuring efficient SLA that guarantees security, privacy, availability, scalability, performance and compliance with HIPAA
- Ensuring that the applications are safe and accurate as to not to have any vulnerability to attack
- Ensuring that applications are udated and patched regulary to protect from zero-day attacks

3.3.1. Username and Password Policy

Weak Passwords raise vital safety issues for healthcare organizations and patients. For-example, weak passwords are vulnerable to hackers who can access patients' devices to increase or decrease their drug dosage. We have designed strong security control policies for using, storing and retrieving username and password described as follows:

- Consumer must enter valid username that can be email or name
- Consumer must enter a valid password that should be hard to detect. It has to be alphanumeric which includes capital and small letters, as well as numbers and special symbols with minimum amount of eight characteristics (e.g., Example12#)
- Number of attempts trying to input username and password is restricted to three times else block and send notification by email and mobile phone for verification

Passwords must be encrypted and stored in form of transparent color and hashes to protect it from malicious access as shown in **Table 1**.

Table 1. Cloud user

Id.	Username	Password
01	example@yahoo.com	#########

Transparent, Encrypted

3.3.2. Identity and Access Management

There are various forms of Identity and Access Management (IAM) scenarios in HTCC framework to ensure access controls and authenticated user privileges from consumer's side and from CSP's side. This is vital to initiate trust and to protect from malicious access threats.

In HTCC we emphasis on utilizing industry standard IAM protocols such as Service Provisioning Markup Language (SPML) that promotes automation of user identity provisioning and Security Assertion Markup Language (SAML) which provides federated Single Sign-On (SSO) which allows multiple systems for distributed access control while maintaining the confidentiality of user credentials without needing to remember a load of different passwords (Krishnan and Chatterjee, 2012).

We propose multi-factor authentication access control technique since strong user authentication and authorization have not yet been extended into the cloud (Choudhury *et al*., 2011). As for authorization privileges, when consumers subscribe to cloud services, they send their data and associated access control policies (if any) that grants CSP data access rights, such as read, write and copy. **Fig. 3** illustrates HTCC authentication scenarios of three users as follows.

3.1.1.1. Cloud Service Provider Authentication

When CSA reach his office or datacenter he cannot access unless he performs and pass biometric access control such as (Fingerprint, Iris Scan, Voice Print):

- If he passes biometric scanning successfully then CSA has to enter access card for identity verification and time stamping

For robust security we assume that CSP place is secured with CCTV camera and security guards:

- Next CSA use his mobile device to sign-in with his username and password according to HTCC policy
- If CSA fails to input valid username or password, then he is granted three opportunities to correct it, else enter forgot username/password and a reset instruction will be sent to his email
- If CSA passes entering his username and password then he must answer the challenge question. If he pass answering the question then he needs to authinticate through mobile One Time Pin (OTP)
- If he fails to enter correct OTP then system will deny access, block user and report incident. It will also report IP address for auditing purposes
- If CSA successfully entered the OTP code then he is granted access to the system.

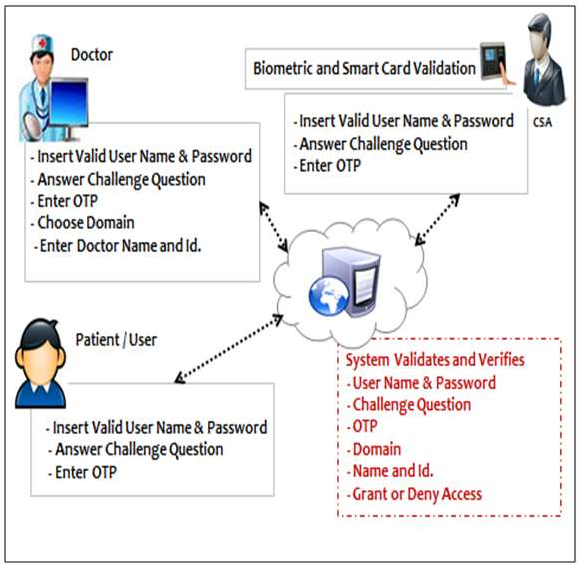

Fig. 3. HTCC people authentication

However, for robust security and to illuminate internal threat, CSA has to choose the right domain for authorization access policy and enters his real name and identification or employee number:

- If his name and identification is correct then he will be granted access to the system
- If he fail then deny access and document the logging attempt for later analysis and auditing purposes

3.1.1.2. Doctor Authentication

Another scenario is from healthcare organization, a working doctor needs to access a patient record. He opens the HTCC-SaaS web portal and signs-in by providing his username and password which complies with HTCC policy terms for more robust security. The system will verify and validate the username and password. If doctor fails to put valid username and password, then he will be granted three chances to correct it, else he has to click on forgot username and/or password and a reset instruction will be sent to his email, in which he will be verified by a challenge question and OTP on his mobile phone or by email. If doctor pass the process of entering username and password successfully then he must answer a challenge question. If answer is correct then an OTP will be sent to his mobile phone for further verification. If successful code input then proceed to access the requested domain and enter doctor id and name. After that doctor has chosen the domain, system will authorize him the access privilege according to the organization's policy. If doctor does not meet the domain policy, then he is denied access, else he can access the patient's record.

3.1.1.3. Patient /User Authentication

A patient is registering to the cloud, accessing, using cloud applications and storing his data from various devices (sensors attached to his body, mobile) and from different places (home, office, car). Patient opens SaaS web portal and signs-in by providing his username and password which is according to our design terms for more robust security. The system will verify and validate the username and password if not accurate, patient will be given three chances to enter the right one else he click on forgot username and/or password and a reset instruction will be sent to his email for new password generated which will be verified by challenge question and OTP on doctor mobile phone, if successfully pass then grant access,else deny access and report logging and IP in the system for mapping the failed registration and keeping records for auditing purpose.

3.3.3. Securing HTCC Data Life Cycle

In HTCC, data is encrypted while in transfer, use, share, store and backup as well as in archive phase to protect healthcare data from breach, misuse or malicious access. We contributed in extending the work of (CSA, 2011) by adding backup in data life cycle as shown in **Fig. 4**. Data backup is used to restore data if it is lost, corrupted or destroyed.

Data backups guaranties availability and continuity of consumers' data within high-speed copy and restores to minimize the impact of failures. While data archive is performed to effectively manage data for retention, long-term access and retrieval (Livens, 2013).

3.4. Middleware Security

In HTCC, middleware refers to a set of software that executes between OS and applications that facilitate unified interface, scalable and transparent abilities forinfrastructure as well as management services (Abbadi, 2011). Middleware will be secured using the same security techniques as the application layer stated in 3.3.

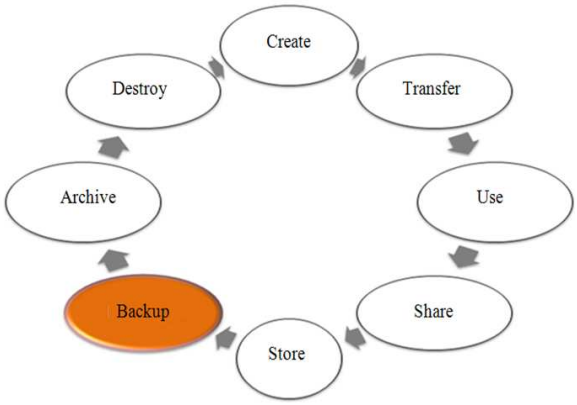

Fig. 4. HTCC cloud data life cycle

4. COMPLIANCE WITH HIPAA

HIPAA requires maintaining the privacy of Personal Health Information (PHI) to protect individual, public health and wellbeing (HHS, 2013). In order for HTCC to comply with HIPAA privacy and security rules, it conducted the following procedures:

- Documentation and periodic refining of policies and procedures to comply with regulation
- In emergency access to patients information has to be activated using "break-glass" access procedures. However, this access is logged and documented for auditing purposes and only accessed by authorized people identified for these situations
- Data is encrypted at rest, in-process and transmit for privacy and protect it from leakage and misuse
- Providing physical and technical safe guards in terms of multiple layers of protection to assist in keeping healthcare data secure against breach and attacks
- Limiting and monitoring access to consumers data as well as maintaining logs of activity
- Implementing robust access control multi-factor authentication mechanism
- Deploying TCG technologies, firewall, anti-virus, malware and IDPS systems
- Employing industry best practices for installation, configuration and patch installation of managed servers and associated devices
- Transmitting healthcare data via SSL/TLS over HTTPS that ensures that all communications are encrypted and protected from interception
- Providing availability and data recovery through backups that are stated in SLA

5. HTCC SERVICE LEVEL AGREEMENT

Regarding to Hon *et al*. (2012) there is no specific tailored SLA and privacy audits for healthcare sector which may raise the risk of non-compliance when storing and processing medical and patient information in the cloud. Our main contribution is proposing an addition context to SLA according to healthcare requirements such as data location, level of security and isolation needed for virtualized and/or physical resource. Also data deleting, retrieving and auditing processes, besides data backups and exit plan to ensure smooth transition of accurate complete data and proof of deletion of all data after transition is done. SLA should protect the right of consumers from each perspective to assure them that their privacy is preserved and their data is securely encrypted and governed in all its life cycle, also defining the e-discovery policies and disaster recovery plans to maintain data availability for best business practices. Penalties for violating the SLA from both sides have to be specified as well as termination terms and conditions.

In our design CSP must provide prove of regulatory and compliance. Since healthcare sector maintain critical data and applications. CSP must be transparent and proactive in notifying consumers when there is a breach in SLA terms. This includes infrastructure issues like outages and performance problems and security incidents. CSP must keep his certificates up to date for maintaining his reliability and reputation (Rodrigues, 2012), (Myerson, 2013).

Security and trust requirements in the cloud environment such as data availability, data encryption, data integrity checks, detailed access log, personnel background checks, data failure and disaster management, accurate working security policy, should be strictly included in the SLA and to be met during the period of a contract as requirements for some countries. Moreover, intellectual property must be clearly defined and protected in the SLA that the CSP will not use the consumers' data for his own purposes (Lehman and Vajpayee, 2011), (Schnjakin *et al*., 2010).

6. EVALUATION AND RESULTS

HTCC framework was evaluated by conducting a survey from experts in information security for cloud computing and healthcare as shown in **Fig. 5.** 75% of experts agreed on the usage of TPM, TNC and SEDs for securing the physical layer.

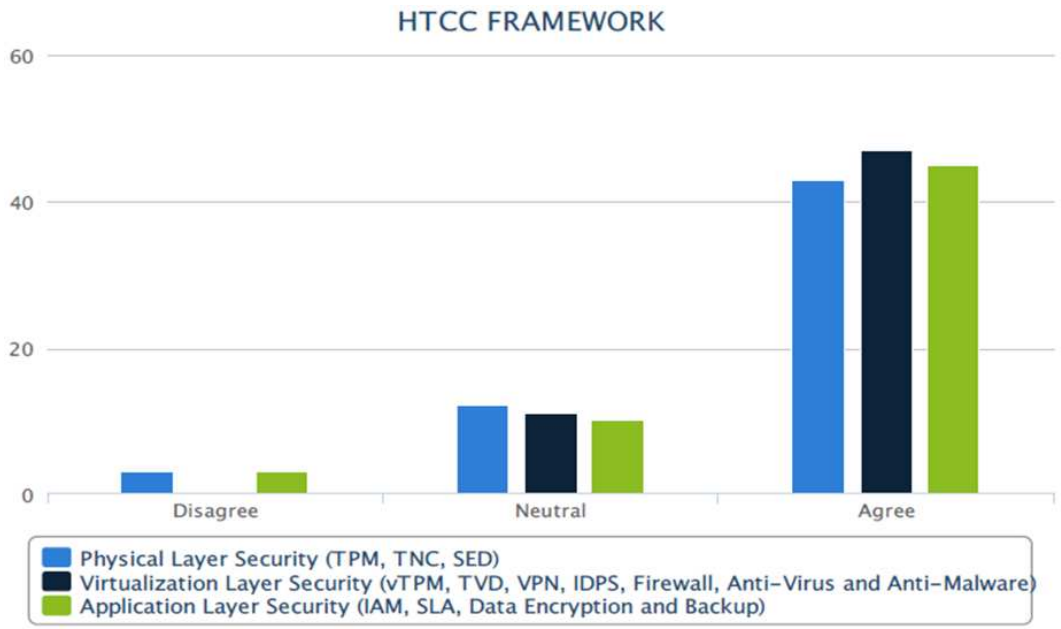

Fig. 5. HTCC framework security survey

While, 81% of respondents have agreed on the usage of security controls such as firewall, Anti-Malware, Anti-Virus and IDPS and vTPM for securing the virtualization layer. Moreover, 78% agreed on the usage of IAM that involves strong password and username policy beside encrypting data and backup for securing application layer. Overall rsults shows majority acceptance of HTCC security mechanisms which can optimize healthcare sector trust to deploy cloud computing.

7. DISCUSSION

After comparison with related work and conducting the survey we found out that our framework is trusted to be used in Health sector. In HTCC we proposed the following contributions that aim to fulfill the gaps of previous researcher's solutions such as:

- Contribution 1: Proposing a trust definition based on (Fan, 2012), (Ko *et al*., 2011) which states that trust can be achieved when consumers are confident that their data and computing resources are safe, available and under their control at known location under appropriate SLA which preserves their rights for auditability and the required level of security and privacy
- Contribution 2: TCG technologies was deployed for optimized security, privacy, interoperability and enhanced performance
- Contribution 3: An addition context to SLA was proposed according to Healthcare requirements
- Contribution 4: HTCC complies with HIPAA data security and privacy requirements
- Contribution 5: Separating data back up as an important stage that must be included for securing the data availability and disaster recovery. Also encrypting data by default during its life cycle
- Contribution 6: Adding storing policy for password.
- Contribution 7: Offering multi-factor authentication with least privileges for robust access controls

8. CONCLUSION AND FUTURE DIRECTIONS

We have critically analyzed the current implementation of cloud computing in healthcare. We found out that there is no current solution that secures whole cloud infrastructure and comply with healthcare rules and regulations. Also there was no SLA that is specifically customized for healthcare requirements. We have designed a trusted cloud computing framework that covers physical, virtualization and

application layers security, as well as access control mechanisms and data privacy considering HIPAA, in addition to providing a customized SLA for healthcare. Our aim is to provide security, privacy and availability for consumers. Due to the limitation of resources we did not implement our design. Future direction of this research focuses on simulating and implementing HTCC in healthcare sector.

9. REFERENCES

Abbadi, I., M. Deng, M. Nalin, A. Martina and I. Baroni *et al*., 2011. Trustworthy middleware services in the cloud. Proceedings of the 3rd International Workshop on Cloud Data Management, Oct. 24-28, ACM, New York, USA, pp: 33-40. DOI: 10.1145/2064085.2064094

Abbadi, I., 2011. Middleware services at cloud application layer. In: Advances in Computing and Communications, Abraham, A., J.L. Mauri, J. Buford, J. Suzuki, S.M. Thampi (Eds.,), Springer-Verlag, Berlin, ISBN-10: 3642227252, pp: 557-571.

Achemlal, M., S. Gharout and C. Gaber, 2011. Trusted platform module as an enabler for security in cloud computing. Proceedings of the Conference on Network and Information Systems Security, May 18-21, IEEE Xplore Press, La Rochelle, pp: 1-6. DOI: 10.1109/SAR-SSI.2011.5931361

Alshehri, S., S. Radziszowski and R. Raj, 2012. Designing a secure cloud-based EHR system using ciphertext-policy attribute-based encryption. Accepted for the DMC2012.

Basit, A., 2009. Guide To trusted computing. approaches for attesting virtualized environments. MSc Thesis, Royal Institute of Technology, Sweden.

Hon, W., C. Millard and I. Walden, 2012. Negotiating cloud contracts: Looking at clouds from both sides now. Stanford Technol. Law Rev., 16: 80-125.

Berger, B., 2012. TPM delivers a hardware root of trust for IT security.

Buecker, A., F. Costa, R. Davidson, E. Matteotti and G. North *et al*., 2013. Managing Security and Compliance in Cloud or Virtualized Data Centers Using IBM PowerSC. International Technical Support Organization. IBM.Red Books. First Edition, ISBN-13:9780738437675, pp: 319.

Celesti, A., A. Salici, M. Villari and A. Puliafito *et al*., 2011. A remote attestation approach for a secure virtual machine migration in federated cloud environments. Proceedings of the First International Symposium on Network Cloud Computing and Applications, Nov. 21-23, IEEE Xplore Press, Toulouse, pp:99-106. DOI: 10.1109/NCCA.2011.23

Choudhury, A., P. Kumar, M. Sain and H. Lim *et al*., 2011. A strong user authentication framework for cloud computing. Proceedings of the IEEE Asia-Pacific Services Computing Conference, Dec. 12-15, IEEE Xplore Press, Jeju Island, pp: 110-115. DOI: 10.1109/APSCC.2011.14

CSA, 2011. Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. USA.

Fan, W., 2012. Building trust into cloud. Int. J. Cloud Comput. Service. Sci., 1, pp: 115-122. DOI: 10.11591/closer.v1i3.742

Harris, J. and R. Hill, 2011. Statictrust: A practical framework for trusted networked devices. Proceedings of the 44th Hawaii International Conference on System Sciences, Jan. 4-7, IEEE Xplore Press, Kauai, HI., pp: 1-10. DOI: 10.1109/HICSS.2011.384

HHS, 2013. Health information privacy. U.S. Department of Health and Human Services.

Jones, A., 2012. SmartCloud tip: Build multiple VPNs and VLANs VPN and VLAN features and capabilities in IBM SmartCloud Enterprise 2.0. IBM. DeveloperWorks.

Khatua, S., N. Mukherjee and N. Chaki, 2011. A new agent based security framework for collaborative cloud environment. Proceedings of the 7th Annual Workshop on Cyber Security and Information Intelligence Research, Oct. 12-14, ACM Press, New York, USA., pp: 1-4. DOI: 10.1145/2179298.2179385

Ko, R., P. Jagadpramana, M. Mowbray and S. Pearson *et al*., 2011. TrustCloud: A framework for accountability and trust in cloud computing. Proceedings of the Services IEEE World Congress on Services, Jul. 4-9, IEEE Xplore Press, Washington, DC., pp: 584-588. DOI: 10.1109/SERVICES.2011.91

Krishnan, D. and M. Chatterjee, 2012. Cloud security management suite-security as a service. Proceedings of the World Congress on Information and Communication Technologies, Oct. 30-Nov. 2, IEEE Xplore Press, Trivandrum, pp: 431-436. DOI: 10.1109/WICT.2012.6409116

Lehman, T. and S. Vajpayee, 2011. We've looked at clouds from both sides now. Proceedings of the Annual SRII Global Conference, Mar. 29-Apr. 2, IEEE Xplore Press, San Jose, CA., pp: 342-348. DOI: 10.1109/SRII.2011.46

Li, M., S. Yu, Y. Zheng, K. Ren and W. Lou, 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distributed Syst., 24: 131-143. DOI: 10.1109/TPDS.2012.97

Livens, J., 2013. 3 Key Differences Between Backup and Archive. Iron Mountain Incorporated.

Lohr, H., A. Sadeghi and M. Winandy, 2010. Securing the e-health cloud. Proceedings of the 1st ACM International Health Informatics Symposium, Nov. 11-12, ACM Press, New York, USA., pp: 220-229. DOI: 10.1145/1882992.1883024

Mell, P. and T. Grance, 2011. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Information Technology Laboratory.

Mell, P. and K. Scarfone, 2012. Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology (NIST).

Metri, P. and G. Sarote, 2011. Privacy issues and challenges in cloud computing. Int. J. Adv. Eng. Sci. Technol., 5: 1-6.

Micro, T., 2010. Cloud Computing Security, Server Security: Making Virtual Machines Cloud-Ready. White Paper.

Mori, P., 2011. Security requirements, specification and architecture for virtual infrastructures D7.1. CONTRAIL Integrated Project Open Computing Infrastructures for Elastic Services, Project no. 257438 co-funded by the European Commission within the Seventh Framework Programme Dissemination Level, pp: 1-82.

Myerson, J., 2013. Best practices to develop SLAs for cloud computing. Develop a standard way to create service level agreements that multiple partners can use. IBM Developer Works.

Narayan, S., M. Gagne and R. Safavi-Naini, 2010. Privacy preserving EHR system using attribute-based infrastructure. Proceedings of the ACM Workshop on Cloud Computing Security Workshop, (SW '10), ACM Press, New York, USA., pp: 47-52. DOI: 10.1145/1866835.1866845

Narayanan, H. and M. Gunes, 2011. Ensuring access control in cloud provisioned healthcare systems. Proceedings of the IEEE Consumer Communications and Networking Conference, Jan. 9-12, IEEE Xplore Press, Las Vegas, NV., pp: 247-251. DOI: 10.1109/CCNC.2011.5766466

Popovic, K. and Z. Hocenski, 2010. Cloud computing security issues and challenges. Proceedings of the 33rd International Convention MIPRO, May 24-28, IEEE Xplore Press, Opatija, Croatia, pp: 344-349.

Ratnam, K. and P. Dominic, 2012. Cloud services-enhancing the malaysian healthcare sector. Proceedigns of the International Conference on Computer and Information Science, Jun. 12-14, IEEE Xplore Press, Kuala Lumpeu, pp: 604-608. DOI: 10.1109/ICCISci.2012.6297101

Rodrigues, T., 2012. Anatomy of a cloud service SLA: Availability guarantees. TechRRepublic's.

Scarfone, K., M. Souppaya and P. Hoffman, 2011. Guide to Security for Full Virtualization. Recommendations of the National Institute of Standards and Technology.

Servos, D., 2012. A role and attribute based encryption approach to privacy and security in cloud based health services. MSc Thesis, Lakehead Univeristy.

Schnjakin, M., R. Alnemr and C. Meinel, 2010. Contract-based cloud architecture. Proceedings of the 2nd International Workshop on Cloud Data Management, (DM '10), ACM Press, New York, USA., pp: 33-40. DOI: 10.1145/1871929.1871936

Takahashi, T., G. Blanc, Y. Kadobayashi, D. Fall and H. Hazeyama *et al*., 2012. Enabling secure multitenancy in cloud computing: Challenges and approaches. Proceedings of the 2nd Baltic Congress on Future Internet Communications, Apr. 25-27, IEEE Xplore Press, Vilnius, pp: 72-79. DOI: 10.1109/BCFIC.2012.6217983

TCG, 2012. Network Access and Identity.

TCG, 2013. TCG Data Security Architects Guide.

Vazhenin, D., 2012. Cloud-based web-service for health 2.0. Proceedings of the 2012 Joint International Conference on Human-Centered Computer Environments, (CE '12), ACM Press, New York, USA., pp: 240-243.DOI: 10.1145/2160749.2160800

Vernier, D. and A. Jones, 2011. SmartCloud tip: Span virtual local area networks Provision and configure an instance that spans a public and private VLAN. IBM DeveloperWorks.

Wu, R., G. Ahn and H. Hu, 2012. Secure Sharing of Elec-tronic Health Records in Clouds.

Zhang, R. and L. Liu, 2010. Security models and require-ments for healthcare application clouds. Proceedings of the IEEE 3rd International Conference on Cloud Computing, Jul. 5-10, IEEE Xplore Press, Miami, FL., pp: 268-275. DOI: 10.1109/CLOUD.2010.62

Zhou, F., F. Cheng, L. Wei and Z. Fang, 2011. Cloud service platform-Hospital Information Exchange (HIX). Proceedings of the IEEE 8th International Conference on In e-Business Engineering Oct. 19-21, IEEE Xplore, Beijing, pp: 380-385. DOI: 10.1109/ICEBE.2011.35