I J C T A, 9(19) 2016, pp. 9291-9303

A Novel Method for Secured Cloud – Health – Care – System

Sudhanshu Maurya[*] and Kuntal Mukherjee[**]

ABSTRACT

The cutting age technology cloud computing can reshape the existing e-health care system by providing the accessibility of data of patients uninterruptedly at any time and by using any device. The cloud based e-health care system, that is c-health care system can provide a means to store huge data of patients compared to the traditional e-health care system at a minimum capital as well as operational expenditure. But there is every chance to tamper with this sensitive data while it is in transit or is stored in cloud environment. In this context, this endeavor has proposed an effective frame work for cloud-health (c-health) care system and algorithms to keep the sensitive data of patients in public cloud so that it can be omnipresent as well as secured. For this, the concept of service oriented architecture (SOA), object oriented software engineering and Hadamard graph have been used.

Keywords: Cloud Computing, Health Care System, Community Cloud, Hadamard Matrix, Security Issue.

I. INTRODUCTION

Cloud computing has opened a new door of opportunity for all types of organizations including manufacturing, insurance, healthcare etc. This new paradigm has enormous potentiality to slash down their capital as well as operational expenditure. Moreover, with the help of its ubiquitous nature, the organizations can provide their services to the users uninterruptedly. In health sectors, it is of paramount importance to provide the medical history of a patient during an emergency. The information can be even accessed by using smart phones. Further, it is observed that the elderly people, who live alone, continuously need to access their health history. The existing e-Health system is based on the concepts of electronic health records and patient-centric personal health records, which are totally centralized by nature. Further, maintaining such huge centralized data of the patients is not only a costly affair, but there is every chance of loss of data also. Data may not even be available remotely during emergency. For this purpose, the omnipresent nature of cloud would be very handy for the development of a system that would be capable enough to provide a patient's medical history from a remote place. In this regard, this endeavor has proposed a framework based on cloud computing for accessing patient's data uninterruptedly, irrespective of geographical barriers. The proposed framework would provide a way to store the vast medical data of the patients in the public cloud and patients can access it during emergency from any place. The patients would be able to access the data through their thin clients. In this way, the data storage facility of the public cloud would be handy for designing an effective cloud based Health care system, which is c-Health care system.

II. LITERATURE SURVEY

An imperative market survey by International Data Corporation (IDC) in 2008 was made (http://blogs.idc.com/ie/?p=210) among the Chief Information Officers in order to reveal the main challenges prior to the adoption of cloud computing. IDC survey report summarizes the following challenges of cloud

[*] Department of Computer Science and IT, Jharkhand Rai University, Ranchi, Jharkhand, India, *E-mail: sam.sudhanshu@gmail.com*

[**] Department of Computer Science and Engineering, BIT Mesra, Ranchi, Jharkhand, India, *E-mail: kmukherjee@bitmesra.ac.in*

computing: security, availability, performance, on-demand model payment, lack of interoperability etc. A re-conduction of survey in 2009 by IDC was done (http://blogs.idc.com/ie/?p=730) for resolving the challenges of cloud computing. The survey reports of two consecutive years, have pointed out that the question of security is the major issue for cloud computing. The survey report of the year 2009 shows a 12.9% hike in security issue compared to the report of the year 2008. In addition to that, as per the National Institute of Standards and Technology (NIST) (http://www.nist.gov/itl/cloud/index.cfm), portability, interoperability and security are considered highest obstacles to cloud computing by governments and industries. A detailed survey about the security and privacy of cloud computing has been observed in the research work of [1] . The authors have presented the survey report highlighting the challenges for adoption of cloud computing by organizations. Their survey report has revealed that security is the main challenge of cloud computing. Again, the authors in [2] have identified several challenges of cloud computing. They have first discussed the relationships between cloud computing with two related computing paradigms, namely Grid Computing and Service-Oriented Computing. After that, the authors have highlighted several challenges of cloud computing, namely security, costing model, charging model, Service Level Agreement, what to migrate into cloud computing etc. In addition to that, researcher in [3] has determined some key challenges of cloud computing like security and privacy, interoperability and portability, service delivery and billing, performance and bandwidth cost, reliability and availability. So, both industries and the research community, have unanimously identified security as the major challenge of cloud computing. Moreover, it is observed that both the organizations and the research community have presented their own taxonomy of the cloud computing security issues due to the lack of the availability of its de facto standard to be followed. In this context, this manuscript has presented their views one by one.

III. A. SECURITY ISSUES ADDRESSED BY ORGANIZATIONS

NIST is continuously doing research in order to develop the standards for security, interoperability and portable for cloud computing [4]. The NIST Cloud Computing Reference Architecture and Taxonomy Working Group (NCCRAT-WG) have presented the first version of the NIST cloud computing reference architecture and taxonomy. Here, the security and privacy aspects of the cloud cut across all layers of the cloud backbone. Further, NIST has provided the security and privacy issues along with related recommendations for organizations to follow while using public cloud services. Their suggestions include governance, trust, compliance, exclusive ownership rights over data, establish clear etc. [5] (http://csrc.nist.gov/publications/nistpubs/800144/SP800-144.pdf). Thus, the cloud computing reference architecture sketches out five major roles, namely cloud consumer, provider, broker, auditor, and carrier. The service provided by the cloud provider is evaluated by the cloud auditor in terms of security, privacy and performance [6]. Moreover, author in [7] has highlighted the security risks associated with cloud computing before migrating into it.

III. B. SECURITY ISSUES ADDRESSED BY RESEARCH COMMUNITY

The authors in [8] have highlighted about the interoperability and integration challenges of existing e-Health care system though it is observed that more emphasized have been done into its design and development. Further, the authors in [9] have argued about the strong protection of huge private data of patients in existing e-Health care system as well as about its availability to clinicians. The security and privacy of this data, its standardization etc. is of the utmost need [9]. Again, the existing e-Health system suffers from the lack of providing the financial assessment related information [10]. Moreover, existing e-Health care system needs a huge capital as well as operational expenditure [11]. Again, authors in [12] have pointed out that the existing e-Health system cannot address all needs of patient's, namely continuously monitoring the status of the patient, the continuously availability of his data etc. Hence, the concept of cloud computing can be very handy to build new health care system, that is c-Health care system. It can

reduce the capital as well as the operational expenditure compared to the existing e-Health care system [11]. But there is other side of coin also. The sophisticated technology cloud computing is also having some serious challenges to be addressed. Hence, before adopting c-Health care system, it is of the utmost need to address the major challenges of cloud computing. The authors in [13] have presented cloud security taxonomy as architecture, privacy and compliance. The architecture dimension is subdivided as network configuration, host, application, data security and storage, security management, identity and access management etc. The compliance dimension provides administrative and legal responsibilities of the cloud service providers, whereas privacy dimension is initially divided into concerns and principles. Further, an interesting classification of cloud computing security issues is observed in the research work of [14]. The classification is based on the viewpoint of customers, service provider and government. The authors have highlighted the security risks that the customers have to confront in order to use cloud computing, which include downtime of cloud computing, leak of commercial secrets etc. Further, the security risks that the cloud providers have to confront include sustainable security of cloud datacentre, keeping the data safe from the network hackers etc., whereas the risks the government administrators need to confront while using cloud computing include protection of a mass scale datacentre, evaluation and ranking of the security level of cloud service providers etc. The authors in [15] have made a detailed study about security of cloud computing, based on gaps within the existing ISO 27002 security control when it is applied to cloud computing. The authors in [15] have made a comparative study of security controls as suggested by ISO 27002 and the use case of cloud computing. Their study has revealed that there are considerable security gaps in cloud models. The author in [16] has focused on possible security risks of cloud computing, along with its potentiality of reducing infrastructure and operational costs for organizations. In cloud security relationship framework proposed by author in [16] has three components, namely delivery, deployment and user and it has been evaluated in contradiction of three grounds which is security, cost and capability. Once more, author indicated that when the data and information of clients exists in cloud, they it may be possible that the data could be stolen, abused, disturbed, harmed or comprised. In this context, he has further proposed information classification to cloud computing. The security and privacy requirements of information assets include confidentiality, integrity, privacy and impact. On the basis of security and privacy requirements of information assets, some assets are not suitable to be migrated to cloud. Finally, he has concluded that his proposed cloud security relationship framework along with information classification model would be used for making decisions regarding which information assets need to be migrated to the cloud. Again, the authors in [17] have presented a holistic view of cloud computing security including data integrity, confidentiality and privacy, physical and process security aspects, legal compliance etc. After identifying the three groups involved in cloud security, namely public and hybrid cloud service providers, individual and organizations that use cloud services and third-party authorities involved in fiduciary duty, their endeavour is to map security concerns and obligation of each of these groups. Finally, the authors have presented a security assessment framework based on high level steps that can be used to assess security of business applications to be migrated to cloud. Again, the authors in [18] have presented a detailed discussion about the security, privacy and trust aspects of cloud computing. After the discussions about the fundamental concepts of cloud computing, the authors have highlighted its security, privacy and trust issues. After a detailed discussion about the security aspect of cloud computing, the authors in [18] have presented the broad categories of security challenges in cloud computing, which are Confidentiality, Integrity and Availability. With a proper discussion of the concept of confidentiality, they have presented the subsequent literature review of it. They have discussed confidentiality at two levels: technical level and social level. The technical level is involved with data encryption. At the Social level, confidentiality issues focus on better and clearer policies and practices adopted by the cloud provider. Further, the authors in [18] have highlighted the integrity issue of cloud computing with a proper literature review. They have also focused on the availability issue of cloud computing. They have presented its basic concepts and its different perspectives, namely cloud interoperability and content-replication. After that, they have focused on the

privacy aspect of cloud computing, addressing its different aspects, namely authentication, authorization and accountability. They have presented a literature review for the same. Finally, they have presented the trust aspect of cloud computing including its different issues, namely compliance, non-repudiation, reputation etc. Again, the authors in [19] have presented the review report of the characteristics of cloud computing with an analysis of security challenges and current security technologies. The security challenges include system reliability, privacy and data protection, data isolation and other challenges. As per the categories of challenges, they have proposed a solution of security from three aspects which is cloud computing operators, enterprise users and regulators. Furthermore, the authors in [20] have presented six sub-categories of security issues in cloud computing environments. These address the ways of providing safety mechanisms, keeping data confidential, avoiding malicious insiders, avoiding of service hijacking, managing multi instance in multi-tenancy virtual environments as well as developing appropriate law and implementing legal jurisdiction. Inter cloud is Cloud of Clouds interconnected globally. An interesting research regarding the inter cloud security including trust model, identity and access management, governance considerations etc. has been observed [21]. The authors in [22] have presented their research work with the aim of evaluating the amount of security that is applied to a cloud computing service. Further, the authors have presented a set of evaluating criteria for security of data in cloud environment. Further, there are three categories of security: traditional security, availability, third-party data control [23]. The control of third-party data is a main threat to cloud computing environment. So, after analysing the above discussions, we conclude that the security issue of cloud computing is mainly categorised in integrity, confidentiality and availability.

III. C. CHALLENGES OF CLOUD BASED E-HEALTH CARE SYATEM

It is observed that security is a big challenge for cloud based health care system [24]. It is beyond doubt that if c-Health care system is to be ubiquitous and trusted; one needs to make data security systems that are not hindered by the application. The data originates from a source, the mode of transport for that data, the place the data is accessed from, or the device it is used upon. The determining factors for successful c-Health care system data security are seamlessness and interoperability built around a core digital-identity-led security policies. Furthermore, when the question arises about the data outsourcing in c-Health care system, the data may be in the hands of 3rd, 4th and nth parties and the trust inherent in direct business-to-business transactions [22]. It is observed that there is no control over the cloud storage servers in c-Health care system by the users. Hence, there is always a chance of exposure of data [17] in the cloud environment. In the light of novelty, security challenges in the c- Health care system also includes confidentiality, integrity and availability. As already discussed the confidentiality issues comprise of two types, namely social and technical. Social problems discuss the practices and policies that the service providers of cloud necessarily approve in order to protect the patient's data in c-Health care system. Again, the technical issue focuses on the encryption of data while accumulation of huge data of patients in c-Health care system. This manuscript has focused only on the technical issue of cloud computing and its use in c-Health care system.

IV. PROPOSED FRAMEFORK OF C-HEALTH-CARE-SYSTEM

There are lot of advantages of the cloud storage services, it can curtail down the storage cost, enhance the data availability etc. compared to the existing centralized e-Health care servers. But there is the other side of the coin-the data stored at public cloud in e-Health care system may suffer from a breach of security. There is chance of tampering with the data. Hence, the main focus of this manuscript is to propose a new security mechanism for the data in c-Health care system. Thus this manuscript has emphasized only on the technical aspect of the confidentiality issue of cloud computing and its use in e-Health care system and to build a robust c-Health care system. The proposed framework has presented a solution for the lack of security and privacy of patients' data. This manuscript has focused on a new security framework, security algorithms for c-Health care system based on Hadamard graph. The results of the implementations are

presented in order to reveal the effectiveness of the proposed algorithms and framework. Our proposed framework is shown in Figure1. In the architecture, the concept of SOA (Service Oriented Architecture) has been used to make the proposed framework to be more agile. Here user can interact with cloud Governance Web services of the private cloud of health care organization, whenever needed. The private cloud encrypts the sensitive data of the patient and hands it over to Data Exchange System and then after to public cloud. Similarly as and when required the encrypted data can be accessed from public cloud and after decryption it can be used by the patient from any place at any time. On contrast to the existing e-Health care system, the proposed c-Health care system is not having any central server to maintain the huge data of patients and neither has it needed any operational expenditure to maintain the huge data. Further, it is of the utmost need that different health organizations must share information of patient, in order to provide him best medical services. In this context, our proposed framework of c-Health care system (Figure 1) is actually a community cloud at which infrastructure is shared by several health organizations. To make the overall system to be more flexible, the concept of SOA has been used. The proposed framework of c-Healthcare system based on SOA principles is shown in Figure 2 and the class diagram of the overall process is shown in Figure 3.

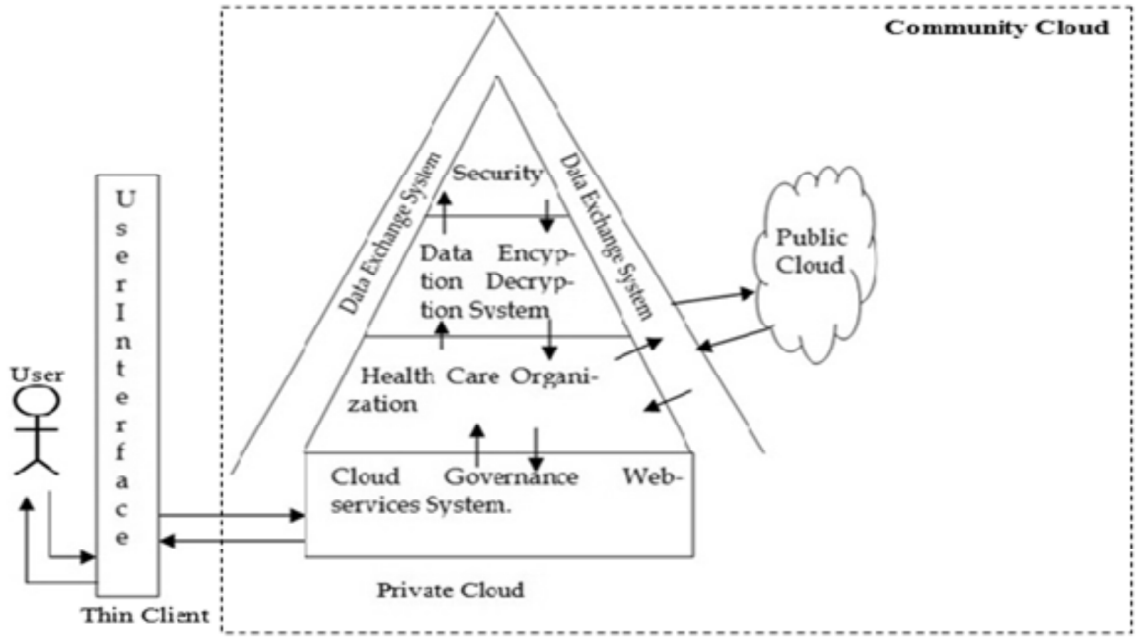

Figure 1: Proposed Framework of c-Health care system

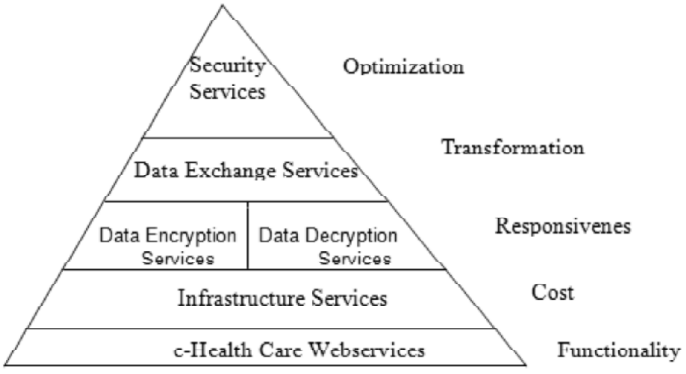

Figure 2: Proposed SOA of Cloud-Governance

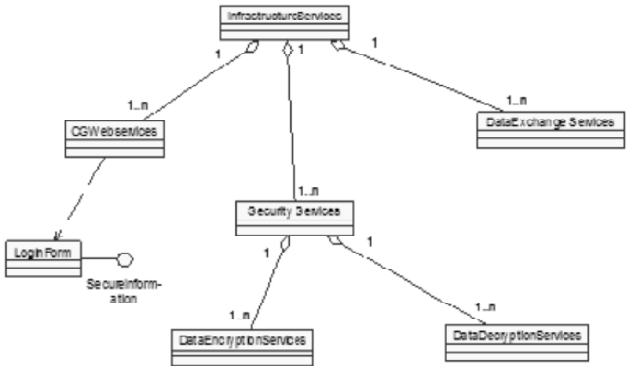

Figure 3: Class Diagram of Cloud based Governance

In our proposed c-Health care system based on SOA, the services can be used by other services. For the interaction among services, the services must be aware of each other. This awareness is achieved through the use of service descriptions. A service description contains the name of the service and the data expected and returned by the service. One service can send message to other service, hence the message is autonomous by nature. The communication among messages is shown in Figure 4. Further, a c-Health care service comprises of a set of steps, that is in other word it encapsulates the entire process logic. The business process layer, service interface layer and application layer of the proposed c-Health care system is shown in Figure 4. In the proposed framework, by implementing standardized service abstraction layers, a loosely coupled relationship also can be achieved between the business and application technology domains of the c-Health care system (Figure 6). Each end only needs an awareness of the other services, therefore allowing each domain to evolve more autonomously. This result is an environment that can better accommodate business and technology-related change, that is organizational agility. Now the next phase involves in taking decision about those process which are candidate to be outsourced to cloud environment. To make the c-Health care system to be more agile, we allocate the bundles of data of patients, process and services to the Infrastructure as a Service(IaaS) of cloud computing (Figure 5).

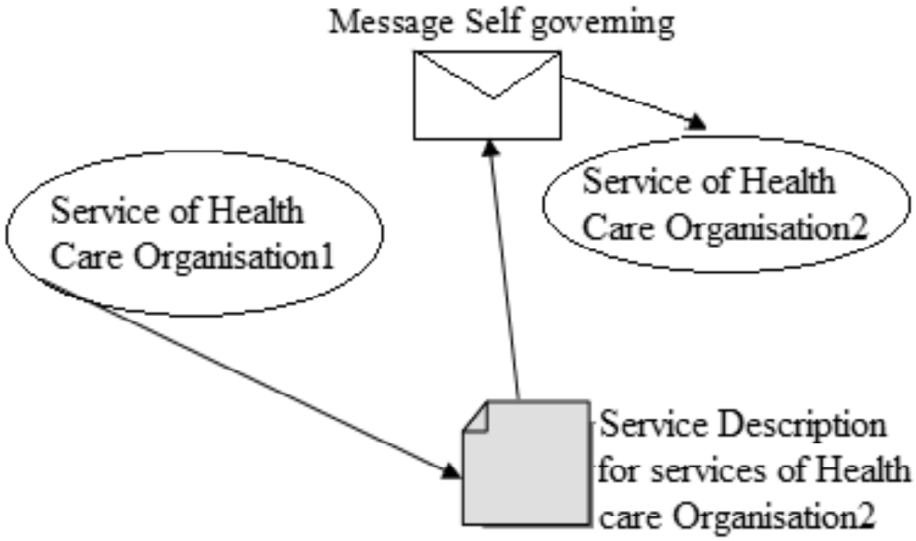

Figure 4: Communication between the services of health care organizations

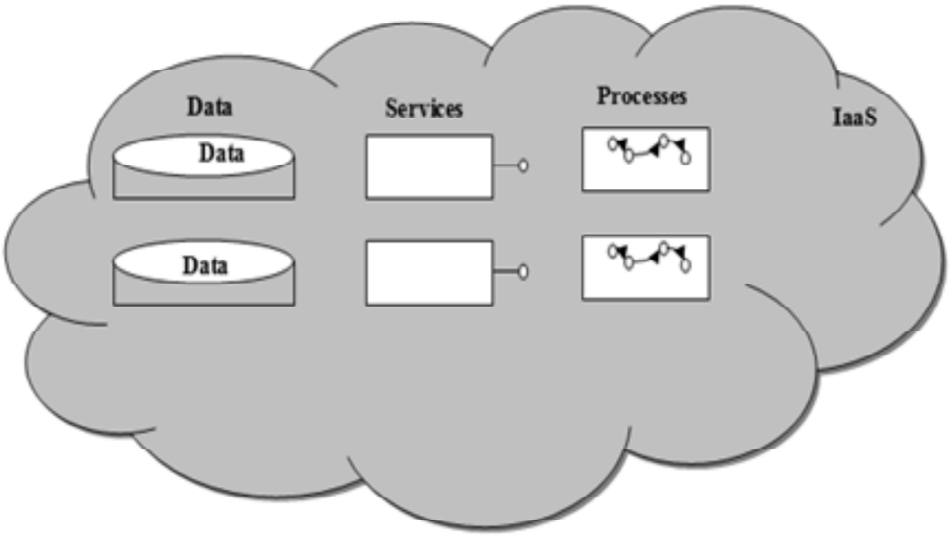

Figure 5: Allocation of data, services and process to cloud computing platform in c-Health care system

Here the agenda of the service is to protect the data of patients in cloud environment from unauthorized user. Here the service contains the entire process logic to provide the technical aspect of data integrity in cloud environment. As already being discussed in the background section of this manuscript that the technical issue of confidentiality of cloud computing addresses the data encryption and decryption, so here the proposed process logic of services addresses data encryption and decryption in cloud environment. The subsequent section of this manuscript has discussed this data security services in details.

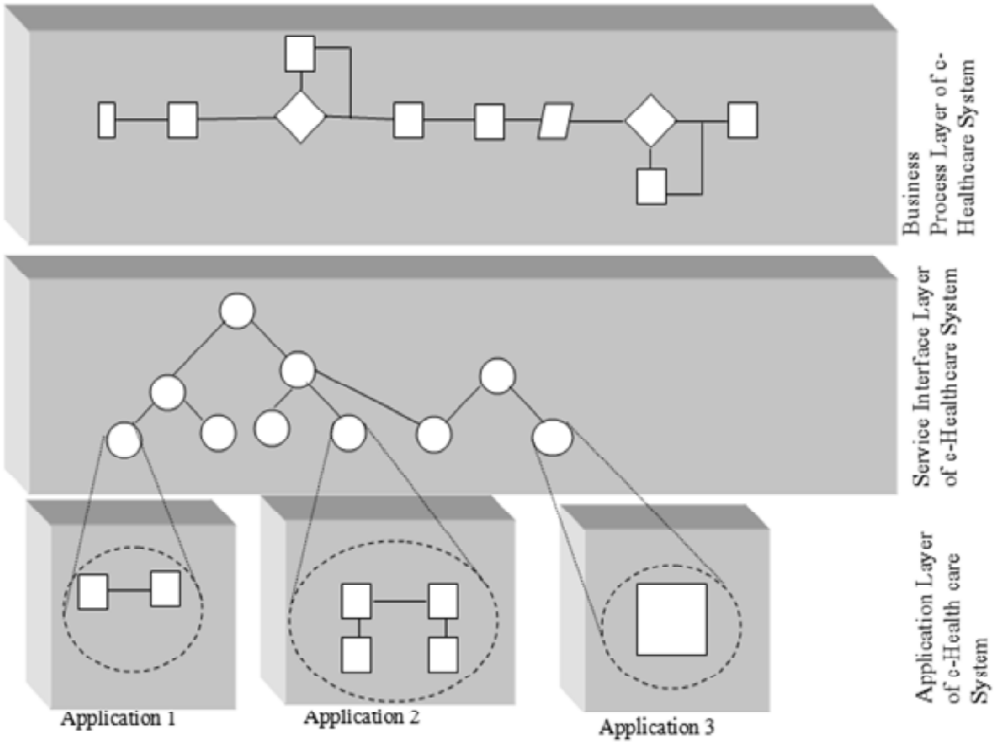

Figure 6: Service interface layer of c-Health care system

V. PROPOSED DATA SECURITY SERVICE

The proposed algorithms consist of two phases, the first phase deals with the exchange of keys, key generation for data encryption and decryption and second phase consists of data encryption and data decryption. The overall technique is based upon Hadamard Matrices. Hadamard matrices were introduced by [25]. A Hadamard matrix of

$$H_1 = [1],\ H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

order n is a matrix, denoted by H_n with the elements of 1, –1, such that $H_n.H_n$ T=n .In The different types of Hadamard matrices are given below:

Figure 7: Different forms of Hadamard Matrix

Further, the Kronecker product (⊗) of Hadamard matrices is given as:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \quad (1)$$

For maintaining high security, we have used challenge – response techniques in our proposed model of Cloud – Health Care system [26]. The above technique is shown in Figure 8.

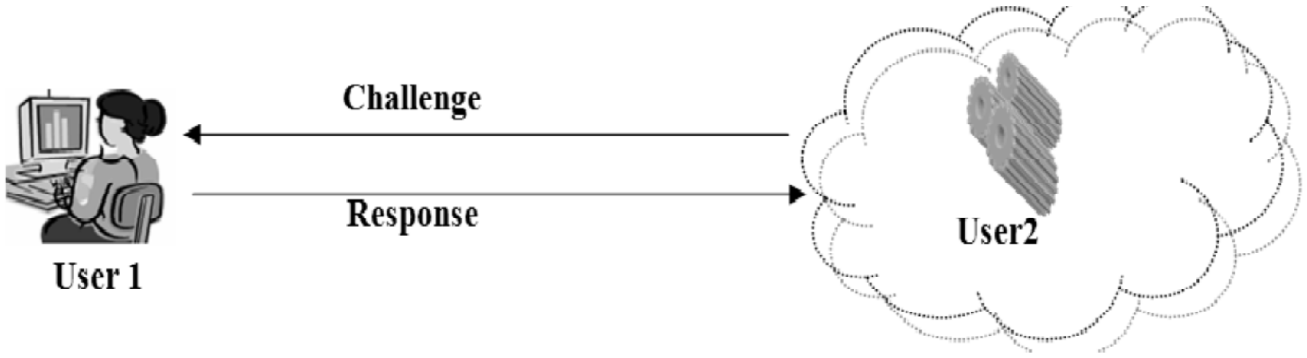

Figure 8: Challenge - Responses

Here, the proposed "Challenge-Response" technique is based upon Hadamard graph. For the sake of simplicity let us consider a Hadamard matrix of order 4, that is, H_4 as shown below:

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Obviously, R1× R2 = 1× 1 + 1× (-1) + 1 ×1 + 1 × (-1) = 0.
Similarly, R2 × R4 = 0, R1× R4 = 0 and so on.

	V1	V2	V3	V4
V1	1	1	1	1
V2	1	-1	1	-1
V3	1	1	-1	-1
V4	1	-1	-1	1

⇒

	V1	V2	V3	V4
V1	1	1	1	1
V2	1	0	1	0
V3	1	1	0	0
V4	1	0	0	1

Figure 9: Adjacency Matrix for Hadamard Matrix by Considering "-1" by "0"

Obviously, R1× R2 = 1× 1 + 1× (-1) + 1 ×1 + 1 × (-1) = 0. Similarly, R2 × R4 = 0, R1× R4 = 0 and so on. Considering "-1" as zero, the Hadamard matrix of the form H4 becomes a combination of "0" and "1" and then we propose a specific directed graph for H4. Here, the Adjacency matrix is shown in Figure 9 and the corresponding directed graph in Figure 11. A directed graph is an order triple G (V, E,η), where V≠ ϕ, V∩ E = ϕ and η: E → V× V) [27].

Now, we propose the proper coloring of the edge of the directed graph, shown in Figure 11, using three colors, Red, Green and Blue, so that no two adjacent edges receive the same color.Where the parameter ± is called embedding intensity and their effect of validity of the algorithm directly is apply after this process, after that apply the inverse wavelet transform to the image for find out watermark image. Further, consider 3-edge color arbitrary graph, shown in Figure 12. Now, we define a rule to join G1(V1,E1,η1) and G2(V2,E2, η2) into G(V,E, η), where V = V1 × V2, as follows:

$$\text{If } \eta 1(e1) = (v_i, v_i) \text{ then } \eta\ (e) = (v_i, v_j),\ \forall\ v_i \in V1,\ \forall v_j \in V2,\ \forall e1 \in E1,\ \forall\ e \in E \quad (2)$$

Here, user1 sends G to user2 in the form of "Challenge". After receiving the "Challenge" from sender, receiver, that is, user 2 cuts G into two 3 - edge colorable Graph G1 and G2 as shown in Figure 13, and then receiver obtains Adjacency Matrix of G1 and G2. After that, receiver replaces all "0" of Adjacency matrix of G1 and G2 by "-1" and consider only that very Graph whose Adjacency Matrix satisfies Hadamard matrix condition, that is,

$$R_i \times R_j = 0,\ \forall\ R_i, R_j \quad (3)$$

Here R_i is the i^{th} row of Hadamard Matrix and Rj is the j^{th} row of Hadamard Matrix. Now, receiver generates the equivalent Hadamard matrix of same order as being sent by user1 and then generates its directed Graph, color its edges properly by using 3-color, and join it with an arbitrary 3-edge colorable Graph using rule (2) and then sends the whole Graph to user as "Response". In this way, both sender and receiver authenticate them, using "Challenge-Response" technique. After authentication, the user1 encrypts their sensitive data, which the user 2 outsource to public cloud.

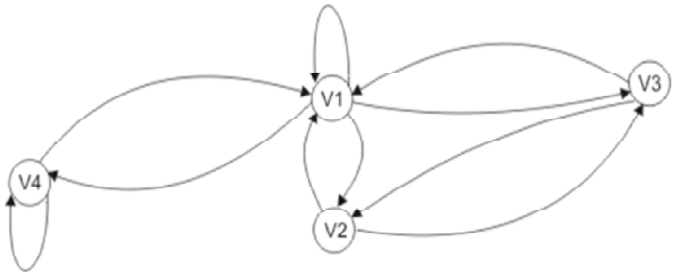

Figure 10: Proposed Directed Graph Representation of Hadamard Matrix

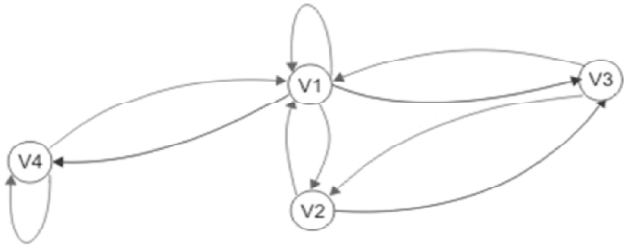

Figure 11: Proposed 3- edge colorable directed Hadamard Graph

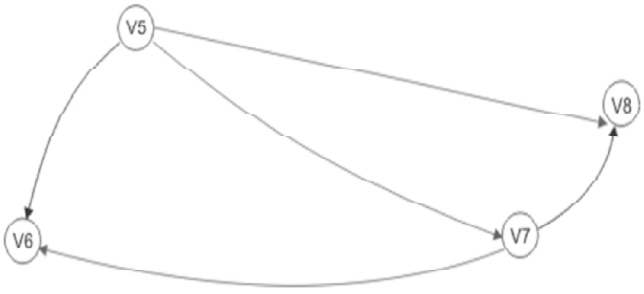

Figure 12: Arbitary 3 – edge colourable directed Graph G2

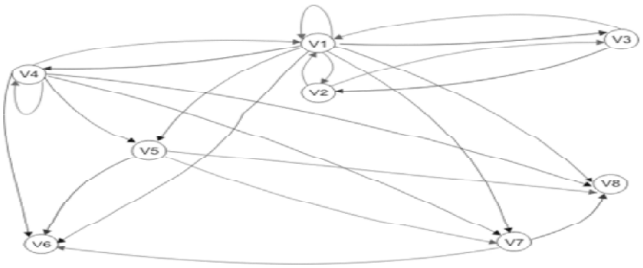

Figure 13: Graph G

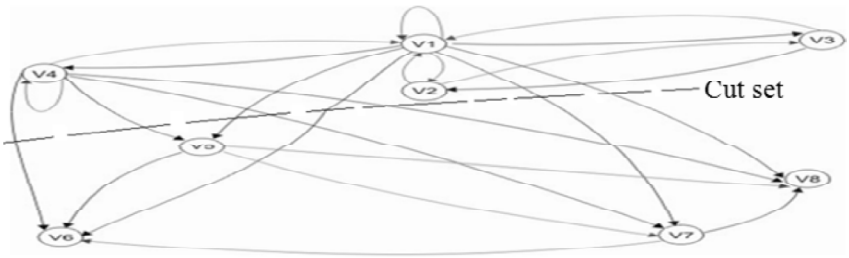

Figure 14: Cut set og Graph G

The proposed Algorithms for Key generation, data Encryption, data Decryption are given in the Algorithm 1, Algorithm 2 and Algorithm 3 respectively. The main featured of the proposed Algorithms are given below:

- User consider an arbitrary Hadamard Matrix, let it is H_k, where k=2n or k= 4n,where n $\in$ N, as "Challenge", then he generates the directed Graph, say, G1 for H_k. Color the edges of G1 using three color Red(R), Green(G) and Blue(B).
- Now User consider any arbitrary Graph, let it is G2. Similarly color its edges using three colors R, G and B.
- Join G1 and G2 using rule 2 to form G. User do not color the joining edges.
- Send G as "Challenge" to service security model.
- User2 cuts the Graph G into two Graphs G1 and G2 by deleting the non-colored joining edges.
- User 2 makes the Adjacency matrix for G1 and G2, then it replaces all "0" (zero) elements of Adjacency matrix by "-1" and then check the Hadamard matrix condition, that is, rule 3.
- The Adjacency matrix which satisfies rule 3 is accepted. In this way, H_k is accepted by user 2.
- Now user 2 finds the equivalent Hadamard matrix of H_k. Let it be H_k and in similar fashion sends H_k as "Response" to user1.
- User after getting H_k, generates the encryption key Hadamard matrix as $H_m = H_k \otimes H_k$, using rule 1.
- User encrypts the Data using the encryption rule as:

  $C \leftarrow M * H_m + d * \text{diagonal}(I_m)$, Here I_m is Identity matrix of order m × m. Further, d is a constant, which is the decimal equivalent of the corresponding row major matrix of H_m after replacing "-1" by "0". To illustrate the point, consider m =2, that is, encryption key Hadamard matrix be H_2. Its equivalent row major matrix be [1 1 1 -1] and then replacing '-1' by '0', and finally one can get [1 1 1 0] and its corresponding decimal equivalent be 14, that is, d = 14.
- The Decryption algorithm is:

  $M \leftarrow \{1/ m\} * [(C - d * \text{diagonal}(I_m))] * H_m^T$.
- Again from the definition of Hadamard Matrix , we can write

$$H_m . H_m^T = m I_m \Rightarrow H_m . \frac{H_m^T}{m} = I_m \Rightarrow H_m . H_m^{-1} = I_m$$

Thus, the above mentioned decryption algorithm can be re-written as follows:

$$M \leftarrow [(C - d * \text{diagonal}(I_m))] * H_m^{-1}, \text{ where } H_m \text{ is the inverse matrix of } H_m$$

So the sensitive data of user is encrypted before it is outsourced to public cloud. The proposed c-Health care system Framework, shown in Figure1 is user 2. User 2 is nothing but a Private Cloud. The user1 is patient that interact to the proposed Private Cloud, shown in Figure 1, through Internet. For this, he first checks that whether communication is taking place between right party or not, for this he uses "Challenge–Response" technique for authentication. They exchange Hadamrd Matrix and using tensor product of two Hadamard matrices, they form their own encryption Hadamard matrix key for data encryption. After that data is encrypted using Algorithm2 and then it is sent to the proposed Private Cloud for outsourcing. Similarly patients can insource their sensitive data from public cloud using the proposed Private Cloud, and then decrypt them, using Algorithm 3.

As per the above discussions, the Key generations Algorithm, Data Encryption Algorithm and Data Decryption Algorithms are given as follows:

A. Algorithm 1

Procedure Generation of Key
Begin
Step 1. Consider a random Hadamard matrix H_k, where k=2n or k= 4n, n∈ N.
Step 2. Generates the directed Graph, say, G1 for H_k. Color the edges of G1 using three colors Red(R), Green (G) and Blue (B).
Step 3. Consider any arbitrary 3-chrometic Graph, let it is G2
Step 4. Join G1 and G2, using rule 2, to get G. Send G as "Challenge".
Step 5. Accept "Response" and then extract Hadamard matrix H_k from it.
Step 6. Obtain Encryption Key Hadamard matrix as: $H_m = H_k \otimes H_k$ using rule 1.
Step 7. End

B. Algorithm 2

Procedure Encryption Algorithm (OriginalMessage)
[Let us suppose the plaintext, entered by user with m letters represented by a vector of length m. Here Hadamard matrix which is denoted as H_m of order m × m, used as Encryption Matrix. Here the plain text is denoted by Original Message]
Begin
Step 1. While (OriginalMessage ! =NULL)
Step 2.[Convert original Message into ASCII Value]
m ← ASCII of (OriginalMessage)
Step 3. [Convert m into binary sequence Message]
M ← binary (m)
Step 4. [Generate d] where d is the decimal equivalent of the corresponding row major matrix of Hm after replacing "-1" by "0".
Step 5. [Encrypt Message M into cipher text]
$C \leftarrow M * H_m + d * diagonal(I_m)$
Here I_m is the Identity matrix of order m × m
Step 6. End

C. Algorithm 3

Procedure DecryptionAlgorithm (C)
Begin
Step 1. [Decrypt decimal Message into ASCII]
$M \leftarrow [(C - d * diagonal \cdot (I_m))] * H_m^{-1}$, Here H_m^{-1} is the inverse matrix of H_m
Step 2. End

VI. ANALYSIS OF ALGORITHM

Due to the combinatorial nature of the formation of Hadamard Matrix by Sylvestor's construction of Hadamard Matrix [25] using the Kronecker product (⊗), obviously the time complexity of Algorithm 1 would be O (2^{2n}). Again, in Algorithm 2, considering the active operations, the conversion of plain text into cipher text would have the time complexity as O (n^2). The time complexity of Algorithm 3 would be O (n^3).

VII. EXPERIMENT SETUP AND RESULT

The overall proposed algorithms have been implemented in a distributed environment, which comprises of master node and slave nodes. The master node schedules the jobs to different slave nodes. The Master Node is Dell Power Edge 1800 with 2 Intel processors of speed 3.40 GHZ with 4 GB RAM and Slave Nodes are Intel core2 Duo PCs. The nodes communicate through a fast local area network. The numerical evaluation of the proposed algorithms are shown in the Figure 15, Figure 16 and Figure 17 respectively.

Analyzing all the results presented above, the following points are inferred on the proposed technique:

- The encryption and decryption time differ approximately linearly in respect to size of the message length.
- The encryption time is smaller as compared to the decryption time.

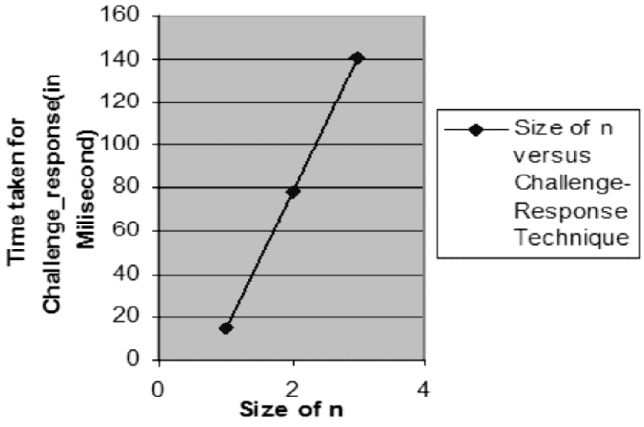

Figure 15: Size of n verses time for Challenge – Response (In Milliseconds)

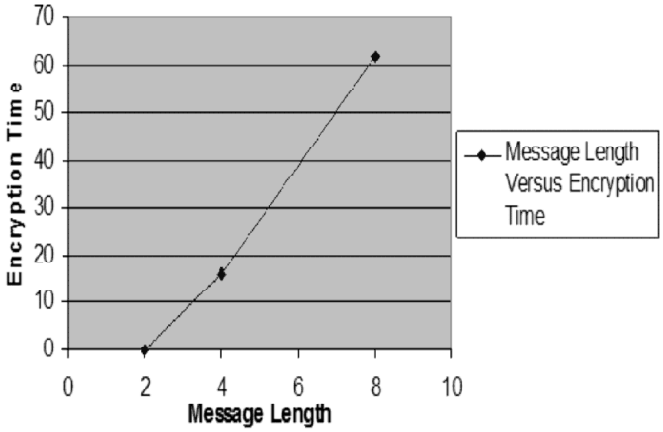

Figure 16: Message Length verses Encryption time (In Milliseconds)

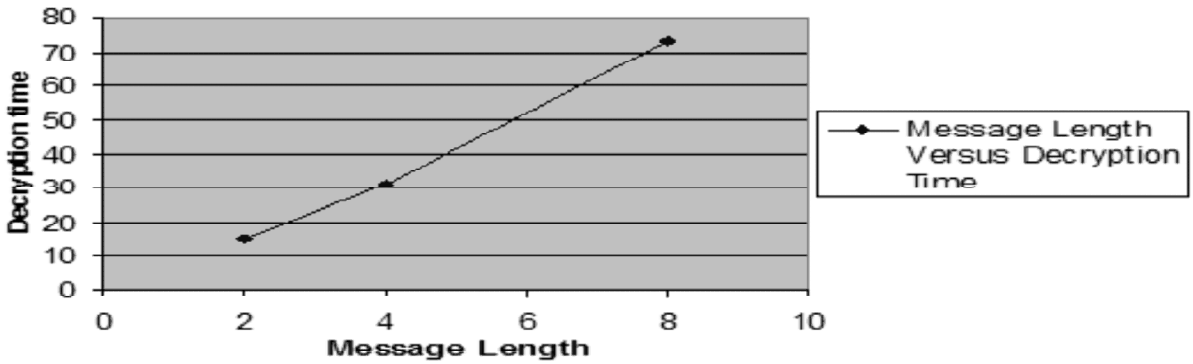

Figure 17: Message Lenth Verses Decryption time (In Millisecond)

VIII. CONCLUSION

Cloud computing is a natural choice for the health care sectors as cloud based e-Health care system, that is cloud-Health care system. The c-Health care system can hike the performance of health care machinery. But one of the major challenges of c-Health care system is security. It is because, in c-Health care system, the sensitive data of the patients would be stored in a place without the knowledge of the sender. In this context, this endeavour has focused only on the security issue of cloud-Healthcare system. Here, the technical issue of confidentiality of cloud computing has been addressed. The sensitive data is stored in cloud storage and prior to storage it is encrypted. Moreover, when encrypted data in cloud environment is accessed then it is first decrypted before use. Here, symmetric crypto system has been used based on Hadamard matrix.

REFERENCES

[1] Zhou, M., Zhang, R., Xie, W.,Qian,W., & Zhou, A. (2010). *Security and privacy in cloud computing: A survey*. Proceedings of the 6th International Conference on Semantics, Knowledge and Grid, China, p.105-112.

[2] Dillon, T., Wu, C., Chang, E., *Cloud Computing: Issues and Challenges*. Proceedings of 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 27-33, 2010.

[3] Rosenblum, J., *Top Five Challenges of Cloud Computing*. Retrieved from *http://www.cloudweaks.com/2012/08/top-five-challenges-ofcloud* computing/, 2012.

[4] Bohn, R.B., Messina J., Liu, F., Tong, J., & Mao, J., *NIST Cloud Computing Reference Architecture*. Proceedings of the 2011 IEEE World Congress on Services, p. 594-596, 2011.

[5] Jansen, W. and Grance, T., *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology (NIST), Special Publication 800-144, U.S. Department of Commerce, USA, pp. 1-70,

[6] Mell, P., What's Special about Cloud Security? *IT Professional, Vol.14*, No. 4, 6-8, 2012.

[7] Brodkin, J., Gartner: Seven cloud-computing security risks. Retrieved online from http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf, 2008.

[8] Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Russell, J., & Potts, H. W.W, Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study. *BMJ*, 2010.

[9] Wainer, J., Campos, C.J.R, Salinas, M.D.U , & Sigulem, D.**,** *Security Requirements for a Lifelong Electronic Health Record System: An Opinion*. Open Med Inform Journal, 160-165, 2008.

[10] Bruce, S., NPfiT failures have left NHS IT stuck eHealth Insider. Retrieved from http://bit.ly/qgE69u , 2011.

[11] Lin, J. et al., *Fine-grained Data Access Control Systems with User Accountability in Cloud Computing*, Proceedings of 2010 IEEE Second International Conference on Cloud Computing Technology and Science, pp. 89-96, 2010.

[12] Zhang, W., & Chen, Q.(2010). *From E-government to C-government via Cloud Computing*. Proceedings of the International Conference on E-Business and E-Government (pp. 679-682)

[13] Gonzalez, N., Miers, C., Redígolo, F., Carvalho, T., Simplicio, M., Näslund, M., & Pourzandi, M., *A quantitative analysis of current security concerns and solutions for cloud computing*. Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science, p. 231-238, 2011.

[14] Che, J., Duan, Y., Zhang, T., & Fan, J., *Study on the security models and strategies of cloud computing*. Proceedings of the International Conference on Power Electronics and Engineering Application, p. 586-593, 2011.

[15] Durbano, J.P., Rustvold, D., Saylor,G., & Studarus, J. Securing the Cloud. In: Antonopoulos, N., Gillam, L.(Eds.) *Cloud Computing: Principles, Systems and Applications, Computer Communications and Networks*, pp. 289-301, London, Springer-Verlag., 2010

[16] Onwubiko, C., Security Issues to Cloud Computing. In Antonopoulos, N., Gillam, L. (Eds.), *Cloud Computing: Principles, Systems and Applications, Computer Communications and Networks* (pp. 271-287). London Springer-Verlag, 2010.

[17] Sengupta, S., Kaulgud, V., & Sharma, V.S., *Cloud Computing Security-Trends and Research Directions*. Proceedings of the IEEE World Congress on Services, pp. 524-531, 2011.

[18] Nepal, S., &and Pathan, M., Editorial. *International Journal of Cloud Computing, Vol. 1*, Nos. 2/3, Inderscience, 101-118, 2012.

[19] Nie, X., & Suo, H., *Security in the Cloud Computing: A Review* Proceeding of the 2nd International Conference on Computer Science and Network Technology, China, pp. 2145-2149, 2012.

[20] Sun, D., Chang, G., Sun, L., & Wang, X., *Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments*. Procedia Engineering, *Vol. 15*, 2852-2856, 2011.

[21] Bernstein, D., & Vij, D., *Intercloud security Considerations*. Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, USA, p. 537-544, 2010.

[22] Abuhussein, A., Bedi, H., & Shiva, S., *Evaluating Security and Privacy in Cloud Computing Services:A Stakeholder's Perspective*. Proceedings of the 7th International Conference for Internet Technology Proceedings of 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012.

[23] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J., *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*. Proceedings of the ACM Workshop on Cloud Computing Security, New York, p. 85-90.

[24] Wooten, R., Klink, R., Sinek, F., Bai, Y., & Sharma, M. (2012), *Design and Implementation of a secure Healthcare Social Cloud System*. Proceedings of 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.

[25] Hadamard, J., Resolution d'une question relative aux determinants'. *Bulletin des Sciences Mathematiques, Vol. 17*, Gauthier-Villars, Paris, 240-246, 1893

[26] Vaquero, L., Rodero-Marino, L., Caceres, J., & Linder, M., *A break in the clouds: towards a cloud definition*. ACM SIGCOMM *Computer Communication Review, Vol. 39*, No. 1, 137-150, 2009.

[27] Harary, F., *Graph Theory*, Narosa Publishing House, India, 1997.