Analysis of Risk Impact in Public Health Care Industry Using Cloud

B.Gayathri[*1] Dr.K.Srinivasa babu[*2]
[*1] Assistant Professor, Department of Computer Science and Engineering
[*2] Professor, Department of Computer Science and Engineering
[*1,2] Nalla Narshima Reddy Group of Institution, Narapally.

***Abstract*— The task of protective Healthcare Data Systems (HDS) from immediate cyber security risks has been interlaced with cloud computing adoption. The information and resources of HDSs are implicitly shared with alternative systems for remote access, higher cognitive process, emergency, and with other fields related to health care. There are various cloud service models which are used in public health care to serve multiple requirements from multiple customers which proves the actuality of cloud computing platform. Within the case of a large number of necessities by multiple stakeholders, various and various cloud models area unit is being adopted across the health care and public health business that defies the important essence of sharing and victimization cloud computing during this domain. The misunderstanding of security is one amongst the key hurdles in the adoption of cloud as an actual normal within the health care and public health sector. During this paper, we demonstrate the similarity of the protection aspects of the cloud computing models, by characteristic the critical assets within the HDS, and by assessing their impact on HDS. We have a tendency to conjointly appraise the danger exposure of the cloud computing models by performing arts and assessment. To the most effective of our information, this can be the primary study of its kind for risk analysis of cloud computing models so as to demonstrate their suitableness for HDS.**

Keywords*— *Risk Analysis, Security, Cyberspace and Healthcare.

I. INTRODUCTION

There has been an incredible growth within the online convenience of digital patient records because of the technological advances in communications. The patient records could contain:

1. Patient personal information, like name, age, address and date of birth;
2. Historical health information like persistent health risks, diseases within the past, the present health condition;
3. Money data like checking account information;
4. Government concessions;
5. Future plans; and
6. Miscellaneous information like the main points of the help required, parking standing, vehicle info, and emergency contact details.

There square measure incentives for the reduction of prices and the improvement of method flow within the digitization of records. The historical records of patients square measure more shared around once they square measure transferred from one building to following or in future examinations.

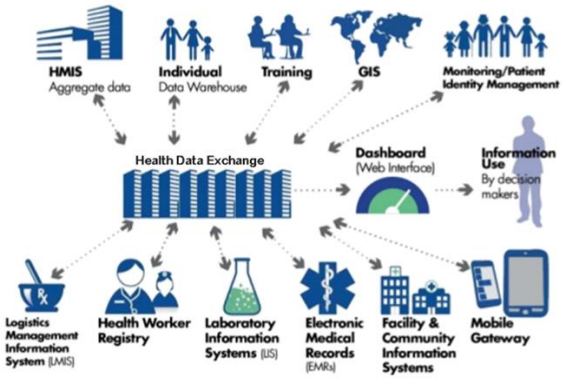

Fig 1: Different sources to Exchange health data

As shown in the Figure there are so many places or data center that are going to exchange health data. From the expansion in technology, the digitization of patients' records and work flow has reached a record high. However, patient information is in high demand by cyber criminals and also most of the attacks were geared toward the aid infrastructure.

In the medical aid sector, cloud computing is taken into account to be a right away remedy, as a result of its ascendable in addition as economical. This sector demands the infrastructure of computing by the means that of quality service levels, however, if the infrastructure isn't designed and maintained properly, it is extremely prone to knowledge breaches [6]. The most church doctrine within the adoption of cloud computing is that the sharing of the chance with the shopper, that is opposite to the client managed risk [7]. Additionally, to risk management, the medical sector is attracted towards cloud computing because of the absence of the other definitive answer which will offer the number of services required and is capable enough to counter the frequent knowledge breaches. many budding firms have offered cloud computing services merchandise that hasn't been adequately qualified for or mapped to the requirements of the purchasers (in this case, the aid industry) like open flow capability, the requirements of connected knowledge, and support for multi-format data during a mutual, and virtualized environment. Cloud computing is classified into 3 service models.

One of the cloud computing models called Infrastructure as a service (IaaS) suits each the service suppliers and the service customers higher because it shares the risks equally among all the parties [9]. The incentives that area unit pictured from cloud adoption area unit, 1) progress improvement, 2) knowledge Security, 3) Infrastructure as a Service, and last 4) Passive supervision of connected medical devices. The improvement of progress is crucial for the people that area unit coping with the public,

particularly with aid organizations thanks to the high chance of the employment of distributed knowledge update models. The host organizations should make sure the handiness and governance of the information to modify dynamic workflows [10]. The sharing of the information will increase the attacked house, and the exposure to a wider audience creates difficulties to solve knowledge security issues. Once the information is held on during a centralized location and is transmitted by applying cruciform data encryption techniques, the reading and maintenance costs can transcend price tolerance thresholds [11].

One of the essences of cloud computing models is that the price sharing model within the technological infrastructure. Different models of infrastructure area unit compared in [12] and also the authors have come back to the conclusion that cloud computing models share the value of operations in addition because of the cost of the risks. The passive direction models, though not widely practiced, are paradigms that we have a tendency to conceive of can prevail within the administration of future medical devices. This remote direction model requires the smallest amount price [13] if applied mistreatment cloud computing models. Therefore, cloud computing exhibits varied benefits, but conjointly present varied problems that can't be unnoticed.

Most noteworthy hurdle within the adoption of cloud computing is the security followed by such alternative matters as isolation. Since cloud computing signifies a relatively novel computing representation at each level, like applications, hosts, network, and data, that successively raises the difficulty of the appliance safety to shift towards Cloud Computing [11], [14]. The indecisions and pressures may cause the adoption of solutions that area unit while not the specified level of safety that's still a priority with cloud computing. Problems associated with cloud security may cause serious threats, for instance, exterior data space for storing, reliance on the public web, multi-tenancy, power problems, and also the interior safety. In distinction to customary technology, cloud computing has several distinct characteristics, as the variety of assets that belong to the cloud contributors are utterly disseminated, numerous and fully virtualized.
Conventional safety measures like distinctiveness, verification and endorsement aren't any longer adequate once intended for cloud computing architectures [15], [16]. Since there are a unit several cloud representations that area unit adopted, with different types and levels of experience utilized to facilitate varied cloud services, cloud computing represents diverse hazards to businesses besides the standard Information Technology (IT) solutions [17]. The design of cloud computing systems involves varied cloud elements that interrelate with one another ultimately to assist the client indeed the specified knowledge a lot of quickly. The user on the forepart solely has to be served, whereas on the backend their area unit large knowledge storage devices, with servers, operating in a distributed manner that produces the cloud.

In this paper, we have a tendency to demonstrate the similarity of the protection aspects of cloud computing models, by characteristic the important assets within the HIS, the threats, and by assessing the impact on the HDS. We have a tendency to lift the review of the connected literature in section 2. The analysis methodology is bestowed in section three and the risk determination techniques in section four. The results and their analysis area unit bestowed in section five and that we conclude the paper in section half-dozen with an outline of our contributions and a discussion of future analysis directions.

II. LITERATURE REVIEW

A typical aid system is shown in Figure two wherever the physical and also the logical sections of the network area unit divided into totally different subnets as per necessities of an aid enterprise. An aid enterprise is well connected to medical analysis backbones, Medicare Advantage Plan (MAP)/MAP Remittance Advice Notice (MRAN) and other aid enterprises on high-speed knowledge links. A Management Information System in HDS provides support to the administrative tasks and is generally unbroken on a separate subnet. The other inheritance systems, i.e., public switched phone network (PSTN), also are connected to the sting routers in a very HDS in a very separate section of the network. In cloud computing, platforms of networking, code infrastructure, and storage are provided as services to level up or level down relying on the claim. Typically, cloud infrastructures area unit classified into three preparation models.

HYBRID CLOUD MODEL

A portion of private cloud that relates to one or many outsourced offerings of a cloud is referred to as hybrid cloud, that is supervised centrally, operates as an unbiased unit, and is limited by a community that is secure [20]. It offers powerful records generation and useful resource usage of both personal and public clouds. Software and information are comfier in a hybrid cloud and therefore it permits a spread of parties for accessing statistics at the internet. The hybrid cloud model also possesses a public structure to combine with similar structures of management. This version explains configuration that combines nearby gadgets like plugged in computers with the offerings of the cloud. The hybrid cloud version additionally encompasses configurations that integrate physical and the virtual related property. For instance, the digital machines deployed at the cloud consume physical assets of routers, bodily servers or in additional hardware like network devices that act like a junk mail filter out or firewall.

Similarly to the cloud computing models, the cloud computing services can be introduced atomically. three essential delivery fashions of cloud offerings are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and software Software-as-a-Service (SaaS). The SaaS can further be divided into software-SaaS, safety-SaaS, and network-SaaS. The SaaS is a `pay-as-you-go' model, provided as a low-cost opportunity to a software program used as software licenses are time shared amongst exceptional users. It lets in the clients of the cloud

services to reduce the software acquisition and preservation fees. The SaaS-based packages are designed for offering support to more than one concurrent user (multi-tenancy) at a time. The security of internet browsers could be very vital because SaaS packages are accessed over the internet thru web browsers. So, diverse strategies for making SaaS applications comfortable should be considered by using information safety officers. Facts safety strategies like Extendable Markup Language for encryption, web services for protection, and Secure Socket Layer, can be applied for effective protection of records over the internet [22]. The cost-added offerings supplied by way of the issuer of cloud computing offerings are divided amongst clients which might be gotten smaller primarily based on a pay-as-you-go model.

The IaaS significantly minimizes want for great preliminary asset and computing hardware like networking devices, servers, as well as processing power. It additionally permits a degree of functional and financial flexibility that is not found in data centers which are inner. When you consider that assets of computing may be released or brought quite a whole lot faster and cost efficiently with collocation services, IaaS is a likable desire for many clients [23].

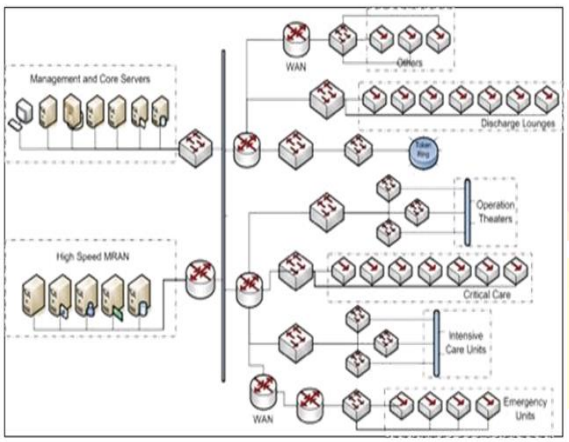

Fig 2: C*loud service support Healthcare Data System*

IaaS in addition to different services that are related allows smooth startups. Many industries focus on their inner capabilities but do no longer positioned tons efforts in handling and provisioning the infrastructure. IaaS absolutely abstracts hardware below it and permits customers for consuming infrastructure as carrier transparently. Cloud possesses a persuasive cost in provisions of expenditure, however, when adopted ``out of the box'', it handiest gives crucial security (e.g., load balancing, perimeter firewall) and those applications that are moving within the cloud would require superior security ranges that the host provides. Depending on the issuer's servers, the model in which software program and tools associated with development are being hosted is known as PaaS. Rather of having any records concerning the backend services, this tends incorporation on an environment of the developer in which a developer wants to establish own packages. Even as looking on the stack, it is one layer over IaaS and above OS (running machine). It presents developers with an entire overdo the improvement technique that gives a whole SDLC control, from collecting necessities, layout coding than exploitation to trying out than a continuance.

III. RESEARCH METHODOLOGY

The risk management system addresses the possibilities, that in future, can also occur and cause disruption to the everyday course of commercial enterprise continuity [26]. But, this definition is not accurate inside the feel that, if the ordinary operation is prone to eavesdropping, in this situation, the normal operation of the organization has to be confined [11]. Parent four describes the tiers in a risk control cycle. The maximum essential principles in danger management are threat evaluation, belongings identification and evaluation, and danger identity.

Table 1: List of assets.

ASSET Name	Perceived value
Healthcare Facility	Very high
Patient trust	Very high
Healthcare staff loyalty and experience	High
Intellectual property	Very high
Personal sensitive data	Very high
Personal data	Medium
Human resource data	High
Service delivery real time services	Very high
Access control	Very high
User directory	Very high
Cloud service	Very high
Management interface APIs	High
Network	High
Physical hardware	Medium

A. RISK ANALYSIS:

In this paper, we use the Operationally Critical Assets Vulnerability Evaluation (OCTAVE) method to identify the risk factors to the normal operating of a task. At the start degree of the chance control technique, we pick out the important assets, coming near threats, and feasible vulnerabilities. In addition to the OCTAVE method, this examine additionally makes use of the Cloud protection Alliance suggestions [28] to hold out the hazard management system. We divide our analysis task into the following steps (subsections B to E).

B. IDENTIFICATION AND EVALUATION:

In this paper, to identify the critical assets in a Healthcare data System we use the ENISA guidelines [29] as given in Table 1. The first step is to identifying and examining critical assets by build threat-based asset profiles. According to the rules ironed out in the literature [30], [31], the assets are assigned a Perceived Value to distinguish them from each other.

C. IDENTIFICATION OF THREAT

Table 2 is constructed from the threats register maintained by the Cloud Security Alliance.

Table 2: CSA identified threats

Security control	ST NO	Security Threat
Data Threats	Thr1	Data Breaches
	Thr2	Data Loss
Network Threats	Thr3	Account Hijacking
	Thr4	Insecure interfaces and APIs
	Thr5	DOS
Cloud Environment	Thr6	Malicious insiders
	Thr7	insufficient due diligence
	Thr8	shared access

BREACHES

A facts breach is the intentional or unintended release of at ease or personal/confidential facts to an untrusted environment [18]. While patient statistics is accessed, considered, shared, or utilized/ processed without authorization or the affected person or the statistics holder, i.e., the HDS administrator, the technique is called a health facts breach. An unintended publicity is exceedingly possibly whilst information like affected person facts is shared amongst HDS with varying security requirements. Frequently this danger is recounted via the affected person thru information disclosure forms. The affected person records breach dangers can be increased because of outsourced services which steer clear of the personnel, logical and bodily controls.

DATA LOSS

Any occasion or manner with consequences in information being deleted, corrupted or made illegible by using a software program, consumer or utility is known as records loss. This consists of ransom ware assaults on HIS, unintentional losses, and deliberate attacks on patient statistics nowadays. Statistics loss is also known as information leakage. It happens whilst the facts owner or the requesting application cannot utilize statistics factors. Facts loss can take region at the same time as data is either in storage or transmitted over the network.

ACCOUNT HIJACKING

A technique by using which they get right of entry to controls related to the user are taken away and are used for malicious purposes by way of an advisory is known as account hijacking. Account hijacking may be achieved on an email, pc, or another account associated with a computing tool or carrier. It's for a kind of identification robbery wherein an unauthorized or malicious pastime is finished by using stolen account statistics.

INSECURE INTERFACES AND APIs

An ordinary cloud purchaser configures, interacts and manages his/her cloud infrastructure via a set of software program interfaces or APIs. The accessibility and security of cloud services rely upon the security of these basic APIs. Those Configurations are shipped at the side of the standard safety controls. If those controls aren't enabled, the configurations of the APIs may be altered and the entire infrastructure may additionally be compromised, e.g., this will happen if relaxed connections are not enabled or applied, and so on.

DoS ATTACK

When the attackers or hackers attempt to prevent legitimate customers from accessing an application or a provider is referred to as Denial of-service attack (DoS). In a DoS assault, immoderate messages are despatched by means of the attacker asking the server or community to authenticate requests having incorrect go back addresses. When the server or community tries to ship the authentication approval, it will not be able to find out the return cope with of the hacker. This situation will reason the server to attend earlier than terminating the connection. When the server terminates the connection, extra authentication messages may be sent by using the hacker with incorrect go back addresses. Consequently, the technique of sending authentication approvals and server waiting will restart, maintaining the server or the community busy and the valid customers can be denied in their offerings.

MALICIOUS INSIDERS

This refers back to the case wherein there's a deliberately misused or unauthorized get entry to a corporation's facts, network, or system by using its former or modern worker, enterprise accomplice or contractor. It's miles achieved in a way that negatively impacts the provision, integrity or confidentiality of the company's belongings or records structures.

INSUFFICIENT DUE DILIGENCE

Every now and then companies may be ignorant of cloud service company's environment, well-known nature of cloud era and related security threats and therefore exhibit insufficient due diligence. HDS directors ought to have cloud and safety professionals in their teams so that the agency can avail their abilities and avoid sudden behaviors from the infrastructure. Without expert information, the adoption to the cloud which may lead to more troubles than benefits.

EXCHANGE ISSUES WITH TECHNOLOGY

One of the key features of cloud computing is multi-tenancy. On this sort of a structure, shared resources are provided to multiple users, to perform scalability. Cloud companies supply their offerings to multiple customers to the percentage the same application, platform, and infrastructure. This joint nature may additionally result in the disclosure of information to other users, and also due to an

unmarried fault, a hacker may want to possibly take a look at all of the different information.

D. VULNERABILITY IDENTIFICATION:

The vulnerability is a flaw or weakness in system protection tactics, layout, implementation, or internal controls that can be exercised (by accident induced or intentionally exploited) and result in a safety breach or a contravention of the system's protection policy [27], [33]. It is vital in a chance assessment procedure to perceive the known vulnerabilities to protect the data and infrastructure from assaults resulting from the recognized vulnerabilities.

E. RISK ASSESSMENT:

In the literature the risk assessment is proposed with a three-step process. The details of the three steps are provided in the following sections:

A. LIKELIHOOD DETERMINATION

In [33], the threat-likelihood is defined as "to derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment". We purpose at determining the breach probability to the crucial assets recognized in table 1. We bear in mind the results from the vulnerability identification wherein every vulnerability is evaluated and assigned a numeric cost and a chance degree. The numeric value degrees from 0.1 to 1.0. A value of 0.1 methods that the chance of a vulnerability being exploited is very low whilst the cost of 1.0 approach that the possibility of a vulnerability being exploited may be very high. The vulnerability chance ranges are defined as very high, high, medium, low and very low. Here, a high stage manner the danger source has excessive motivations or talents to take advantage of certain vulnerability even as a low level suggests the lack of required abilities and incentives to exploit the given vulnerability. Table 4 suggests the mapping of every vulnerability and its probability degree and rate.

B. ANALYSIS IMPACT

All through impact analysis, we examine the loss impact of each asset based totally on its fee. Further, the effect stage is divided into the ranges or severity: very excessive, high, medium, low and very low. These values represent knowledgeable guesses over an extensive range of commonplace cloud deployments and do now not have a precise semantics. In practice, the chance degrees are related to the values of belongings where an excessive price asset can also have a high impact to a particular scenario whilst a low level asset may additionally have a low impact. Every asset is given an impact value that Levels from 1 to 5 as shown in table 3.

Table 3: The perceived values of effect and its corresponding numeric scale.

Perceived value	Impact value
very high	5
High	4
Medium	3
Low	2
Very low	1

Table 3 suggests the effect of threats (ti) in non-safety configured public clouds. From Table 3, this study estimates the fee of an asset primarily based on how a hazard influences given property. Then, it calculates the total value of every asset as follows:

The impact factor of a threat event = Dividing the total of the impact factors of affected assets (Asti) / the number of affected assets (n).

Assuming that the breaches in HDS have a Bayes' theorem (Bayesian), the reparative breaches can be modeled as

$$\mu = \beta_0 + \beta_1 + t_1 + \beta_2 t_2 + \beta_3 t_3 + \ldots + \beta_n t_n$$

$$\beta 0 \sim N(\log(Sn), 1)$$

$$\beta i \sim N\left(0, \frac{1}{Var[t_i]}\right)$$

$$\tau \sim \text{Gamma}\ (1,1)\ \text{as randomize the variable}$$

the following Operationally Critical Assets Vulnerability Evaluation method from, estimate the risk exposure as follows

$$Sn \sim Lognormal\left(\sum_{i=1}^{i=n}(\mu_i, \tau)\right)$$

Table 4: non-security configured cloud Impact of Threats

ST	AFFECTED ASSET	IMPACT FACTOR
Thr1	A1,A2,A4,A5,A6,A7	4.1
Thr2	A1,A2,A5,A6,A7,A12	4.3
Thr3	A1,A2,A5,A6,A7,A12,A23	3.5
Thr4	A1,A2,A5,A6,A7	4
Thr5	A1,A2,A9,A10,A16	4.3
Thr6	A1,A2,A3,A4,A5,A6,A7,A8	4.1
Thr7	A5,A6,A7	3.3
Thr8	A1,A5,A6,A8,A9,A10,A16	4

We advocate the impact component of a danger event as the sum of the effect of all the property that have an effect on the given danger, then divide it by using variety of affected belongings as shown in table 4 as graphically represented in discern 5. From table 4, impact factor which is also known as danger exposure may be used as, for instance, a risk having an effect component greater than four may be considered as having a intense or catastrophic unfavorable effect on organizational operations, organizational property, or people. A hazard with an effect factor among and four is considered as having a extreme detrimental impact on organizational operations, organizational assets, or people. A threat with an impact factor of much less than will have a

limited damaging impact on organizational operations, organizational belongings, or people.

C. DETERMINATION OF RISK

We map the countermeasures for every risk, which we identified for every asset in table 4. This helps slender down the threats space. But, the countermeasures against every chance are those which might be reported inside the literature [3], [38][40]. It's far quite in all likelihood that more powerful countermeasures can also exist for each hazard that has been highlighted in these studies. We aim at investigating the pleasant desirable set of countermeasures in future paintings. A degree of hazard publicity is furnished in table eight. In table 4, we provide a comparison among non-security configured and protection configured public clouds. From Table nine, we see those impact elements are significantly reduced by applying counter measurements. In figure 6, we present our findings from an empirical evaluation of protection configured cloud infrastructures and non-security configured infrastructures.

The determine indicates that the general effect of threats is decrease than the effect of threats in non-security configured clouds. By non-safety configured clouds, we seek advice from hybrid clouds, the cloud computing environments where protection practices are not taken into consideration as a primary challenge.

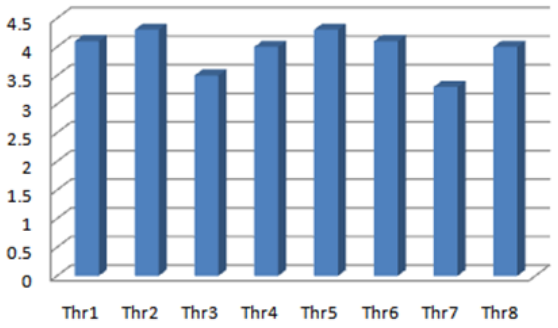

Figure 3: Risk exposure of the identified threats

Table 5: security configured cloud Impact of Threats

ST	AFFECTED ASSET	Impact Factor
Thr1	A1,A2,A4,A5,A6,A7	1.83
Thr2	A1,A2,A5,A6,A7,A12	2
Thr3	A1,A2,A5,A6,A7,A12,A23	1.71
Thr4	A1,A2,A5,A6,A7	1.8
Thr5	A1,A2,A9,A10,A16	3.4
Thr6	A1,A2,A3,A4,A5,A6,A7,A8	1.5
Thr7	A5,A6,A7	1
Thr8	A1,A5,A6,A8,A9,A10,A16	1.86

The effects are opposite to the commonplace false impression that a non-public cloud infrastructure can be cozier than a public cloud infrastructure, in the standard. An essential aspect in both of the paradigms, this is public and private clouds, is the presence of key safety countermeasures. We plan to offer a further account of those key security countermeasures in our destiny work. Those countermeasures do now not always make a public cloud infrastructure an outright preference for the healthcare enterprises. The emphasis is multiplied on authentication, authorization, and accounting manipulate, so the proper people can be capable of access data. The data possession and rendering problems also are of sizeable importance. Some other undertaking of public clouds is the juristic and cyber regulation approximately the hosting of data in public clouds.

Table 6: impacts on different configured cloud

ST	Impacts of Non-Security configured cloud.	Impacts of Security configured cloud.
Thr1	4.1	1.83
Thr2	4.3	2
Thr3	3.5	1.71
Thr4	4	1.8
Thr5	4.3	3.4
Thr6	4.1	1.5
Thr7	3.3	1
Thr8	4	1.86

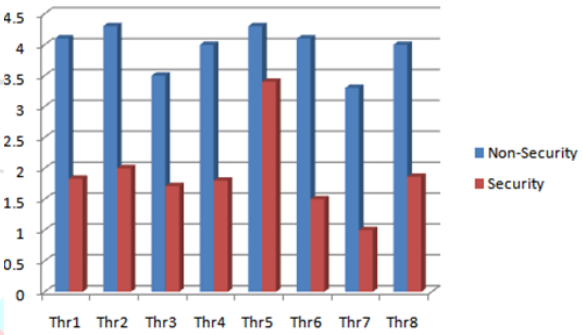

Fig 3: security and non-security configured cloud

VI. CONCLUSION

An increasing variety of risks to digital healthcare enterprise due to the persistent threats stimulates the acquisition and improvement of recent generation. Cloud computing is seems to be a quick fix too many safety vulnerabilities within the healthcare and public health region which might be mentioned in this paper. Notwithstanding their benefits, this paper provides the findings that highlight the hurdles in the adoption of cloud computing solutions. Furthermore, applicable risk factors are identified and classified, which in the end sluggish down the adoption of cloud computing within the medical zone. In addition, the belongings in a healthcare system and their criticality that results in the overall integrity of HDS are identified, and the vulnerabilities are tabled. Such info helps us determine the effect of a breach and risk exposure of the additives. The presented analysis demonstrates that using cloud computing environments can reduce the said vulnerabilities and alleviate the threats to the integrity of HDS.

REFERENCES

[1] K. Saleem, Z. Tan, andW. Buchanan, ``Security for cyber-physical systems in healthcare," in Health 4.0: How Virtualization and Big Data are Revolu- tionizing Healthcare, C. Thuemmler and C. Bai, Eds., Cham, Switzerland:Springer, 2017, pp. 233_251.

[2] J. Al-Muhtadi, B. Shahzad, K. Saleem, W. Jameel, and M. Orgun,``Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment,"Health Informat. J., pp. 1_15, Apr. 2017.[Online].Available: http://journals.sagepub.com/doi/full/10.1177/1460458217706184

[3] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, ``Ideas and challenges for securing wireless implantable medical devices: A review," IEEE Sensors J., vol. 17, no. 3, pp. 562_576, Feb. 2017.

[4] K. Saleem et al., ``Survey on cybersecurity issues in wireless mesh networks based eHealthcare," in Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Sep. 2016, pp. 1_7.

[5] H. Journal, ``Summary of September 2017 healthcare data breaches," HIPAA J., Oct. 2017. [Online]. Available: https://www.hipaajournal.com/september-2017-healthcare-data-breaches/

[6] H. S. Lamba and G. Singh. (2011). ``Cloud Computing Future Framework for e-management of NGO's." [Online]. Available: https://arxiv.org/abs/1107.3217

[7] G. Singh, S. Sood, and A. Sharma, ``CM-measurement facets for cloud performance," Int. J. Comput. Appl., vol. 23, no. 3, pp. 37_42, 2011.

[8] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, ``NIST cloud computing reference architecture," in Proc. IEEE World Congr. Services (SERVICES), Jul. 2011, pp. 594_596.

[9] J. Aikat et al., ``Rethinking security in the era of cloud computing," IEEE Security Privacy, vol. 15, no. 3, pp. 60_69, Jun. 2017.

[10] H. Liu, D. Xu, and H. K. Miao, ``Ant colony optimization based service _ow scheduling with various QoS requirements in cloud computing," in Proc. 1st ACIS Int. Symp. Softw. Netw. Eng., 2011, pp. 53_58.

[11] J. Chaudhry, U. Qidwai, M. H. Miraz, A. Ibrahim, and C. Valli, ``Data security among ISO/IEEE 11073 compliant healthcare devices through statistical _ngerprinting," presented at the 9th IEEE-GCC Conf. Exhib. (GCCCE), Manama, Bahrain, May 2017.

[12] Z. Mahmood, ``Cloud computing technologies for open connected government," in Cloud Computing Technologies for Connected Government. Hershey, PA, USA: IGI Global, 2016, pp. 1_14.

[13] A. M. AlZadjali, A. H. Al-Badi, and S. Ali, ``An analysis of the security threats and vulnerabilities of cloud computing in oman," in Proc. Int. Conf. Intell. Netw. Collaborat. Syst., 2015, pp. 423_428.

[14] D. G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, ``Security analysis in the migration to cloud environments," Future Internet, vol. 4, no. 2, pp. 469_487, 2012.

[15] W. Li and L. Ping, ``Trust model to enhance security and interoperability of cloud environment," in Proc. IEEE Int. Conf. Cloud Comput., Dec. 2009, pp. 69_79.

[16] J. A. Chaudhry and U. A. Qidwai, ``On critical point avoidance among mobile terminals in healthcare monitoring applications: Saving lives through reliable communication software," in Proc. IEEE Conf. Open Syst. (ICOS), Oct. 2012, pp. 1_5.

[17] CSA Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Secur. Alliance, Seattle, WA, USA, 2017.

[18] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, ``Security and privacy challenges in cloud computing environments," IEEE Security Privacy, vol. 8, no. 6, pp. 24_31, Nov./Dec. 2010.

[19] Enterprise Cloud Computing: Transforming IT, Platform Comput. Inc, Markham, ON, Canada, Jul. 2009.

[20] Demystifying the Cloud: Important Opportunities, Crucial Choices, Global Netoptex Incorporated, San Jose, CA, USA, 2009, pp. 4_14. [Online]. Available: http://www.gni.com and http://hosteddocs.ittoolbox.com/gni_demystifyingthecloud_november2009.pdf

[21] M. Almathami, ``Service level agreement (SLA) based risk analysis in cloud computing environments," M.S. thesis, Dept. Comput. Secur., Rochester Inst. Technol., Rochester, NY, USA, 2012.

[22] S. Subashini and V. Kavitha, ``A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1_11, 2011.

[23] J. Brodkin, ``Gartner: Seven cloud-computing security risks," in Proc.Infoworld, 2008, pp. 1_3.

[24] A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, ``What's inside the cloud? An architectural map of the cloud landscape," in Proc. ICSE Workshop Softw. Eng. Challenges Cloud Comput., 2009, pp. 23_31.

[25] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio ``Security issues in cloud environments: A survey," Int. J. Inf. Secur., vol. 13, no. 2, pp. 113_170, Apr. 2014.

[26] I. Foster, Y. Zhao, I. Raicu, and S. Lu, ``Cloud computing and grid computing 360-degree compared," in Proc. Grid Comput. Environ. Work- shop (GCE), 2008, pp. 1_10.

[27] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, ``An analysis of security issues for cloud computing," J. Internet Services Appl., vol. 4, no. 1, p. 5, Feb. 2013.

[28] The Notorious Nine: Cloud Computing Top Threats in 2013, Cloud Secur. Alliance, Seattle, WA, USA, 2013.

[29] D. Catteddu, ``Cloud Computing: Bene_ts, risks and recommendations for information security," in Web Application Security. Cham, Switzerland: Springer, 2010, p. 17.

[30] Cloud Computing Risk Assessment, Eur. Union Agency Netw. Inf. Secur., Heraklion, Greece, Nov. 2009.

[31] J. Lloret, M. Garcia, J. Tomas, and J. J. Rodrigues, ``Architecture and protocol for intercloud communication," Inf. Sci., vol. 258, pp. 434_451, Feb. 2014.

[32] N. Ahmed and A. Abraham, ``Modeling security risk factors in a cloud computing environment," J. Inf. Assurance Secur., vol. 8, no. 6, pp. 279_289, Dec. 2013. [Online]. Available: www. mirlabs.net/jias/index.html

[33] G. Stoneburner, A. Goguen, and A. Feringa, ``Risk management guide for information technology systems," in Proc. Inf. Syst. Secur. Risk Model_RC Model, 2004, p. 4, N. SP800.

[34] B. Grobauer, T. Walloschek, and E. Stocker, ``Understanding cloud computing vulnerabilities," IEEE Security Privacy, vol. 9, no. 2, pp. 50_57, Mar./Apr. 2011.

[35] A. Mehmood, H. Song, and J. Lloret, ``Multi-agent based framework for secure and reliable communication among open clouds," Netw. Protocols Algorithms, vol. 6, no. 4, pp. 60_76, 2014.

[36] 36. E. Cayirci, A. Garaga, A. Santana, and Y. Roudier, ``A cloud adoption risk assessment model," in Proc. IEEE/ACM 7th Int. Conf. Utility Cloud Comput. (UCC), Dec. 2014, pp. 908_913.

[37] J. Jacobs, ``Analyzing ponemon cost of data breach," Data Driven Secur., Dec. 2014. [Online]. Available: http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/

[38] R. Lacuesta, J. Lloret, S. Sendra, and L. Peñalver, ``Spontaneous ad hoc mobile cloud computing network," Sci. World J., vol. 2014, Aug. 2014, Art. no. 232419.

[39] J. Lloret, S. Sendra, J. M. Jimenez, and L. Parra, ``Providing security and fault tolerance in P2P connections between clouds for mHealth services," Peer-to-Peer Netw. Appl., vol. 9, no. 5, pp. 876_893, 2016.

[40] R. Kamatchi, K. Ambekar, and Y. Parikh, ``Security mapping of a usage based cloud system," Netw. Protocols Algorithms, vol. 8, no. 4, pp. 56_71, 2017.