IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 16, 2017, accepted September 14, 2017, date of publication February 14, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2805919

Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry

HINA ABRAR[1], SYED JAWAD HUSSAIN[2], JUNAID CHAUDHRY[3,4], (Senior Member, IEEE), KASHIF SALEEM[5,6], MEHMET A. ORGUN[6], (Senior Member, IEEE), JALAL AL-MUHTADI[5,7], AND CRAIG VALLI[4]

[1]Department of Computer Science and Engineering, HITEC University, Taxila 47120, Pakistan
[2]Department of Computer Science and Information Technology, The University of Lahore, Lahore 53710, Pakistan
[3]College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ 86305, USA
[4]Security Research Institute, Edith Cowan University, Joondalup, WA 6027, Australia
[5]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia
[6]Department of Computing, Macquarie University, Sydney NSW 2109, Australia
[7]College of Computer and Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia

Corresponding author: Kashif Saleem (ksaleem@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, Riyadh, Saudi Arabia, through the International Research Group Project under Grant IRG14-07B.

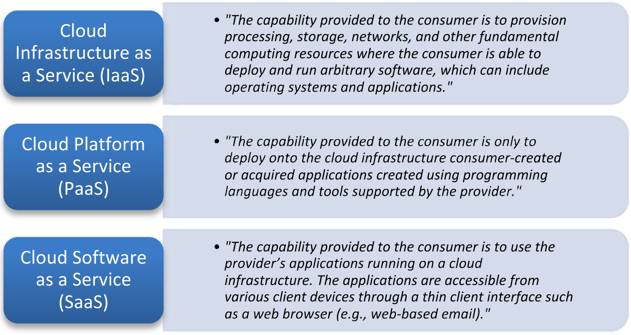
ABSTRACT The task of protecting healthcare information systems (HIS) from immediate cyber security risks has been intertwined with cloud computing adoption. The data and resources of HISs are inherently shared with other systems for remote access, decision making, emergency, and other healthcare related perspectives. In the case of a multitude of requirements by multiple stakeholders, various, and diverse cloud models are being adopted across the healthcare and public health industry, which defies the real essence of sharing and using cloud computing in this domain. The misconception of security is one of the key hurdles in the adoption of cloud as a de facto standard in the healthcare and public health sector. In this paper, we demonstrate the similarity of the security aspects of the cloud computing models, by identifying the critical assets in the HIS, and by assessing their impact on the HIS. We also evaluate the risk exposure of the cloud computing models by performing a critical analysis. To the best of our knowledge, this is the first study of its kind for risk analysis of cloud computing models in order to demonstrate their suitability for the HIS.

INDEX TERMS Clouds, cyberspace, public healthcare, risk analysis, security.

I. INTRODUCTION

There has been a tremendous growth in the online availability of digital patient records due to the technological advances in communications. The patient records may contain: 1) patient personal data, such as name, age, address and date of birth; 2) historical health data such as the persistent health risks, diseases in the past, the current health condition; 3) financial data such as bank account information; 4) government concessions; 5) Friend of a Friend (FoaF) information such as related-to, lives close-to; 6) future plans; and 7) miscellaneous information such as the details of the assistance required, parking status, vehicle information and emergency contact details. There are incentives for the reduction of costs and the optimization of process flow in the digitization of records. The historical records of patients are further shared around when they are transferred from one healthcare facility to the next or in future examinations. From the growth in technology, the digitization of patients' records and work flows has reached a record high. However, patient data is in high demand by cyber criminals and the most of the attacks were aimed at the healthcare infrastructure [1]–[4]. With patients' lives often depending on connected systems, it is critical that immediate solutions are found. Recently, the incidents reported in the month of September 2017 by HIPAA Journal [5] shows that 76.81% of health information with the number of 363,364 records were exposed. In fact, since its infancy, the digital healthcare industry has faced crippling threats in the form of ransomware, information theft, and records compromise.

In the medical healthcare sector, cloud computing is considered to be an immediate remedy, because it is scalable as well as economical. This sector demands the infrastructure


Cloud Infrastructure as a Service (IaaS)
Cloud Platform as a Service (PaaS)
Cloud Software as a Service (SaaS)

- *"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications."*
- *"The capability provided to the consumer is only to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider."*
- *"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email)."*

FIGURE 1. Cloud service models.

of computing by the means of quality service levels, but if the infrastructure is not configured and maintained properly, it is highly vulnerable to data breaches [6]. The main tenet in the adoption of cloud computing is the sharing of the risk with the client, which is opposite to the customer managed risk [7]. In addition to risk management, the medical sector is attracted towards cloud computing due to the absence of any other definitive solution that can provide the level of services required and is capable enough to counter the frequent data breaches. Several budding companies have offered cloud computing services products that have not been adequately qualified for or mapped to the needs of the customers (in this case, the healthcare industry) such as open flow capability, the needs of connected data, and support for multi-format data in a mutual, and virtualized milieu. Cloud computing is categorized into three service models [8] as illustrated in Figure 1.

One of the cloud computing models known as Infrastructure as a Service (IaaS) suits both the service providers and the service customers better as it shares the risks equally among all the parties [9]. The incentives that are envisioned from cloud adoption are, 1) Workflow Optimization, 2) Data Security, 3) Infrastructure as a Service, and lastly 4) Passive supervision of connected medical devices. The optimization of workflow is essential for the people who are dealing with the public, especially with healthcare organizations because of the high probability of the use of distributed data update models. The host organizations must ensure the availability and governance of the data to enable dynamic workflows [10]. The sharing of the data increases the attack space, and the exposure to a wider audience creates difficulties to solve data security problems. When the data is stored in a centralized location, and is transmitted by applying symmetric data encryption techniques, the deployment and maintenance costs will go beyond cost tolerance thresholds [11].

One of the essences of cloud computing models is the cost sharing model in the technological infrastructure. Different models of infrastructure are compared in [12] and the authors have come to the conclusion that cloud computing models share the cost of operations as well as the cost of the risks. The passive supervision models, although not widely practiced, are a paradigm that we envisage will prevail in the administration of future medical devices. This remote supervision model requires the least cost [13] if applied using cloud computing models.

Therefore, cloud computing exhibits numerous advantages, but also presents various issues that cannot be ignored. Most noteworthy hurdle in the adoption of cloud computing is the security followed by such other matters as isolation. Since, cloud computing signifies a comparatively novel computing representation at every level, like applications, hosts, network, and data, that in turn raises the issue of the application safety to shift towards Cloud Computing [11], [14]. The indecisions and pressures could cause the adoption of solutions that are without the required level of safety that is still a concern with cloud computing. Issues related to cloud security could cause serious threats, for example, exterior data storage space, reliance on public Internet, multi-tenancy, power issues, and the interior safety. In contrast to customary technology, cloud computing has many distinct characteristics, as the range of assets that belong to the cloud contributors are completely disseminated, diverse and entirely virtualized. Conventional safety measures such as distinctiveness, verification, and endorsement are no longer adequate when intended for cloud computing architectures [15], [16].

Since there are many cloud representations that are adopted, with different types and levels of expertise utilized to facilitate numerous cloud services, cloud computing represents diverse hazards to businesses besides conventional Information Technology (IT) solutions [17]. The architecture of cloud computing systems involves numerous cloud components that interrelate with each other ultimately to help the client in acquiring the required data more quickly. The user on the front end only needs to be served, whereas on the backend there are massive data storage devices, with servers working in a distributed manner that makes the cloud.

In this paper, we demonstrate the similarity of the security aspects of cloud computing models, by identifying the critical assets in the HIS, the threats, and by assessing the impact on the HIS. We present the review of the related literature in section 2. The research methodology is presented in section 3 and the risk determination techniques in section 4. The results and their analysis are presented in section 5 and we conclude the paper in section 6 with a summary of our contributions and a discussion of future research directions.

II. LITERATURE REVIEW

A typical healthcare information system is shown in Figure 2 where the physical and the logical sections of the network are divided into different subnets as per requirements of a healthcare enterprise. A healthcare enterprise is well connected to medical research backbones, Medicare Advantage Plan (MAP)/MAP Remittance Advice Notice (MRAN), and other healthcare enterprises on high speed data links. A Management Information System in HIS provides support to the administrative tasks and is normally kept on a separate subnet. The other legacy systems, i.e., public switched telephone network (PSTN), are also connected to the edge routers in a HIS in a separate section of the network. In cloud computing,

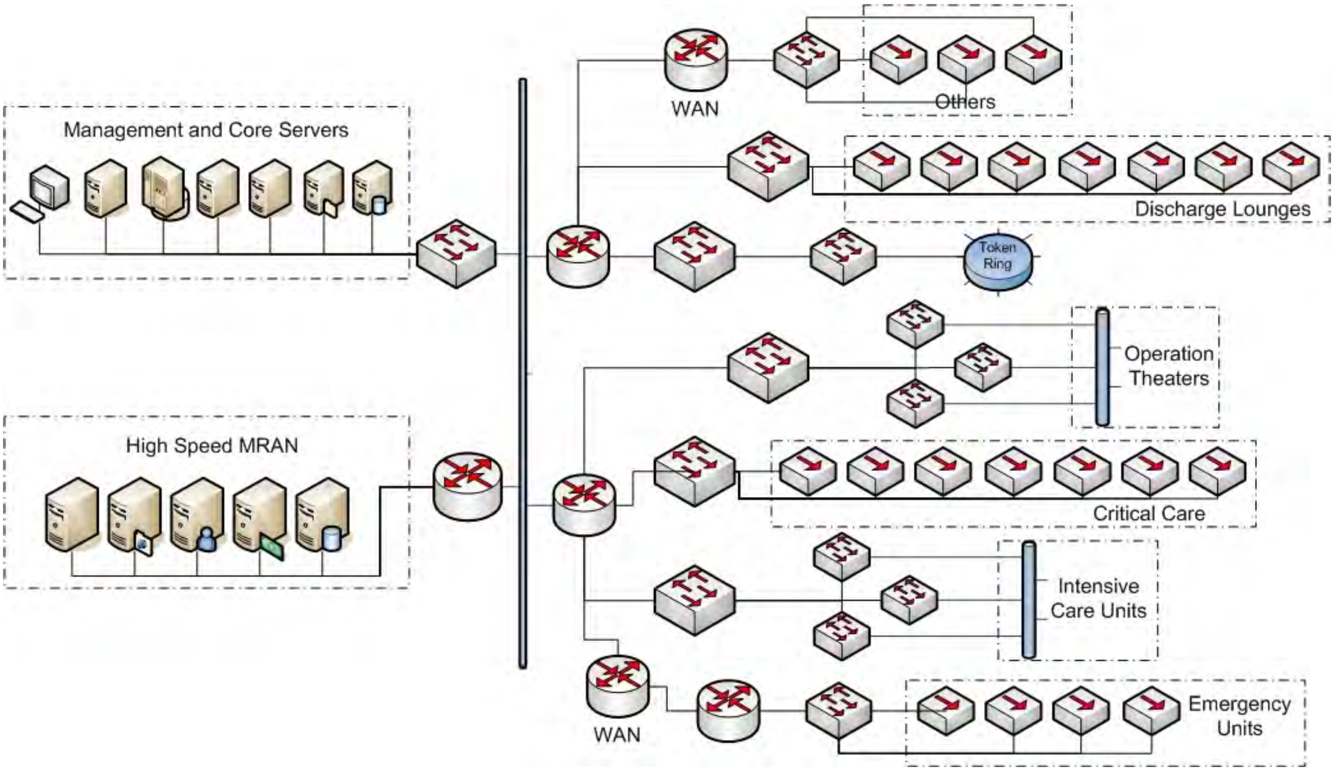


FIGURE 2. Healthcare Information System (HIS) with cloud service support.

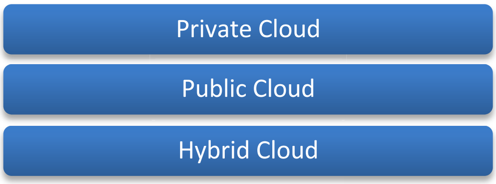


FIGURE 3. Cloud deployment models.

platforms of networking, software infrastructure plus storage is provided as services to level up or level down depending on claim. Typically, cloud infrastructures are classified into three deployment models as presented in Figure 3.

A. PRIVATE CLOUD MODEL

The term "*private clouds*" is coined by cloud services vendors that is used for cloud computing for confidential networks. In other words, the cloud infrastructure is not shared with the others and is reserved for only one client. The cloud purveyor provides virtual applications and scalable resources that are joined collectively and are available to cloud consumers for using and sharing through their own outbound channels. Private cloud is different from public cloud in the sense that the organization itself supervises all applications and sources of the cloud that is like functionality

of an Intranet. It is a common conception that the operation on a private cloud is more secured than a public cloud due to its limited exposure [18].

B. PUBLIC CLOUD MODEL

Public cloud is based on a customized conventional logic whereby methods and techniques assume a self-serviced and fine-grained foundation on the Internet, by means of web services/applications, from third-party contributors. It is based on a pay-as-you-go model that is adjustable enough for catering spikes in demand [19]. Other cloud models are more secure than public cloud since this model of cloud puts an extra load to ensure that every data item accessed and application on public cloud is never manipulated by malevolent attacks.

C. HYBRID CLOUD MODEL

Portion of private cloud that relates to one or many outsourced services of cloud is called hybrid cloud, that is supervised centrally, operates as an independent unit, and is restricted by a network that is secure [20]. It offers effective information technology and resource utilization of both private and public clouds. Application and data are more secure in a hybrid cloud and hence it permits a variety of parties for accessing information on the Internet. The hybrid cloud model also possesses a public architecture to integrate with further systems of management. This model explains configuration that combines local devices like plugged in computers with the services of the cloud. The hybrid cloud model also encompasses configurations that combine physical and the virtual associated assets. For example, the virtual machines deployed on the cloud consume physical resources of routers, physical servers or further hardware like network devices that act like a spam filter or firewall.

In addition to the cloud computing models, the cloud computing services may be delivered atomically. Three major delivery models of cloud services are: Software-as-a-Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) [21] as illustrated in Figure 1. The SaaS can further be divided into application-SaaS, Security-SaaS, and network-SaaS. The SaaS is a 'pay-as-you-go' model, offered as a low-cost alternative to software usage as software licenses are time shared among different users. It allows the clients of the cloud services to cut the software acquisition and maintenance costs. The SaaS-based applications are designed for providing support to multiple concurrent users (multi tenancy) at a time. The security of web browsers is very important because SaaS applications are accessed over the Internet through web browsers. So, various methods for making SaaS applications secure should be considered by Information security officers. Data protection methods like Extendable Markup Language (XML) encryption, Web Services (WS) security and Secure Socket Layer (SSL), can be utilized for effective protection of data over the Internet [22]. The value-added services provided by the provider of cloud computing services are divided among customers that are contracted based on a pay-as-you-go fee. The IaaS significantly minimizes need for enormous initial asset and computing hardware like networking devices, servers, as well as processing power. It also permits a degree of functional and financial flexibility that is not found in datacenters that are internal. Since resources of computing may be released or added relatively much faster and cost-efficiently with collocation services, IaaS is a likeable choice for many clients [23]. IaaS as well as other services that are associated enable easy startups. Many industries focus on their internal competencies but does not put much efforts in managing and provisioning the infrastructure. IaaS completely abstracts hardware underneath it and allows users for consuming infrastructure as service transparently. Cloud possesses a persuasive value in provisions of expenditure, however, when adopted "out of the box", it only offers essential security (e.g., load balancing, perimeter firewall) and those applications that are moving inside the cloud would require superior security levels that the host provides. Relying on the provider's servers, the model in which software and tools related to development are being hosted is called PaaS. Instead of having any information regarding the backend services, this tends incorporation on an atmosphere of developer where a developer wants to establish own applications. While looking at the stack, it is one layer over IaaS and above OS (Operating System). It presents developers with complete overdo the development process that offers a whole SDLC (Systems/Software Development Life Cycle) management, from gathering requirements, design coding than exploitation to testing than continuance.

From the software development perspective, the PaaS layer of cloud offers "rented" utility of compliance level [20]. In Cloud computing, the utilization of known equipment provide efficiency in the Platform as a Service layer. Such as cloud malware, the virtual machines must be protected from being compromised. Hence preserving the applications accuracy and to enforce precise confirmation tests by data transfer between channels that are elementary. The services provided by the clouds include virtualized infrastructure, physical resources and middleware platforms with various applications related to business [24]. The security of cloud computing interfaces should be effectively maintained by the cloud vendors and clients [25].

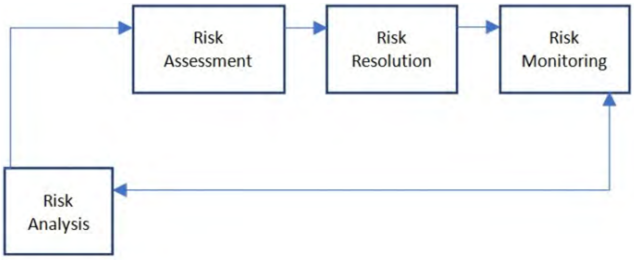


FIGURE 4. **Risk management process.**

III. RESEARCH METHODOLOGY

The risk management process addresses the possibilities, that in future, may occur and cause disruption to the normal course of business continuity [26]. However, this definition is not accurate in the sense that, if the normal operation is susceptible to eavesdropping, in this case, the normal operation of the organization must be restricted [11]. Figure 4 describes the stages in a risk management cycle. The most important concepts in risk management are risk analysis, assets identification and evaluation, and threat identification.

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. The OCTAVE model is well studied in the literature [27] however some parts of this method are not used in this study.

At the beginning stage of the risk management process, we identify the critical assets, imminent threats, and possible vulnerabilities. In addition to the OCTAVE method, this study also uses the Cloud Security Alliance guidelines [28] to carry out the risk management process. We divide our analysis task into following steps (subsections B to E):

B. ASSETS IDENTIFICATION AND EVALUATION

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

TABLE 1. List of assets.

ASSET NAME	Perceived Value
Healthcare Facility reputation	Very High
Patient trust	Very High
Healthcare Staff loyalty and experience	High
Intellectual property	Very High
Personal sensitive data	Very High
Personal data	Medium
Personal data -critical	Medium
Human Resource data	High
Service delivery – real time services	Very High
Service delivery	Medium
Access control/ authentication/ authorization (root/admin v others)	Very High
Credentials	Very High
User directory(data)	High
Cloud service management interface	Very High
Management interface APIs	Medium
Network (connections, etc.)	High
Physical Hardware	Medium

TABLE 2. Nine notorious threats identified by CSA.

Security Control (SC)	ST NO.	Security Threat (ST)
Data Threats	Thr1	Data Breaches
	Thr2	Data Loss
Network Threats	Thr3	Account Hijacking
	Thr4	Insecure Interfaces and APIs
	Thr5	Denial of Service Attack (DOS)
Cloud environment Specific threats	Thr6	Malicious Insiders
	Thr7	Abuse and nefarious use of Cloud Computing
	Thr8	Insufficient Due Diligence
	Thr9	Shared Access

C. THREAT IDENTIFICATION

Table 2 is constructed from the threats register maintained by the Cloud Security Alliance (CSA) [28].

We discuss these threats as follows:

1) DATA BREACHES

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment [18]. When patient data is accessed, viewed, shared, or utilized/ processed without authorization or the patient or the data holder, i.e., the HIS administrator, the process is called a health data breach. An accidental exposure is highly likely when records like patient data is shared among HIS with varying security standards. Often this risk is acknowledged by the patient through information disclosure forms. The patient data breach risks may be increased because of outsourced services which evade the personnel, logical and physical controls.

2) DATA LOSS

Any event or process with consequences in data being deleted, corrupted or made illegible by a software, user or application is called data loss. This includes ransomware attacks on the HIS, accidental losses, and deliberate attacks on patient data in recent times. Data loss is also known as data leakage. It happens when the data owner or the requesting application can no longer utilize data elements. Data loss can take place while data is either in storage or transmitted over network.

3) ACCOUNT HIJACKING

A process by which the access controls associated with the user are taken away and are used for malicious purposes by an advisory, is called account hijacking. Account hijacking could be performed on an email, computer, or any other account associated with a computing device or service. It is a kind of identity theft in which an unauthorized or malicious activity is carried out by the use of stolen account information.

4) INSECURE INTERFACES AND APIs

A typical cloud customer configures, interacts and manages his/her cloud infrastructure by a set of software interfaces or APIs. The accessibility and security of cloud services is dependent upon the security of these basic APIs. These configurations are shipped along with the typical security controls. If those controls are not enabled, the configurations of the APIs can be altered and the whole infrastructure may be compromised, e.g., this could happen if secure connections are not enabled or utilized, etc.

5) DENIAL-OF-SERVICE ATTACK (DoS)

When the attackers or hackers try to prevent valid customers from accessing an application or a service is called Denial-of-Service attack (DoS). In a DoS attack, excessive messages are sent by the attacker asking the server or network to authenticate requests having incorrect return addresses. When the server or network attempts to send the authentication approval, it will not be able to discover the return address of the hacker. This situation will cause the server to wait before terminating the connection. When the server terminates the connection, more authentication messages will be sent by the hacker with incorrect return addresses. Therefore, the process of sending authentication approvals and server waiting will restart, keeping the server or the network busy and the legitimate users will be denied of their services.

6) MALICIOUS INSIDERS

This refers to the case where there is a deliberately misused or unauthorized access to an organization's data, network, or system by its former or current employee, business partner or contractor. It is done in a manner that negatively affects the availability, integrity or confidentiality of the organization's assets or information systems.

7) ABUSE OF CLOUD RESOURCES

An unauthorized use of cloud capabilities is classified as an abuse of cloud computing. Sometimes cloud service providers cannot maintain control over their infrastructure, which allows an attacker to abuse cloud services, e.g., by requesting repetitive free limited trials [32].

8) INSUFFICIENT DUE DILIGENCE

Sometimes organizations may be unaware of cloud service provider's environment, general nature of cloud technology and related security threats and therefore exhibit insufficient due diligence. HIS administrators should have cloud and security experts in their teams so that the organization can avail their skills and avoid unexpected behaviours from the infrastructure. Without expert knowledge, the adoption to cloud which may lead to more troubles than benefits.

9) SHARED TECHNOLOGY ISSUES

One of the key features of cloud computing is multi-tenancy. In this type of an architecture, shared resources are provided to multiple users, to accomplish scalability. Cloud providers deliver their services to multiple customers to share the same application, platform and infrastructure. This joint nature may result in the disclosure of data to other users, and also due to a single fault, a hacker could possibly observe all the other data.

D. VULNERABILITY IDENTIFICATION

Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy [27], [33]. It is essential in a risk assessment process to identify the known vulnerabilities to protect the data and infrastructure from attacks caused by the known vulnerabilities as listed in Table 3.

Grobauer *et al.* [34] define vulnerability as "the probability that an asset will be unable to resist the action of a threat agent". The research by Grobauer *et al.* determines the risks and identifies cloud-specific vulnerabilities that could affect any cloud environment.

E. RISK ASSESSMENT

In the literature [33], [35], [36], a risk assessment framework is proposed which is a three-step process. The details of the three steps are provided in the following sections:

1) 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 aim at determining the breach likelihood to the critical assets identified in Table 1. We consider the results from the vulnerability

TABLE 3. List of vulnerabilities in cloud adoption.

VULNER-ABILITY NO.	Vulnerability Name
V01	Insecure Interfaces and APIs [33] a) Weak credential b) Insufficient authorization checks c) Insufficient input-data validation
V02	Unlimited Allocation of Resources [33]
V03	Data Related Vulnerabilities [33] a) Incomplete data deletion – data cannot be completely removed. b) Data backup done by untrusted third-party providers. c) Information about the location of the data usually is unavailable or not disclosed to users. d) Data is often stored, processed, and transferred in clear plain text. e) Data can be allocated with the data of unknown owners (competitors, or intruders) with a weak separation. f) Data may be in different jurisdictions which have different laws.
V04	Virtual Machines Vulnerabilities [27, 33] a) To provide flexibility VMs can be copied that is known as uncontrolled snapshots and may results in data leakage. b) Cloud cartography - within the cloud the attackers can map where the target VM is located, because the VM's IP addresses are visible to anyone within the cloud. c) VMs can be restored from the backups to a previous state, but patches disappear that are applied after the backup was taken, which leads to reset vulnerabilities. This is called as uncontrolled rollback. d) In the colocation of VMs, the possible covert channels. e) One server to another server migration of VMs called as Uncontrolled Migration that can due to hardware maintenance, load balance, or fault tolerance. f) With VMs the unrestricted deallocation and allocation of resources.
V05	Virtual Machine Images Vulnerabilities [27, 33] a) Since the VM images are dormant artifacts and is therefore could not be patched. b) In public repositories the uncontrolled placement of VM images.
V06	Hypervisor Vulnerabilities [33].
V07	Vulnerabilities in Virtual Networks [33].
V08	AAA Vulnerabilities.
V09	Inappropriate encryption of data in rest and in transit.
V10	Impossibility of processing of encrypted data while in transit.
V11	Possibility that internal network probing will occur (cloud).
V12	Application vulnerabilities or poor patch management.
V13	Service Level Agreement thrashing in multi-vendor environment.
V14	Service Level Agreement clauses containing exclusive business risk.
V15	Audit not available to customers.
V16	Session Riding and Hijacking
V17	Reliability and Availability of Service
V18	Insure Cryptography
V19	Data Protection and Portability
V20	Virtual Machine Escape
V21	CSP lock-in
V22	Internet Dependency
V23	Malicious Insider Threats
V24	Unclear Roles and Responsibilities
V25	Poor Provider Selection
V26	System or Operating system Vulnerabilities
V27	Lack of Security Awareness
V28	Mal-configuration
V29	Malicious Users

TABLE 4. Relationship of threat and vulnerabilities.

ST. NO.	Vulnerabilities
Thr1	V01, V08, V09, V11, V12, V17, V22, V25
Thr2	V03a, V03c, V03d, V03f, V04a-f, V05a, V07, V17
Thr3	V01, V16
Thr4	V01
Thr5	V01, V16
Thr6	V22, V23, V27
Thr7	V26, V27, V28
Thr8	V13, V14, V15, V20, V24
Thr9	V08, V19

TABLE 5. Perceived value of Impact and its corresponding numeric scale.

Perceived Value	Impact Value
Very Low	1
Low	2
Medium	3
High	4
Very High	5

identification where each vulnerability is evaluated and assigned a numeric value and a likelihood level. The numeric value ranges from 0.1 to 1.0. A value of 0.1 means that the probability of a vulnerability being exploited is very low while a value of 1.0 means that the probability of a vulnerability being exploited is very high. The vulnerability likelihood levels are defined as very high, high, medium, low and very low. Here, a high level means the threat source has high motivations or capabilities to exploit a certain vulnerability while a low level indicates the lack of required skills and incentives to exploit the given vulnerability. Table 4 shows the mapping of each vulnerability and its likelihood level and rate.

2) IMPACT ANALYSIS

During impact analysis, we assess the loss impact of each asset based on its value. Similarly, the impact level is divided into five levels or severity: very high, high, medium, low and very low. These values represent educated guesses over a wide range of common cloud deployments and do not have a precise semantics. In practice, the risk levels are related to the values of assets where a high value asset may have a high impact to a particular scenario while a low level asset may have a low impact. Each asset is given an impact value that ranges from 1 to 5 as shown in Table 5.

Table 5 shows the impact of threats (t_i) in non-security configured public clouds. From Table 5, this research estimates the value of an asset based on how a threat impacts given assets. Then, it calculates the total value of each asset and finds the average as follows:

TABLE 6. Impact of Threats in non-security configured cloud.

ST	Affected Asset	Impact Factor
Thr1	A1, A2, A4, A5, A6, A7	4
Thr2	A1, A2, A5, A6, A7, A12	4.2
Thr3	A1, A2, A5, A6, A7, A12, A23	3.6
Thr4	A1, A2, A5, A6, A7	4
Thr5	A1, A2, A9, A10, A16	4.4
Thr6	A1, A2, A3, A4, A5, A6, A7, A8	4
Thr7	A1, A2, A6, A17	3.75
Thr8	A5, A6, A7	3.33
Thr9	A1, A5, A6, A8, A9, A10, A16	4

The impact factor of a threat event ($\mathrm{Imp_e}$) is calculated by dividing the total of the impact factors of affected assets ($\mathrm{Ast_i}$) by the number of affected assets (n).

$$\mathrm{Imp_e} = \frac{1}{\mathrm{n}}\left(\sum_{\mathrm{i=1}}^{\mathrm{n}} Ast_i\right) \tag{1}$$

Assuming that the breaches in HIS have a Bayesian distribution, from [37] the reparative breaches can be modelled as:

$$\mathrm{Sn} \sim \mathrm{Lognormal}\,(\mu, \tau) \tag{2}$$

where,

$$\mu = \beta_0 + \beta_1 + \mathrm{t}_1 + \beta_2\mathrm{t}_2 + \beta_3\mathrm{t}_3 + \ldots. + \beta_n\mathrm{t}_n \tag{3}$$

$$\beta 0 \sim \mathrm{N(log(Sn), 1)} \tag{4}$$

$$\beta \mathrm{i} \sim \mathrm{N}\left(0, \frac{1}{\mathrm{Var[t}_i]}\right) \tag{5}$$

$$\tau \sim \text{Gamma (1,1) as randomize the variable} \tag{6}$$

If follow the Operationally Critical Assets Vulnerability Evaluation (OCTAVE) method from [27], we may estimate the risk exposure as follows:

$$Sn \sim Lognormal\left(\sum_{i=1}^{i=n}(\mu_i, \tau)\right) \tag{7}$$

We propose the Impact factor of a threat event as the sum of the impact of all the assets that affect the given threat, then divide it by number of affected assets as shown in Table 6 as graphically represented in Figure 5. From Table 6, impact factor which is also known as risk exposure can be used as, for instance, a threat having an impact factor greater than 4 will be considered as having a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A threat with an impact factor between two and four is considered as having a serious adverse effect on organizational operations, organizational assets, or individuals. A threat with an impact factor of less than two will have a limited adverse effect on organizational operations, organizational assets, or individuals.

TABLE 7. Security Threat along with its counter measurements.

ST. NO.	Counter Measurements
Thr1	□ Web application scanners [21]. □ Encryption. □ Efficient key management algorithm. □ Protection of key. □ Isolation among VMs.
Thr2	□ FRS techniques [41]. □ Digital Signatures [42]. □ Encryption [43]. □ Homomorphic encryption [44].
Thr3	□ Identity and Access Management Guidance [28]. □ Dynamic credential [41].
Thr4	□ The Open Web Application Security Project (OWASP) [34] provides standards and guidelines to develop secure applications that can help in avoiding such application threats.
Thr5	□ Achieved the perfection of properties like isolation, inspection, and interposition [32]. □ Stricter initial registration and validation processes [32]. □ Monitoring public blacklists for one's own network blocks [32].
Thr6	□ All user accounts are current with regards to security access and employment status. □ Access removal into the termination process. □ Review of all accounts to look for any suspicious activity or rogue accounts. □ Strong passwords and two-step verification.
Thr7	□ The implementation of strict initial registration and validation processes can help in identifying malicious consumers. □ The Service Level Agreement definition language (SLAng) [45] enables to provide features for SLA monitoring, enforcement and validation.
Thr8	□ Cloud provider should also perform risk assessment using qualitative and quantitative methods after certain intervals to check the storage and processing of data.
Thr9	□ Hypervisor must be secured to ensure proper functioning of other virtualization components, and implementing isolation between VMs.

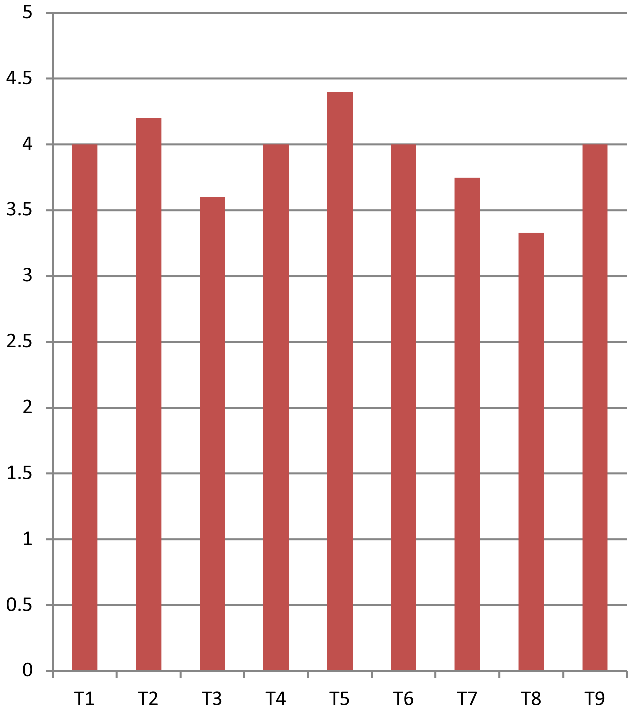


FIGURE 5. Risk exposure of the identified threats to health information systems.

3) RISK DETERMINATION

In Table 7, we map the countermeasures for each threat, which we identified for each asset in Table 6. This helps narrow down the threats space. However, the countermeasures against each threat are the ones that are reported in the literature [3], [38]–[40]. It is highly likely that more effective countermeasures may exist for each threat that has been highlighted in this research. We aim at investigating the best suited set of countermeasures in future work. A measure of risk exposure is provided in Table 8.

TABLE 8. Impact of Threats in security configured cloud.

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	A1, A2, A6, A17	1.75
Thr8	A5, A6, A7	1
Thr9	A1, A5, A6, A8, A9, A10, A16	1.86

In Table 9, we provide a comparison between non-security configured and security configured public clouds. From Table 9, we see that impact factors are significantly reduced by applying counter measurements. In Figure 6, we present our findings from an empirical analysis of security configured cloud infrastructures and non-security configured infrastructures. The figure shows that the overall impact of threats is lower than the impact of threats in non-security configured

TABLE 9. Comparison of Impacts between non-security configured and security configured cloud.

ST	Impact of non-security configured Cloud	Impact of security configured Cloud
Thr1	4	1.83
Thr2	4.2	2
Thr3	3.6	1.71
Thr4	4	1.8
Thr5	4.4	3.4
Thr6	4	1.5
Thr7	3.75	1.75
Thr8	3.33	1
Thr9	4	1.86

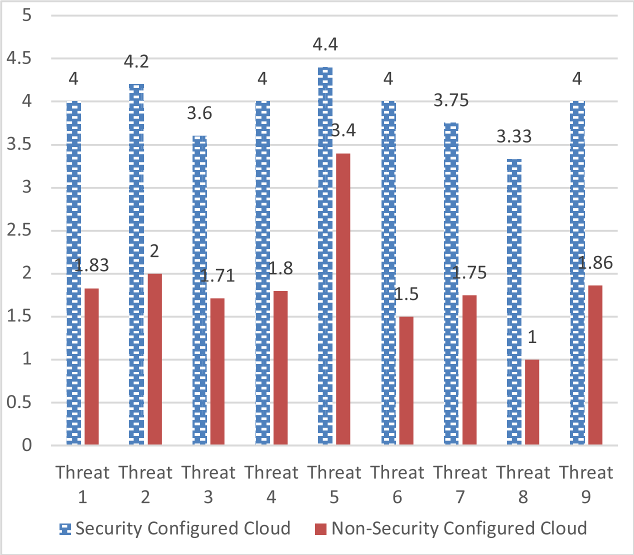


FIGURE 6. A Comparison between non-security configured and security configured clouds.

clouds. By non-security configured clouds, we refer to hybrid clouds, the cloud computing environments where security practices are not considered as a primary concern.

The results are contrary to the common misconception that a private cloud infrastructure may be more secure than a public cloud infrastructure, in general. An important aspect in both of the paradigms, that is public and private clouds, is the presence of key security countermeasures.

We plan to present a further account of those key security countermeasures in our future work. Those countermeasures do not necessarily make a public cloud infrastructure an outright choice for the healthcare enterprises.

The emphasis is increased on authentication, authorization, and accounting (AAA) control, so the right people may be able to access information. The data ownership and rendering issues are also of considerable importance. Another challenge of public clouds is the juristic and cyber law about the ''hosting'' of data in public clouds.

IV. CONCLUDING REMARKS AND FUTURE WORK

An increasing range of risks to digital healthcare industry due to the persistent threats, stimulates the acquisition and development of new technology. Cloud computing is seen as a quick fix to many security vulnerabilities in the healthcare and public health sector that are discussed in this paper. Despite their benefits, this paper presents the findings that highlight the hurdles in the adoption of cloud computing solutions. Furthermore, relevant risk factors are identified and classified, which ultimately slow down the adoption of cloud computing in the medical sector. In addition, the assets in a healthcare system and their criticality that effects the overall integrity of the HIS are identified, and the vulnerabilities are tabled. Such details help us determine the impact of a breach and risk exposure of the components. The presented analysis demonstrates that the use of cloud computing environments can reduce the said vulnerabilities and alleviate the threats to the integrity of the HIS.

We plan to present a more detailed account of the listed key security countermeasures in our future work. Another challenge of public clouds is the juristic and cyber law about the ''hosting'' of data in public clouds, which we will also address in our future research.

REFERENCES

[1] K. Saleem, Z. Tan, and W. Buchanan, ''Security for cyber-physical systems in healthcare,'' in *Health 4.0: How Virtualization and Big Data are Revolutionizing 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 flow 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 fingerprinting,'' 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. Workshop (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: Benefits, 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] 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.

[41] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing," in *Proc. 1st Int. Conf. Parallel Distrib. Grid Comput. (PDGC)*, 2010, pp. 211–216.

[42] D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage," *IEEE Security Privacy*, vol. 8, no. 6, pp. 40–47, Nov./Dec. 2010.

[43] M. Tebaa, S. El Hajji, and A. El Ghazi, "Homomorphic encryption method applied to Cloud Computing," in *Proc. Nat. Days Netw. Secur. Syst. (JNS2)*, 2012, pp. 86–89.

[44] E. Fong and V. Okun, "Web application scanners: Definitions and functions," in *Proc. 40th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2007, p. 280b.

[45] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," Dept. Softw. Eng. INST, Carnegie-Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2007-TR-012, May 2007. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419 and ftp://ftp.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf

HINA ABRAR was born in Taxila, Pakistan. She received the B.E. and M.S. degrees in software engineering from the University of Engineering and Technology, Taxila, in 2013 and 2016, respectively. She is currently a Lecturer with the Computer Science and Engineering Department, HITEC University, Taxila. She has also supervised projects to undergraduate students in the domain of digital image processing, artificial intelligence, and cloud computing. Her research interests include cloud computing.

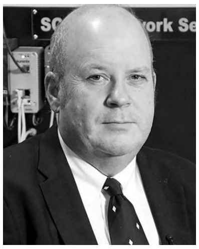
SYED JAWAD HUSSAIN received the B.S. degree with major in mathematics in 1999, the MCS degree from International Islamic University, Islamabad, Pakistan, in 2002, the PG.Dip. degree from Massey University in 2009, and the Ph.D. degree in computer networks in 2015. He was with industry for five years as an Embedded System Developer. His current research interests include machine learning and cyber security.

JUNAID CHAUDHRY (M'16–SM'17) received the degree in cyber security from Ajou University in 2009. His career has so far led him on a journey through academia, law enforcement, and industry. He is currently a Cyber Security Faculty with the College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ, USA. He has written three books and almost 100 peer-reviewed research papers. His areas of research include critical infrastructure protection, context aware security, and digital forensics. He is a member of the High Technology Crimes Investigators Association, a Life member of the Criminology Society of Pakistan, and a Senior Member of the Australian Computing Society and the Australian Information Security Association.

KASHIF SALEEM received the M.E. and Ph.D. degrees in electrical engineering from University Technology Malaysia in 2007 and 2011, respectively. He is an Assistant Professor at the Center of Excellence in Information Assurance (CoEIA), King Saud University, since 2012, and a Visiting Fellow at Department of Computing, Faculty of Science and Engineering, Macquarie University, Sydney, Australia. He is an Associate Editor and reviewer for over 30 reputed international journals. Dr. Saleem has organized International and local events as Reliability of eHealth Information Systems (ReHIS), Security and Privacy in Next Generation Networks (SPNGN), International Symposium on Health Informatics (HInfo), International Workshop on Networks of Sensors, Wearable, and Medical Devices (NSWMD) etc. He has also served as TPC member of numerous international conferences and workshops. He has authored and co-authored over 90 papers in refereed international journals and conferences. Dr. Saleem acquired several research grants in KSA, EU, and the other parts of the world. His research interests include telecommunications, computer security, wireless communication, wireless security, artificial intelligence, and bioinformatics.

MEHMET A. ORGUN (SM'96) received the B.Sc. and M.Sc. degrees in computer science and engineering from Hacettepe University, Ankara, Turkey, in 1982 and 1985, respectively, and the Ph.D. degree in computer science from the University of Victoria, Canada, in 1991. He is currently a Professor with the Department of Computing, Macquarie University, Sydney. His professional service includes editorial and review board memberships of several leading journals and program committee and senior program committee memberships of numerous national and international conferences. He was the Program Co-Chair of the 14th Pacific-Rim International Conference on Artificial Intelligence (PRICAI 2010) and the Conference Co-Chair of the 7th and 8th International Conferences on Security of Information and Networks (SIN 2014 and SIN 2015). His current research interests include knowledge discovery, multi-agent systems, and trusted and secure systems.

JALAL AL-MUHTADI received the M.S. and Ph.D. degrees in computer science from the University of Illinois at Urbana–Champaign, USA. He is currently the Director of the Center of Excellence in Information Assurance, King Saud University. He is also a Faculty Member with the Department of Computer Science, King Saud University. He has over 50 scientific publications in the areas of cyber security and the Internet of Things. His areas of expertise include cyber security, information assurance, privacy, and Internet of Things.



CRAIG VALLI has over 30 years' experience in the ICT Industry and consults to industry and the government on cyber security and digital forensics issues. He is currently the Director of the Security Research Institute, Edith Cowan University and a Professor of Digital Forensics. He has over 100 peer-reviewed academic publications in cyber security and digital forensics. He is also the Founder and the Chair of the Australian Digital Forensics Conference. His main research and consultancy is focused on securing networks and critical infrastructures, detection of network borne threats, and forensic analysis of cyber security incidents. He is also a Fellow of the Australian Computer Society. He is currently the Director of the Australian Computer Society Centre of Expertise in Security, ECU. He is also the current Research Director of the Australian Cyber Security Research Institute. He is also a member of the High Tech Crime Investigators Association (Australian Chapter) and a member of the Interpol Cyber Crime Experts Group.