An Enhanced and Secure Cloud Infrastructure for e-Health Data Transmission

Vasileios A. Memos[1], Kostas E. Psannis[1], Sofoklis Kyriazakos[2], and Sotirios K. Goudos[3]
1: Department of Applied Informatics, University of Macedonia, Greece
2: Department of Business Development and Technology, Aarhus University, Denmark
3: Department of Physics, Aristotle University, Greece

Abstract— **The daily rapid malware growth and spread has enforced the security community of antivirus companies to introduce cloud computing technology to their existing protection methods so as to be able to deal with efficiently the active malware threats. A new hybrid security model, based on cloud computing, must be developed so as to offer optimized protection to the connected users. In this research, we describe our proposed cloud infrastructure and analyze it with mathematical models so as to export significant diagrams about various metrics. Our cloud model architecture consists of four layers: the master cloud server, the slave servers, the virtual subservers and the users connected to the cloud. Experimental results demonstrate that our proposed layered cloud architecture verifies the trust of its implementation and establishment, due to the fact that it makes the current architecture more lightweight, efficient and secure for e-health data transmission.**

Index Terms— **Algorithm, Cloud Security, Cloud Model Infrastructure, e-Health, Layered Cloud Architecture, Mathematical Model, Virtualization.**

I. Introduction

TODAY computer viruses and other malicious software (malware) have been increased and spread rapidly daily. Previous existing protection methods provided by traditional antivirus companies were not adequate to deal with this problem and thus, security community has involved cloud computing technology so as to reinforce antivirus software against such threats [1], [2].

Cloud computing has many advantages in the computer network security area. The basic presupposition is the proper use of this technology. The main advantage is the quicker response to the new threats, such as unknown malware and zero-day threats which spread constantly on the internet. In addition, since user computers do not need to store virus signatures and all the malware analysis takes part in the "cloud" – in the cloud servers where signatures are collected into it – the new cloud based antivirus programs consume low memory and system resources, and most of the processes of these programs take part in the connected server somewhere in the cloud. In other words, these programs operate as clients in the cloud environment [2]-[6].

Information security in the healthcare system is more crucial than ever, given the penetration of IoT devices, as well as the involvement of decisions support systems that consume IoT data and take intelligent decisions.

Many use cases around IoT devices involve smart-phones and wearable sensors that are utilized to capture users' data. Even in the clinical research sector, which is a highly regulated domain, the industry makes small steps towards substitution of manpower for measurements and surveys with the support of electronic Patients Reported Outcomes (ePROs) and electronic Clinical Outcome Assessment (eCOA).

At the same time cloud applications perform Big Data analytics and train reasoners to detect clinical situations and behaviors and apply intelligent decisions support mechanisms, machine learning and Artificial Intelligence techniques for premium services, such as coaching.

Both the IoT environment and the cloud infrastructure of ePRO/eCOA solutions are therefore highly critical, as they involve sensitive data of patients and they participate in critical processes, such as coaching and medication monitoring. The need of a robust cloud infrastructure for Big Data delivery is therefore a mandatory requirement for any vendor or service provider.

This current research focuses on the cloud model architecture for e-health networks, which we classify it in to four layers. In the highest layer, we have the master server where are collected and stored all the virus signatures. Next layers include slave servers in various geographical areas, connected to the master, and virtual subservers created by slave servers for minimizing the total energy consumption and operating costs**.**

The paper is organized as follows: In Section 2, we review all the related previous work in e-health, cloud computing, security, communication, computation, and storage. In Section 3, we analyze our proposed cloud security architecture for e-health networks and describe the layers with variables. In Section 4 we present the architecture with mathematical models and algorithms and classify the experimental results with diagrams. Section 5 includes the security analysis of our proposed infrastructure. Section 6 concludes the paper.

II. Related Work

Cloud computing technology is a new approach applied to antivirus software as a solution to the increased malware samples discovered and spread on the internet every day. Last years, many research studies have taken place in the computer and network security areas, and all of them converge to the importance of cloud technology incorporation to the existing antivirus software [1]-[6].

Corresponding authors:
V. A. Memos, vmemos@uom.edu.gr
K. E. Psannis, kpsannis@uom.edu.gr

In recent years several techniques for cloud-based wireless data delivery have been devised [7]-[11]. Jianqiang Li, et al. in their research [7], proposed a model of computation partitioning. This model provides better performance for the stateful data in a dynamic environment. Moreover, the researchers have determined the issue of calculation segmentation decision for a multi-frame flow of data. Also, they proved that in a network environment with changing bandwidth, the method for the calculation of single-frame data is less efficient than the calculation method of multi-frame data.

In [8] a framework for a healthcare system was designed to address the issues of information security and privacy. This system uses WBANs (Wireless Body Area Networks) to collect health data, then sends these data through a WSN to a WPAN. In the WPAN the data will be published through a gateway. The researchers have decided to use Groups of Send-Receive Model (GSRM) to provide transmission security of the data and the HEBM (Hommomorphic Encryption based on Matrix) to provide privacy. In the end, after experiments in the proposed and implemented scheme, the system was verified for its feasibility.

Moreover, in [9] Jiafu Wan, et al. designed a solution for active preventive maintenance using manufacturing big data. Also, for the processing of data the researchers used the cloud services. Even though, algorithms were proposed for the real time active maintenance and the offline predictive active maintenance. Finally, they analyzed and compared the active preventive maintenance method proposed with the traditional method.

Another relative study is that in [10], where a novel way to use personal cloud storage services for building covert channels has been investigated so as to furtive exchange data through the internet. The authors focused on Dropbox application. Then, a performance evaluation about two different covert communication methods of this application was shown. Finally, behaviors of Dropbox were explored in a production quality deployment.

In [11], Dawei Chen uses artificial bee colony (ABC) algorithm for the optimization of the threshold value and the weight in radial basis function (RBF) neural networks. Then, the nonlinear time series have been analyzed. After experimentation with the proposed model, it was concluded from the results that it has high accuracy in predicting and reflecting the changing law of the data flow. Finally, the authors considered that the proposed model has good perspective in prediction of the traffic flow.

Other relevant research studies were conducted on data storage security, data encryption and privacy in cloud environments. Kan Yang and Xiaohua Jia proposed an efficient and secure dynamic auditing protocol for data storage in cloud environments [12]. H. C. H. Chen and P. P. C. Lee implemented an efficient and practical data integrity protection (DIP) scheme and evaluated it using many parameters in a cloud storage testbed [13]. Chang Liu et al. proposed a new scheme which can support authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates [14]. Seung-Hyun Seo et al. implemented a mediated certificateless public key encryption (mCL-PKE) and the overall cloud based system, and evaluated its security and performance to show its effectiveness [15].

Moreover, in [16] is shown a new multilayered vehicular data cloud platform. This novel platform uses IoT and cloud computing technologies. Also, the authors present an efficient parking service and a vehicular data mining service, both based on cloud. Finally, the researchers present two models for data mining that were modified, and provide some of the challenges for future work.

Furthermore, a hierarchical distributed fog computing architecture was proposed in [17]. This architecture is used in Smart Cities for the integration of bulky number of infrastructure services and components. After experimentation, the feasibility of the system was proved.

The applications of IoT and Cloud in industrialization were explored by the researchers in [18]. Also, a cloud manufacturing service system (CMfg) proposed, which is based on the technologies of IoT and Cloud Computing. In the end, the challenges, the benefits, and future directions were discussed.

In [19] the authors present solutions for the issues in communication, computation, and storage. Therefore, a resolution framework was proposed that is based on fog computing. With this framework the researchers give a solution for the identity of individuals. They also provide better processing. Finally, for the evaluation of the proposed scheme they have developed a system which is based on Local Binary Patterns (LBP) identifier. Experimental results demonstrate that the bandwidth can be saved thanks to this system, while more intelligence is provided to face identification and resolution.

In addition, other studies focus on time critical applications, such as those in the automobile industry and in aerospace, where both of them require real-time automation. A Software Workbench for Interactive, Time Critical and Highly self-adaptive cloud applications (SWITCH) has been proposed in [26], which improves the existing development and execution model of time critical applications by introducing a novel conceptual model in which the combination of QoS and QoE application with the programmability and controllability of Cloud environments can be all imported in the whole applications' lifecycle. Moreover, an energy-efficient task scheduling algorithm in Dynamic Voltage and Frequency Scaling (DVFS) - enabled cloud [27] environment promises power savings up to 46,5% for parallel applications. The algorithm makes use of DVFS in which the parallel tasks are distributed in the idle slots under a lower voltage and frequency, avoiding the violence of the dependency constraints and the increase of the slacked makespan.

Another research [20], discusses the issues and challenges that appear in the cloud for the processing and storing of big data. Therefore, after a thorough analysis, the authors propose a framework for storing all kinds of big data (structured and unstructured). The big data which have been collected by the IoT devices are stored and also managed by a combination of databases and Hadoop that have been extended. Finally, to show how effective is the proposed framework, the authors have developed a prototype system. Moreover in [21] the authors propose a two-tier Demand Side Management (DSM) which is based on cloud, in order to control the residential load of customers who are equipped with alternative sources of energy. After simulations and experiments, they conclude that their proposed model provides lower consumption cost for the customers and improvements in the power grid.

The authors in [22] propose an IoT-based surveillance system for ubiquitous healthcare monitoring. The system consists of sensors, actuators, and cameras. Mesh topology was decided to be used as it provides important advantages. Moreover, the Constrained Application Protocol (CoAP) is used for the data compression and transferring, and the Scalable High-Efficiency Video Coding (SHVC) is used for the video compression and transferring. The SHVC can deliver the same video quality in half of the bit rate than the High-Efficiency Video Coding (HEVC). It should be emphasized that cloud services are provided, such as storage and real-time monitoring. Scalable video coding technology (SVC) has been also used for novel hybrid 3D video delivery [24], and in combination with texture analysis [25]. Both schemes present many advantages in terms of video delivery efficiency.

Last but not least, the paper in [23] proposes an innovative topology paradigm which could offer a better use of IoT technology in Video Surveillance systems. Additionally, the third technology that takes place in the IoT’s contribution in Video Surveillance is Cloud Computing. It should be emphasized that in [23] the Cloud server could provide primarily the important role of storage system, and afterwards could act as data manager that receives these data with the aim to transmit them to the Network Server. Consequently, the Cloud server could interpolate another Local Server in order to clarify and transmit the data to its final destination, which is the Network Server.

Finally, the authors in [29] review the impact of Internet of Things (IoT) and Cyber Physical Systems (CPS) on industrial automation from the Industry 4.0 perspective, and highlight the current status of Ethernet time-sensitive networking (TSN) and shed light on the role of 5G generation telecom networks in automation.

III. Proposed Method

We represent the cloud as a weighted undirected graph of the form:

$$\textit{Cloud} = (\textit{Master Server, Slave Servers, Virtual Subservers, Devices, Users}) \qquad (1)$$

Each of the above entities has its unique features. In the case of ‘Devices’, we regard it as ‘Users’, because each terminal device has its user and the system requirements it should have to access the cloud with the network service of the installed cloud antivirus program (client), are considered to be negligible. This happens because of the fact that the installed cloud antivirus program which runs the cloud as a client, consumes very low system resources and memory.

Our cloud model architecture consists of four layers, as it is depicted in Fig. 1: the master cloud server, the slave servers, the virtual subservers and the users connected to the cloud. A mathematic description of these layers follows.

A. Description of the Layers

Our proposed cloud infrastructure has the following layers (from highest to lowest one):

Layer 4: In the highest layer there is the master cloud server. This is the main server where all virus signatures are collected from the connected - to the cloud - users and stored inside it.

Let *MS* be the Master Server. For optimal performance, its features should be:

- as minimum as possible Wh E (energy consumption)
- as maximum as possible TB HDD (hard disk storage)
- as maximum as possible TB RAM (memory)
- as maximum as possible GHz CPU (speed processor)
- as maximum as possible TB/s B (bandwidth)

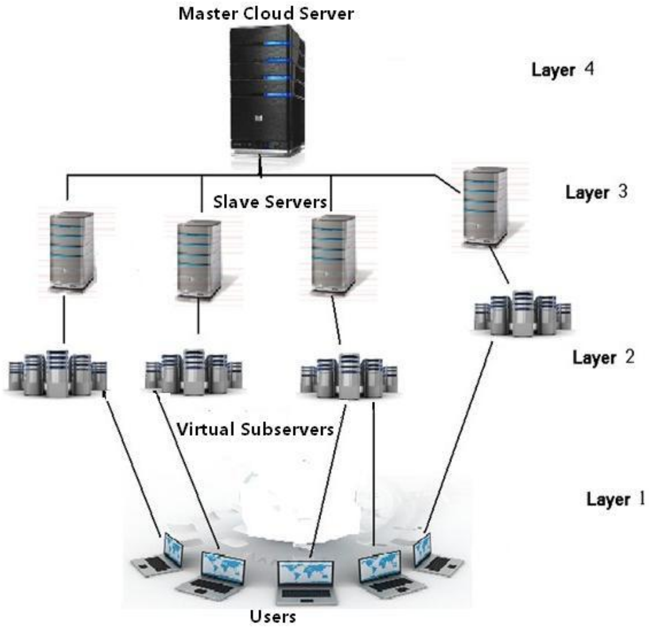

Fig. 1 The layered cloud architecture

Layer 3: This is the next lower layer, where there are the slave servers. These slave servers are connected to the master server and help the serve of the users all over the world. The slave servers will be located in various geographical areas for serving the closest users by their IP address criterion.

Thus, let *m* Slave Servers connected to Master Server:

$$MS = (SS_1, SS_2, \ldots, SS_m) \qquad (2)$$

Their features of each one are defined as follows:

- p W P
- α TB HDD
- μ TB RAM
- σ GHz CPU
- β TB/s B
- x users that is able to serve (maximum number)

Layer 2: In this layer, we have virtual subservers created by the slave servers for minimizing the total energy consumption and operating costs. In addition, virtualization allows for multiple connected users to share common physical resources of the slave servers, so we have better resource allocation that result to better serve to the users' requests.

Let k Virtual Sub Servers in each Slave Server:

$$SS_j = \{VS_1, VS_2, ..., VS_k\} \quad (3)$$

where $j=1...m$ (slave servers).

Each virtual subserver will have the following features:

- p/k W P
- α/k TB HDD
- μ/k TB RAM
- σ/k GHz CPU
- β/k TB/s B
- x/k users that is able to serve (maximum number)

Layer 1: This layer is the lowest and includes the users all over the world that are connected to the cloud. Each user's terminal has a cloud antivirus program installed that is used as a client for communication with the cloud servers and specifically with the next higher layer, the virtual cloud subservers. Most processes of the program take part in the connected virtual subserver in the cloud. At frequent intervals, the client automatically scans the computer for virus existence, using the information it takes from the web service's database of the cloud server that it is connected to. Generally, cloud antivirus programs consume low memory and system resources, with minimum computer resources. Therefore, the RAM consumption caused by the client must be as minimum as possible MB to the computer where it runs.
Let n Users:

$$U = \{u_1, u_2, ..., u_n\} \quad (4)$$

To define each unique user, we divide the n users to m user groups, as many as the slave servers, as follows:

$$U_j = \{U_{j1}, U_{j2}, ..., U_{jx}\} \quad (5)$$

where $j=1...m$, and

x: the maximum number of users connected to each slave server

Each user group is divided to k user subgroups as many as the virtual subservers:

$$U_{jh} = \{U_{jh1}, U_{jh2}, ..., U_{jhx/k}\} \quad (6)$$

where $h=1...k$

Let U_{jhy} each user of each slave's virtual subserver, in other words, unique user in the world,
where $y=1...x/k$ (x/k: the maximum number of users connected to each slave's virtual subserver).

B. Internet Connections and Networks

In our scheme there are the following connections and networks:

Between Layer 1 – 2: communication between users' computers and virtual sub servers of the slave servers. Features: user dependent internet connection, specific bandwidth, downstream/upstream speed – DSL 24/7 connections recommended.

Between Layer 2 – 3: Virtual LANs (communication between the virtual sub servers and the Slave Servers). Features: specific bandwidth, downstream/upstream speed – as maximum as possible recommended.

Layer 3: MANs and WANs (connection between the Slave Servers). Features: specific bandwidth, downstream/upstream speed – as maximum as possible recommended.

Between Layer 3 – 4: WAN (communication between the Slave Servers with the Master Cloud Server). Features: specific bandwidth, downstream/upstream speed – as max as possible recommended.

IV. Experimental Results

In this section we present our scheme with mathematical analysis and then we export indicative graphs to show some properties of the model.

A. Mathematical Model Analysis

Let z timeslots:

$$t_z = \{t_1, t_2, ..., t_\infty\} \quad (7)$$

where $z=1...\infty$ with δ duration in seconds each one.
Let λ files (f) uploaded per timeslot:

$$f_{t_z} = \{f_1, f_2, ..., f_\lambda\} \quad (8)$$

Let $s_{f_{t_z}}$ bytes the length of each file f_{t_z}.

Each timeslot (t_z), each user (U_{jhy}) automatically upload for analysis λ files (f) with $s_{f_{t_z}}$ size each one. So the bandwidth in each virtual subserver is given below:

$$\frac{1}{\delta} \times \sum_{y=1}^{x/k} \left\{ \sum_{f=1}^{\lambda} s_{f_{t_z} U_{jhy}} \right\} = \frac{\beta}{k} \quad TB/s \;\; B_{VS_h SS_j} \Leftrightarrow$$

$$B_{VS_h SS_j} = \frac{k}{\beta \cdot \delta} \times \sum_{y=1}^{x/k} \left\{ \sum_{f=1}^{\lambda} s_{f_{t_z} U_{jhy}} \right\} \quad (TB/s) \quad (9)$$

where: $VS_h SS_j$ is an $h=\{1...k\}$ Virtual Subserver of a $j=\{1...m\}$ Slave Server,
k is the total virtual subservers connected to each slave server,
m is the total slave servers,
$s_{f_{t_z} U_{jhy}}$ is the total size of the U_{jhy} user's uploaded files in every timeslot t_z.

Based upon the above formula (9), the algorithm which gives the bandwidth in each virtual subserver is the following Algorithm 1. The logic flow of the algorithm is briefly summarized as follows:

Algorithm 1. The algorithm which counts the bandwidth in each virtual subserver

```
Set $\beta, \delta, x, k, r, t_z = \{t_1, t_2, ..., t_\infty\}$
Initialize $y=1, sum'=0$
$r = x/k$
for $y \le r$ do
    Set $\lambda, f_{t_z} = \{f_1, f_2, ..., f_\lambda\}, s_{f_{t_z}}$
        Initialize $f=1, sum=0$
    while $f \le \lambda$ do
        $sum \leftarrow sum + s_{f_{t_z}}$
        $f \leftarrow f+1$
    end while
    Update $sum$
    $sum' \leftarrow sum' + sum$
    $y \leftarrow y+1$
end for
Update $sum'$
$B_{VS_hSS_j} = k \cdot sum' / \beta \cdot \delta$
Return ($B_{VS_hSS_j}$)
```

To find the power consumption per second in each virtual subserver, we will use the below formula.

$$P_{VS_hSS_j} = \frac{1}{\delta} \times \sum_{y=1}^{x/k} \left\{ \sum_{f=1}^{\lambda} p_{f_{t_z}U_{jhy}} \right\} W \left(\frac{J}{sec}\right) \quad (10)$$

where $p_{f_{t_z}U_{jhy}}$ the power consumption of the analysis of the f_{t_z} files (per specific timeslot) of the U_{jhy} user.

Thus, the power consumption in whole slave server is the sum of its virtual subservers:

$$P_{SS_j} = \sum_{h=1}^{k} P_{VS_hSS_j} \quad W\,(J/sec) \quad (11)$$

Therefore, the energy consumption of each slave server will be:

$$E_{SS_j} = P_{SS_j} \times t \Rightarrow$$

$$E_{SS_j} = P_{SS_j}\,(W) \times 1\,(hr) \Rightarrow$$

$$E_{SS_j} = P_{SS_j} \; Wh \quad (12)$$

To find the available minimum RAM, CPU and HDD features allocated to the maximum number of connected users to each virtual subserver, we use the following formulas:

$$RAM_{VS_hSS_j} = \frac{\mu/k}{x/k} = {}^{\mu}/_{x} \; TB \text{ (min. per user)} \quad (13)$$

$$CPU_{VS_hSS_j} = \frac{\sigma/k}{x/k} = {}^{\sigma}/_{x} \; THz \text{ (min. per user)} \quad (14)$$

$$HDD_{VS_hSS_j} = \frac{a/k}{x/k} = {}^{a}/_{x} \; TB \text{ (min. per user)} \quad (15)$$

B. Graphical representation of the mathematical model properties

RAM per user: μ/x is the minimum RAM size of the virtual subserver which is distributed per connected user, when we have the maximum limit of users (x/k) connected to the virtual subserver. In the case of $i < x/k$ users: ${}^{\mu}/_{i} > {}^{\mu}/_{x}$, which means that there is larger available amount of RAM per connected user. Fig. 2 shows this ratio between RAM usage and connected users.

Conditions:

- $While\ i \to 0, RAM_{VS_hSS_j} \to max$ (16)
- $While\ i \to x/k, RAM_{VS_hSS_j} \to min$ (17)

In other words, the increase of connected users to a virtual subserver of a slave server causes the reduction of the available virtual-subserver's memory per user. When the number of connected users reaches the maximum allowable limit which has each virtual subserver, the available memory per user is the minimum possible.

CPU per user: σ/x is the minimum CPU size of the virtual subserver which is distributed per connected user, when we have the maximum limit of users (x/k) connected to the virtual subserver. In the case of $i < x/k$ users: ${}^{\sigma}/_{i} > {}^{\sigma}/_{x}$, which means that there is larger available amount of CPU per connected user. Fig. 3 shows this ratio between CPU usage and connected users.

Conditions:

- $While\ i \to 0, CPU_{VS_hSS_j} \to max$ (18)
- $While\ i \to x/k, CPU_{VS_hSS_j} \to min$ (19)

In other words, the increase of connected users to a virtual subserver of a slave server, cause the reduction of the available virtual-subserver's processor speed per user. When the number of connected users reaches the maximum allowable limit which has each virtual subserver, the available processor speed per user is the minimum possible.

HDD per user: a/x is the minimum HDD size of the virtual subserver which is distributed per connected user, when we have the maximum limit of users (x/k) connected to the virtual subserver. In the case of $i < x/k$ users: ${}^{a}/_{i} > {}^{a}/_{x}$, which means that there is larger available amount of HDD per connected user. Fig. 4 shows this ratio between HDD availability and connected users.

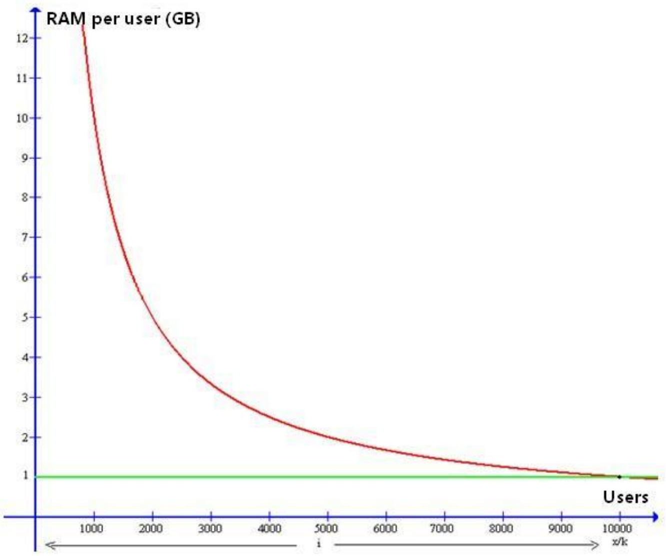

Fig. 2. Ratio between connected users and available RAM per user in each virtual subserver of the 2nd layer

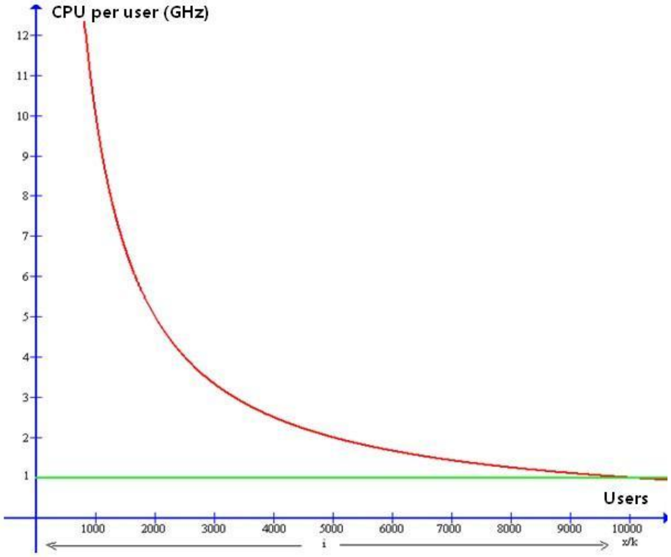

Fig. 3. Ratio between connected users and available CPU per user in each virtual subserver of the 2nd layer

Conditions:

- $While\ i \rightarrow 0, HDD_{VS_hSS_j} \rightarrow max$ (20)
- $While\ i \rightarrow x/k, HDD_{VS_hSS_j} \rightarrow min$ (21)

In other words, the increase of connected users to a virtual subserver of a slave server, cause the reduction of the available virtual-subserver’s disk storage per user. When the number of connected users reaches the maximum allowable limit which has each virtual subserver, the available disk storage per user is the minimum possible.

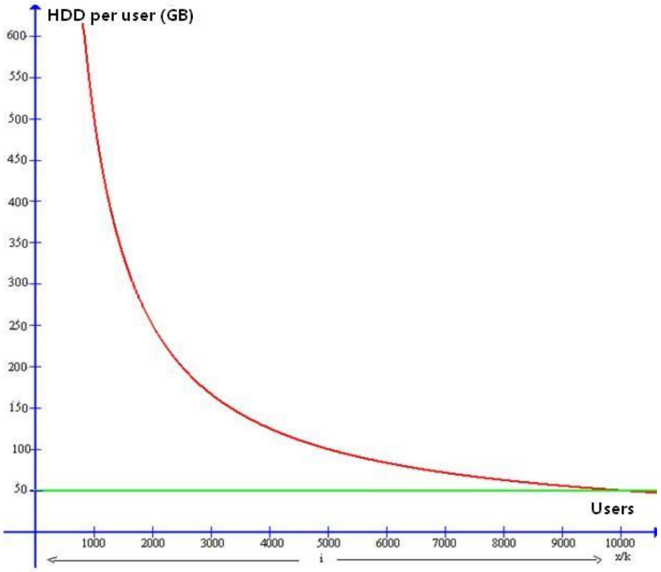

Fig. 4. Ratio between connected users and disk storage availability per user in each virtual subserver of the 2nd layer

V. Security Analysis

A. File upload and analysis time - privacy issues

The files’ analysis depends on the size of the files. In the case of media files, which are usually many MB or GB, the files uploading process will take part in too much time to be completed and the analysis may be slow. In addition, there are many security concerns about privacy, which are about the collected e-health data in the cloud servers and the concern if everyone can have access to the contents of the files [17].

Thus, user files should not be uploaded whole, but only a part of them and specifically as a small reverse signature of each file, created by the antivirus program which will be installed in users’ computers and will run as a client. Therefore, the signature file will what gets uploaded and checked against the cloud, which means that there is not possible for someone to have access to potential personal information contained in the files.

Reverse engineering malware signatures is the new well-promising scheme which is under research [28] and presents many advantages compared to the conventional method. In the following figures we present graphically the results of our experiments between our proposed and the conventional method which is used by antivirus programs, for both upload and analysis time in the cloud servers, and the overall power consumption.

Fig. 5 shows the ratio between the size of the files and the upload time to a cloud server if they will be uploaded whole and in case that they will be uploaded as a small reverse signature. As it is clearly shown, the uploading of only reverse file signatures saves significant time in comparison with the uploading of whole files. Fig. 6 shows the ratio between the size of the files and their analysis time in a cloud server. In both cases, the size of the files increases the time. As it is clearly shown, the analysis time of only reverse file signatures saves significant time in comparison with the analysis time of whole files. Thus, from these two figures, we observe that in

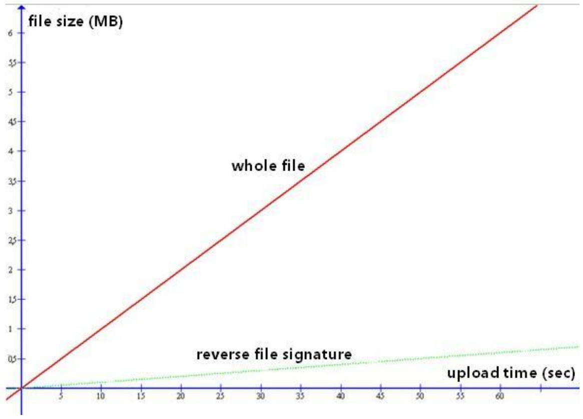

Fig. 5. Ratio between file size and its upload time to a cloud server

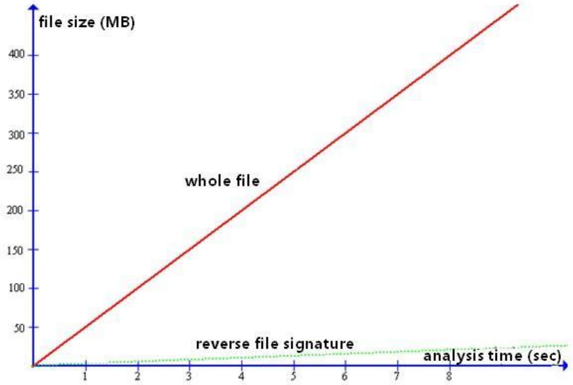

Fig. 6. Ratio between file size and its analysis time in a cloud server

the case of reverse signature use, the upload and analysis time is significantly reduced.

Our scheme takes care of the privacy of the users-patients connected to the cloud servers. Privacy issues in cloud computing are caused because of the concerns about the personal information and health data which are collected by the cloud servers. In our proposed infrastructure, none of whole user files will be uploaded to the cloud servers, but only their small reverse signatures created by the antivirus program which will run as client in users' computers. This method solves privacy issues, increase the time analysis of the files and reduce significantly the power consumption of the cloud servers, making the whole cloud infrastructure more lightweight and effective.

The Master and Slave servers make use of Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) encryption algorithms which support secure and confidential transmission of the e-health data of the patients. In addition, both master and slave servers make use of anti-DDoS hardware and software modules, and more specifically network firewalls and specialized web application firewalls, and load balancers for avoiding Denial of Service / Distributed Denial of Service (DoS/DDoS) attacks and flood attacks. Therefore, our proposed architecture demonstrates secure e-health data transmission over the internet.

B. *Power consumption of the slave servers:*

As we defined in the formulas (10) and (11), the power consumption of each slave server depends on the processor's power consumption of the users' files analysis, which are uploaded to its virtual subservers.

In addition, the power consumption of the file analysis depends on the analysis time, which as we describe previously, depends on the size of the files. Therefore, there is a ratio between power consumption and total size amount of the uploaded files to the cloud server, which is represented in Fig. 7.

As it is clearly shown, the increase of the size amount of the files, increase significantly the power consumption too. Thus, in the case of small reverse signatures, the power consumption will be notably less (Fig. 7 – dotted line) compared to whole files. This is another important reason that it is not recommended for the whole files to be uploaded to the cloud servers.

It is worth to mention that the slave servers' existence is necessary for the proper distributed serving of the closest users depending on their geographical area they are located. In other words, each slave server is used to a specific geographical area, and therefore to a specific target group. The use and proper distribution of the slave servers over the world, demonstrates better allocation of the available system resources and enables power savings.

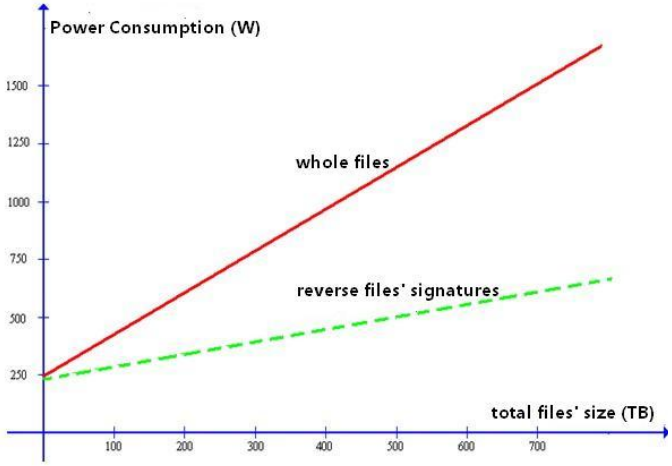

Fig.7. Ratio between total size of the files and their power consumption of analysis in a cloud server

C. *Superiority of the Proposed Model*

As it is described in the previous section, our proposed model is based on a novel and lightweight approach to gain advantages in terms of energy efficiency (low consumption) and time efficiency (both upload and analysis). In addition, security and privacy issues are taken into account.

The proposed scheme has been compared to general and common methods of conventional antivirus vendors. Specifically, while antivirus vendors rely on malware signatures and some other heuristics scanning techniques, our proposed method is based on reverse engineering – pattern-based – malware signatures, automatically deriving [28].

Moreover, our idea for uploading only a part of each file for scanning, and more specifically as a small reverse signature, offers the above benefits. This feature is reinforced by our proposed redesigned layered cloud infrastructure, which presents superiority compared to conventional network infrastructures in terms of resource allocation (RAM, CPU, disk storage).

VI. CONCLUSIONS

Last years, antivirus software vendors implement cloud computing technology to their provided protection methods for better detection rates to deal with the daily malware spread. The use of Cloud computing in the antivirus software has many benefits in the computer network security area, such as low system resources consumption and quicker and more effective detection of new unknown malware that is spread daily on the internet.

Our approach is the redesign of cloud computing model in order to support better resource allocation, less analysis time of the users' e-health data and quicker response to the users' requests to the cloud servers of the e-health networks.

Future work will include the incorporation of security algorithms to our proposed scheme so as to be able to offer better security in e-health data encryption and e-health data storage areas in the cloud. Moreover, new features such as intelligent sandbox in the client antivirus program and system-changes based virus-signatures that will be created in the cloud, should be proposed in the near future to ensure maximum detection rates and high security protection level.

Finally, the data error ratio is an important parameter which will be studied in the future, as far as how it affects our well-promising transmission scheme. It is also worth pointing out that cloud technology in future communication e-health networks will optimize energy consumption. This is also a potential research direction.

REFERENCES

[1] Ali Abdullah Hamzah, Sherif Khattab and Salwa S. El-Gamal, "Resource Allocation for Antivirus Cloud Appliances", *IOSR Journal of Computer Engineering,* Vol. 10, Issue 3, pp 33-42, March-April, 2013.

[2] V. Memos and Kostas E. Psannis**,** A New Methodology based on Cloud Computing for Efficient Virus Detection, New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering, Lecture Notes in Electrical Engineering Volume 312, , pp 37-47. 2015

[3] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, December 2016

[4] Dharma Agrawal, B. B. Gupta, Shingo Yamaguchi and Kostas E. Psannis, "Recent Advances in Mobile Cloud Computing", Wireless Communications and Mobile Computing, 2017

[5] Christos Stergiou & Kostas E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey," International Journal of network management, DOI: 10.1002/nem.1930, pp. 1-12, March 2016

[6] Christos Stergiou and Kostas E. Psannis, Efficient and Secure BIG Data Delivery in Cloud Computing, Multimedia Tools and Applications, 2017

[7] Jianqiang Li, Luxiang Huang, Yaoming Zhou, Suiqiang He, and Zhong Ming, "Computation partitioning for mobile cloud computing in a big data environment", IEEE Transactions on Industrial Informatics, 2017.

[8] Haiping Huang, Tianhe Gong, Ning Ye, Ruchuan Wang, and Yi Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System", IEEE Transactions on Industrial Informatics, 2017.

[9] Jiafu Wan, Shenglong Tang, Di Li, Shiyong Wang, Chengliang Liu, Haider Abbas, and Athanasios V. Vasilakos, "A Manufacturing Big Data Solution for Active Preventive Maintenance", IEEE Transactions on Industrial Informatics, 2017.

[10] Luca Caviglione, Maciej Podolski, Wojciech Mazurczyk, and Massimo Ianigro, "Covert Channels in Personal Cloud Storage Services: the case of Dropbox", IEEE Transactions on Industrial Informatics, 2016.

[11] Dawei Chen, "Research on traffic flow prediction in the big data environment based on the improved RBF neural network", IEEE Transactions on Industrial Informatics, 2017.

[12] Kan Yang and Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", *IEEE Transactions on Parallel and Distributed Systems,* vol 24, no 9, September 2013.

[13] Henry C. H. Chen and Patrick P. C. Lee, "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation", *IEEE Transactions on Parallel and Distributed Systems,* 2013.

[14] Chang Liu, Jinjun Chen, Laurence T. Yang, Xuyun Zhang, Chi Yang, Rajiv Ranjan and Kotagiri Ramamohanarao, "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-grained Updates", *IEEE Transactions on Parallel and Distributed Systems,* 2013.

[15] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding and Elisa Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", *IEEE Transactions on Knowledge and Data Engineering,* 2013.

[16] Wu He, Gongjun Yan, and Li Da Xu, "Developing Vehicular Data Cloud Services in the IoT Environment", IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, May 2014.

[17] Bo Tang, Zhen Chen, Gerald Hefferman, Shuyi Pei, Tao Wei, Haibo He, and Qing Yang, "Incorporating Intelligence in Fog Computing for Big Data Analysis in Smart Cities", IEEE Transactions on Industrial Informatics, 2017.

[18] Fei Tao, Ying Cheng, Li Da Xu, Lin Zhang, and Bo Hu Li, "CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System", IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, May 2014.

[19] Pengfei Hu, Huansheng Ning, Tie Qiu, Yanfei Zhang, and Xiong Luo, "Fog Computing-Based Face Identification and Resolution Scheme in Internet of Things", IEEE Transactions on Industrial Informatics, 2016.

[20] Lihong Jiang, Li Da Xu, Hongming Cai, Zuhai Jiang, Fenglin Bu, and Boyi Xu, "An IoT-Oriented Data Storage Framework in Cloud Computing Platform", IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, May 2014.

[21] Mohammad Hossein Yaghmaee, Morteza Moghaddassian, and Alberto Leon-Garcia, "Autonomous Two-Tier Cloud Based Demand Side Management Approach with Microgrid", IEEE Transactions on Industrial Informatics, 2016.

[22] Andreas Plageras, Kostas Psannis, Yutaka Ishibashi and Byung-gyu Kim, IoT-based surveillance system for ubiquitous healthcare, 42nd Annual Conference of IEEE Industrial Electronics Society, Piazza Adua, 1 - Firenze (Florence), Italy October 23-26, 2016

[23] Christos Stergiou, Kostas E. Psannis, Andreas P. Plageras, Giorgos Kokkonis, Yutaka Ishibashi, Architecture for security monitoring in IoT environments, The 26th *IEEE* International Symposium on Industrial Electronics, 19-21 June *2017* Edinburgh, Scotland, UK

[24] A Novel Hybrid 3D Video Service Algorithm Based on Scalable Video Coding (SVC) Technology, Displays 40, doi:10.1016/j.displa.2015.05.005, (2015) 45–52.

[25] Fast Algorithm for the High Efficiency Video Coding (HEVC) Encoder Using Texture Analysis (Kalyan Goswami, Jong-Hyeok Lee, Byung-Gyu Kim), Information Sciences, Volumes 364–365, 10 October 2016, Pages 72–90.

[26] Zhao Z, Taal A, Jones A, Taylor I, Stankovski V, Vega IG, Hidalgo FJ, Suciu G, Ulisses A, Ferreira P, de Laat C. A Software Workbench for Interactive, Time Critical and Highly self-adaptive cloud applications (SWITCH). InCluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on 2015 May 4 (pp. 1181-1184). IEEE.

[27] Tang Z, Qi L, Cheng Z, Li K, Khan SU, Li K. An energy-efficient task scheduling algorithm in DVFS-enabled cloud environment. Journal of Grid Computing. 2016 Mar 1;14(1):55-74.

[28] Christian Wressnegger, Kevin Freemany, Fabian Yamaguchi, and Konrad Rieck, "Automatically Inferring Malware Signatures for Anti-Virus Assisted Attacks", ACM ASIA Conference on Computer and Communications Security (CCS), April 2017.

[29] M. Wollschlaeger, T. Sauter and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things

and Industry 4.0," in *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17-27, March 2017. doi: 10.1109/MIE.2017.2649104