International Journal of Grid and Distributed Computing
Vol. 9, No. 8, (2016), pp.137-158
http://dx.doi.org/10.14257/ijgdc.2016.9.8.13

Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study

Abdelrafe Elzamly[1*], Burairah Hussin[2] and Abd Samad Hasan Basari[3]

[1]*Department of Computer Science, Al-Aqsa University, Gaza, Palestine*
[2,3]*Information & Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia*
[*] [1]*E-mail: Abd_elzamly@ {yahoo.com, alaqsa.edu.ps}*

Abstract

The aim of this study is to classify critical security issues in cloud banking organizations, according to the cloud service models (CSM), and the cloud deployment models (CDM). We classified and ranked the critical cloud security issues for banking organizations based on secondary and primary data. In this regard the cloud Delphi study is modified into three phases like identifying, analysis, and evaluating security issues. In this study, the samples of 40 panelists were selected from inside and outside Malaysian banking organizations based on their experienced in the banking environment to set the insight of the cloud issues. The study starts with a list of cloud security issues based on secondary data and interview. In addition, we illustrated the level of risk for all the cloud security issues in banking organizations as small, medium, and large risk. We also indicated that the highest risk of "Trusted cloud" in [3]rd party (providers) and policies security issues and the highest risk of "Availability and Mobility" in application and program (software) security, etc. The study has been conducted on groups of cloud IT managers and cloud banking developers. As a future work, we will control and mitigate the critical security issues by using artificial intelligence techniques (ANN). A successful classification of critical cloud security issues will greatly improve the probability of cloud banking success rate.

Keywords*: Cloud computing, Cloud Security Issues, Cloud Service Models, Cloud Deployment Models, cloud banking organization, Cloud Delphi Study*

1. Introduction

Although much research and progress in the area of cloud computing project, many cloud computing projects have a very high failure rate especially when it comes to the banking area. However, several serious issues concerning security, data protection and ownership, quality of services, and mobility need to be resolved before cloud computing can be widely adopted [1]. In addition, cloud computing provides lots of advantages, but today cloud computing is suffering from security issues. Security is the biggest concern of client these days. If a client want to take a full advantage of cloud computing, then this client must be ensured about data, infrastructure and application security [2]. Integrating formal cloud risk management with project management is a new phenomenon in software engineering and product management community [3]. In addition, cloud risk is an uncertainty that can have a negative or positive effect on meeting project objectives. In addition, there are 5 main phases such as risk identifying, risk analysis and evaluation, risk treatment, risk controlling, risk communication and documentation for software development life cycle [4][5]. The goal of cloud risk management is identification and

[*] Corresponding Author

ISSN: 2005-4262 IJGDC

recognition of issues at an early stage and then actively changing the course of actions to mitigate and reduce the cloud computing issue [6]. Today, cloud computing risk management has become a common practice amongst leading banking organization's success. In the increasing effort to improve development processes and security; recent studies have pointed out to an area of cloud computing risk. Risk management helps software project managers and team to make better decisions to mitigate cloud-computing risks. Finally, the Cloud Delphi study is to classify critical security issues in Malaysian banking organizations and to determine the importance of cloud security issues based on experienced and cloud knowledgeable of developers and IT managers in developing cloud risk management.

2. Literature Review

Cloud computing is normally associated with failures. Risk of failure is defined as the possibility of suffering loss, or exposure in the cloud-computing life cycle. Commonly, cloud computing risk management consists of the processes, methods and techniques that are useful to mitigate cloud computing risks failure. In general, risk management starts with risk identification and classification of potential risk elements [7]. Security risk management is becoming increasingly important in a variety of areas related to information technology (IT), such as telecommunications, cloud computing, banking information systems [8]. Taking into consideration, a cloud computing is different kinds of stakeholder templates serve to understand and describe a given cloud development problem by using an online banking cloud scenario [9]. Cloud security is a broad topic and any combination of policies, technologies, and controls to protect data, infrastructure and services from possible attacks. Furthermore, existing researches focused on providing security technologies, rather than business features such as service stability, continuity and availability [10]. Cloud Risk management is the process of identifying, analyzing, and controlling risk throughout the life of a project to meet the project objectives [11]. Additionally, the cloud bank model is a resource management modeling based on economic principles. Its function is very similar to commercial banks in deposit and loan business [12]. Furthermore, techniques and models for mitigating risk in software development projects classified into three categories–namely, qualitative, quantitative, and intelligent approaches [13]. Quantitative risk is based on statistical methods that deal with accurate measurement about risk or lead to quantitative inputs that help to form a regression model to understand how software project risk factors influence project success [11]. The discriminant analysis (DA) techniques are proposed to classify and manage risks in the software planning development process [14]. Hence, they classified risks to three levels by predicting group membership. This study will classify the critical cloud computing issues in Malaysian banking organizations. However, the information acquired from the Delphi technique can be used especially to support identifying and classifying issues, qualification, quantification, or response development [15].

3. The Concepts of Cloud Modelling for Banking Organizations

Indeed, they introduced the conceptual framework for cloud banking that included components such as security, privacy, legal, compliance and regulatory issues in banking [16]. Furthermore, it presented the security risk analysis that includes three steps to mitigate risks: Analyze issues in virtual machines (VMs), identify risks and vulnerabilities and then concluded a set of security recommendations for using by the cloud deployed [17]. According to previous studies, we divide the framework modelling cloud computing to five stages as mobility and banking application, cloud service models (CSM), cloud deployment models (CDM), cloud risk management models (CRMM), and cloud security model as follows:

3.1 Mobility, Banking Applications, and Web Service API

Mobility referred to the possibility of moving and taking place in different locations and across multiple times using any type of portable devices such as smart phones, personal digital assistants (PDAs) and wireless laptops. The current availability of the internet and mobile technologies has led to the popularity of mobile application in different aspects of modern life. Mobile application referred to the use of portable devices equipped with the possibility of internet access, such as the use of smart phones, laptops, PDAs and tablet PC technologies in any user needs [18]. Application programming interface (API) clouds deliver programming environments that simplify not just the delivery of infrastructure, but also the actual implementation of the application for cloud deployment. APIs support common application functions from gaining access to resources and inter-process/inter-application communication services for database and caching functions [19]. Finally, mobile banking referred to any operation that related to banking services such as balance check, account transactions, payments and receiving bank SMS via a mobile device [18].

3.2 Cloud Service Models (CSM)

Cloud service models (CSM) depend upon several state of the art web technologies such as Web Services, Application Programming Interface (API), Web 2.0, and *etc*. [20]. CSM is divided into four categories that are available from a cloud provider: Banking Process as a service (BPaaS), Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) occurring at different rates as follows:

Table 1. Illustrate the Parts of Cloud Service Models (CSM)

CSM	Definition
BPaaS	**Banking process as a Service:** Banks still believe the technology to be connected with many business issues that are not yet solved. Such matters include privacy, security, legal, compliance and regulatory risks. Because of the lack of professionals and sufficient security frameworks in the area, the matter is getting scaled up to become a severe problem [16]. Business aspect represents organizations (e.g. banks) that may offer banking services to their customers through mobile banking (e.g. mobile payments). M-banking applications can be supported by mobile computing or technology like 3G, mobile wallet, and mobile payments [21].
SaaS	**Software as a Service (SaaS)** is a model where software is implemented using any of the four cloud deployment models (CDM). The users don't have access to data or the configuration and can only use the software hosted in the cloud computing [22]. SaaS provides users with remote access to the application, usually through a web browser. Facilities need not worry about storage or application management as only specific parameters are enabled for the user [23].
PaaS	**Platform as a Service** provides a platform for development and deployment software applications by supporting entire application life cycle. Cloud provider is responsible for security and monitoring. Furthermore, cloud provider provides runtime, middleware, OS, networking, servers, storage and virtualization. Cloud developer takes several benefits from PaaS [2]. In the PaaS, customers use an API to deploy their own cloud applications using programming languages and tools supported by the cloud provider [9].
IaaS	**Infrastructure as a Service** provides virtual and physical hardware as a service and entire infrastructure is delivered over the internet with more security control for clients [2].

3.3 Cloud Deployment Models (CDM)

Cloud Deployment Models (CDM) can be divided into four the different types:

Table 2. Illustrate the Parts of Cloud Deployment Models (CDM)

CDM	Definition
Public Cloud	**Public Cloud** is made available to the general public or a large industry group and are owned by a third party selling cloud services [9]. As cloud technology matures, public cloud services are becoming more attractive to enterprise users as well. Interest in the cloud has been shown by players such as critical infrastructure providers, including banking industries [24].
Private Cloud	**Private Cloud** is operated and owned by a single organization or company that concentrates on controlling the mechanism of virtualizing resources and automating services those are used and customized by various lines of business and constituent groups [4]. A private cloud provides services to an organization through an intranet. Private clouds can be connected to each other to form a partner cloud. Private Cloud private clouds are operated solely for an organization [9].
Community Cloud	**Community Cloud** falls between public and private clouds with respect to the target set of consumers [25]. The community cloud aspires to combine distributed resource provision from grid computing, distributed control from digital ecosystems and sustainability from green computing, with the use cases of cloud computing, while making greater use of self-management advances from autonomic computing [25]. The cloud infrastructure is shared by several organizations and supports a specific community that share common goals. It may be owned, managed, and operated by any organization in the community or a third party. It may exist on or off premises [26]. Community cloud model is used by a particular group of community within an organization that has the same concern, goals or security requirements [27].
Hybrid Cloud	**Hybrid Cloud** uses both public and private cloud techniques, where it applies the strategic ideas of the services of public cloud with the foundation of the private cloud. Actually, the private cloud must be connected to the rest of company's IT resources and cannot be isolated from the public cloud [18]. The hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability like cloud bursting for load-balancing between clouds [28].

3.4 Cloud Risk Management (CRM)

In Cloud computing, risk needs to be considered at all phases of interactions and investigated at each service stage in relation to the assets that need to be protected [29]. Besides, there are different types of risks that bank management need to protect against. For many banks, the main risk is credit risk but there are many other risks that supervising authorities should notify banks about related criteria and require them to follow [30]. There are the eight phases for successful a cloud risk management in banking organizations such as cloud risk planning phase (CRPL), cloud risk identification phase (CRI), cloud risk prioritization phase (CRP), cloud risk analysis phase (CRA), cloud risk evaluation phase (CRE), cloud risk treatment phase (CRT) includes four strategies for responding to cloud risks: Cloud risk mitigation, cloud risk avoidance, cloud risk transfer,

elimination cloud risk, cloud risk acceptance, cloud risk controlling phase (CRC), and cloud risk communication & documentation phase (CRCD).

3.5 Cloud Security Issues Models (CSIM)

Cloud security is a broad topic and any combination of policies, technologies, and controls to protect data, infrastructure and services from possible attacks or achieving business objectives all the security domains should work in an effective manner [2]. Computer and information security are concerned with ensuring the availability, integrity and confidentiality of information. Each of these aspects covers an integral part of security aspects of the infrastructure [31]. In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others [32]. The building blocks of cloud security are [33]: **Confidentiality:** The ability to access the protected data by the authorized users refers to confidentiality. **Authentication:** Authentication refers to identify the credentials of the individual and verify whether they are privileged users or not [23]. **Integrity:** During the data transmission capability to the protect data from not being destroyed or manipulated by unauthorized persons refers to integrity. There are the sex levels for the (CSIM) model: ^{3}rd party (providers) & policies security; application & program (software) security; data & information security; security control & network; security and service management; and physical infrastructure security.

4. Classification of Critical Cloud Security Issues based on Cloud Security models in Banking Organizations

Cloud computing is a new emerging technology, which every organization these days wants to adapt for its business for more profitability and scalability. This communication defined cloud computing, highlighted all the service models of cloud computing and discussed the features of public, private, hybrid and community cloud computing [25]. In addition, information security risks under traditional IT architecture, cloud service security is still facing new business and management risk arising from virtualization, multi-tenancy, and data encryption technology [10]. Cloud computing is changing the current IT delivery model for services. Benefits for business and IT include reduced costs, scalability, flexibility, capacity utilization, higher efficiencies and mobility [34]. The enterprise will be able to identify its weakness and strength for each factor, and then build and prepare plan that can help them to make appropriate decision toward a successful adoption of Cloud Computing [35]. Cloud computing's risks can bring negative effects on any companies or organizations, therefore an effective risk management is needed to balance the operational and financial cost as well as proactive actions to secure data, information systems and technologies [27]. Understanding the true potential of mobile cloud computing and identifying issues with mobile cloud security, privacy, feasibility and accessibility remain a major concern for both the customers and the enterprises [36]. However, classification of critical security issues in cloud banking is needed to highlight in this section:

4.1 [3]rd Party (Providers) and Policies Security:

Table 3. illustrate the Critical [3]rd Party (Providers) and Policies Security Issues

No.	Security Issues	Definition
SI1	**Lack of standards**	Interoperability impedes the quick development of cloud computing, as there is no common cloud standard being followed by different cloud providers who have their own API's [37].
SI2	**Service Level Agreement (SLAs)**	SLAs refer to a legal contract that describes the minimum performance criteria CSPs promises to meet while delivering the required service(s) to their client(s) [19].
SI3	**Governance**	Governance is a set of activities that are conducted to execute strategy, proper implementation of policies and procedures, relation between policies, assessing policies in practice, assessing and updating policies and providing frameworks to observe regulations in an organization [30].
SI4	**Legally and policy**	Third-party cloud service providers and their customer organizations are distinct enterprises. However, if the Cloud service providers neglects or fails in its responsibilities, it could have legal liability implications for the CSP's customer organizations. But if a cloud customer organization fails in its responsibilities, it is less likely there would be any legal implications to the CSP [38]. **Policy** is foundational issues related to legal definitions and organizational charters to help establish the roles, missions, responsibilities, and authorities of major actors in cloud computing organization [39].
SI5	**Dependency**	Currently, dependency on browser to access the internet as a better way of accessing mobile web other than browser. In order to get speedy mobile internet access new technologies like HTML5 are being developed, which provide facility of local caching [37].
SI6	**Lack of transparency**	A CSP is unlikely to expose the detailed information about its processes, operations, controls, and methodologies. For instance, cloud customers have little insight into the storage location (s) of data, algorithms used by the CSP to provision or allocate computing resources, the specific controls used to secure components of the cloud computing architecture, or how customer data is segregated within the cloud [38].
SI7	**Cloud service provider viability**	Many cloud service providers are relatively companies, or the cloud computing business line is a new one for a well-established company. Hence the projected longevity and profitability of cloud services are unknown. Cloud computing service providers might eventually go through a consolidation period [38].
SI8	**Malicious insiders**	In particular, both reports agree that insider attacks and malicious insiders are a major technical risk and among the top threats [40]. Attacks are usually modelled through the use of a graphical, mathematical, decision tree structure called an attack tree [41]. Besides, Malicious insider can get unauthorized access of cloud resource which can be a greater loss of business [2]. On the other hand, insiders malicious they can be current employee, a contractor, or business partner who can access the network or data for causing damage [42].
SI9	**Regulatory**	Compliance risks meaning problems for cloud customers in

No.	Security Issues	Definition
	compliance & requirements	achieving certification to meet regulatory requirements [40]. That could depends on the fact that the cloud provider cannot provide evidence of his own compliance or that the cloud provider does not permit audit by the cloud customers [43] Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements encourage them to devote the utmost attention and priority to information security risks [44]. Compliance involves conformance with an established specification, standard, regulation, or law [45]. Finally, regulatory compliance is responsibility of customers for the security and integrity of their own data [20].
SI10	**Shared technology issues**	Virtualization platform should have the feature to effectively isolate the difference users [40]. The platform also should protect the user resource and keep the users inviolable space [46]. Guest operating systems may exploit the weaknesses of hypervisors to gain inappropriate level of control on the underlying platform [47].
SI11	**Unknown risk profile**	Service provides should continuously enhance security for reducing cloud computing security risk[40]. There are many main concerns that should be studied carefully such as software versions and updates, security measures, vulnerability reports, unauthorized attempts and security design [48].
SI12	**Trusted cloud**	Trusted software and server identity is the service running the right software over the correct set of servers [24]. There some of area for trust cloud like trusted People, trusted devices, trusted operating system (OS), trusted software and applications, trusted data , *etc*. [49].
SI13	**Abuse and nefarious use of cloud computing**	Providers should use a seriously inspection procedure to audit the user qualifications and authorities [46]. By abusing relative anonymity behind cloud registration and usage models, malicious activities can be conducted with relative impunity [47].

4.2 Application and Program (Software) Security Issues

Table 4. Illustrate the Critical Application & Program (Software) Security Issues

No.	Security Issues	Definition
SI14	**Authentication**	Provides the access permission to only the authorized users and restricts the unauthorized users [50]. In addition, the authentication is the first level verification applied with authorization check to avail the right services to right user. Hence, this kind of check is required to achieve the integrity, security and the reliability while performing the communication in open environment. In more dedicated security systems, the authentication check is applied relative to the information type or the domain type [51].
SI15	**Authorization**	The cloud computing is important for the users when they login to some cloud service because it enables prove of their identities. So, authorization is usually employed after the authentication [52].

No.	Security Issues	Definition
SI16	**Insecure Interfaces API's**	Insecure Applications Programming Interfaces (APIs) refers to cloud services are accessed and managed by clients via software interface and APIs [40]. These APIs have significant roles in provisioning, monitoring, orchestration and management of the processes running in a cloud computing environment [53].
SI17	**Availability and Mobility**	One of the key arguments when migrating an banking system to a cloud platform is availability [40]. Organizations must thoroughly analyze and understand the impacts on performance and availability and must take actions in order to be able to provide resources for the highest possible load. Furthermore, service unavailability will prevent mobile users from accessing a cloud service [54]. Furthermore, availability refers to whether the data is available when needed by authorized parties. also the cloud mobility supports access anywhere using a Web [55].
SI18	**Portability and Interoperability**	Lack of application portability or interoperability refers to many CSPs offer application software development tools with their cloud solutions. When these tools are proprietary, they may create applications that work only within the CSP's specific solution architecture [20]. Hence, these new applications might not work well with systems residing outside of the cloud solution.

4.3 Data and Information Security Issues:

Table 5. Illustrate the Critical Data and Information Security Issues

No.	Security Issues	Definition
SI19	**Privacy**	Providing sensitive or private information such as providing user's current location creates scenarios for privacy issues [36].
SI20	**Confidentiality**	It is one of the most important security mechanisms for users' data protection in the cloud. It includes encryption of the plaintext in cipher text before the data is stored in the cloud [52].
SI21	**Data Protection**	Data Protection solutions from CA Technologies company detect and prevent unauthorized use of confidential banking data and provides a spectrum of remediation actions so that effective enforcement of information use policies can be achieved [56]. To protect the data in cloud database server database encryption is one of the important methods [57].
SI22	**Data Limitations and Segregation**	Data segregation should be enforced through correctly defined security perimeters and adequate and secure configuration of virtual machines and hypervisors [34].
SI23	**Data integrity and scavenging**	Integrity can be regarded as the opposite of duplicity, in that it regards internal consistency as a good feature, and suggests that parties holding apparently contradictory values should account for the inconsistency or alter their beliefs [50]. Hence, if they cannot modify the originality of the information, so integrity is regarded as the honesty and truthfulness or precision of one's actions [2]. In addition, data scavenging cannot be completely removed and attacker can reconstruct data again[37]**.**
SI24	**Data Location**	Use of an in-house computing center allows an organization to

No.	Security Issues	Definition
		structure its computing environment and to know in detail where data is stored and what safeguards are used to protect the data. Hence, data centers can be located in specific jurisdictions [20].
SI25	**Data Loss/Leakage**	Data can be deleted or modified at any time by intruders, and if data are not backed up, this can lead to data loss [31]. Removing the link from a record linked to a larger context may also result in data loss, and therefore impossible to retrieve them. However, strong data encryption while transferring data to and from the cloud may help remediate from data loss or leakage [48]. Data leakage threats remain as a result of technology and architecture weaknesses that affect cloud providers as they do other businesses [58].
SI26	**Detection and Recovery**	Security events detection: Users apply user interface or user APIs to control and accept the cloud computing service and to accomplish to resource sharing objective [46]. In cloud computing service, user authority, interface validation, APIs dependence and security should be paid more attention and carefully inspected. Two other ways of combating deadlock are to avoid it completely by identifying unsafe states using the Banker's algorithm, or to detect it and recover from it [59]. Recovery refers to create a complete data recovery mechanism for handling information security events by cloud service provider [46].
SI27	**Hijacking of Account or Service & Traffic**	More precisely, the top four threats identified are: Data leakage, data loss, account hijacking and insecure APIs [60]. The top threats in this category named account and credentials hijacking. If the provider stored data in multiple countries, then the access to data may be subjected to the privacy laws of host country [42].

4.4 Security Control and Network Issues

Table 6. illustrate the Critical Security Control and Network Issues

No.	Security Issues	Definition
SI28	**Information flow Controlling**	Securing the flow of information during the computation of confidential information in the cloud is very important. Where, the more sensitive the information, such as credit card data, government intelligence or personal medical information being processed in the cloud, the more important it is to ensure the confidentiality of this information [45].
SI29	**Intrinsic Constrains of Wireless Network**	Wireless network is heart of cloud computing as it forms the base for communication in cloud computing. But it has its own set of issues asking for attention, like data rate constraint, not so good throughput, longer latency delays and intermittent connectivity issues [37]
SI30	**Network Access Schemes**	In MCC, wireless network is major communication media, which can be cellular, WLAN or Satellite based. This variation affects mobility causing call frequent drops. Hence we require soft handover schemes, avoiding connection failure and connection reestablishment when moving from one network access point to another [37].
SI31	**Bandwidth**	Low bandwidth of mobile network is another cause of concern in

No.	Security Issues	Definition
		the cloud computing domain. So we are required to check for improvement in network bandwidth so to improve data transfer across cloud and other devices, especially in case of mobile applications [40].
SI32	**Anonymity and Network Traffic Analysis**	Not only the private data owned by a particular user, but also the anonymity may need to be protected [47]. In addition, CSP should prevent users from unauthorized analysis of the network traffic to derive information about the results of a simulation based study.
SI33	**Network Security**	Attack graphs are important tools to analyze network security and provide a framework for a security analyst to identify the most likely attack paths, highest-loss attack paths and then make decisions about countermeasures [17] [40].
SI34	**Virtual Network Protection**	Most virtualization platforms have the ability to create software-based switches and network configurations as part of the virtual environment to allow virtual machines on the same host to communicate more directly and efficiently [61].
SI35	**Limited control**	The applications and services are running on remote thus a third party virtual environments; users and companies have limited control over the function of the used hardware and software [45]. Moreover, it usually lacks the features of an application running locally because of the used remote software [45].
SI36	**Distributed Denial of Service (DDoS)**	Attacks in medium access control (MAC), denying service to valid users [62], and higher layers of networking protocols [40]: Malicious intermediate nodes in the routes between the users/clients and centralized services can degrade the service quality.
SI37	**Heterogeneity in Mobile cloud Devices**	It is caused because of technological variation in terms of OS, software, hardware, platform (android, windows, *etc*.), features and communication medium among mobile devices [37]. Additionally, there are numerous cloud vendors in market, who provide different cloud services with their own accustomed policies. This leads to heterogeneity among cloud as these vendors work on their respective infrastructures, platforms, and APIs, leading to interoperability and portability challenge [37]. Also, we are dealing with highly heterogeneous networks in terms of wireless network interfaces [54].
SI38	**Platform Reliability and Latency**	Reliability of cloud services typical cloud configurations consist of infrastructure in a data center, applications that are accessed in the cloud, or specific applications for software development [40]. Furthermore, data latency is based on wireless network interfaces [54]. Hence, cloud data transfer in a wireless network is not as continuous and consistent as in a dedicated wired LAN. Data latency will directly impact the usability of an application by a mobile cloud user [54].

4.5 Security and Service Management Issues

Table 7. Illustrates the Critical Security and Service Management Issues

No.	Issues	Definition
SI39	**Session Management**	In cloud Services in the cloud are typically hosted in more than one server for increased availability. Client requests to the services often lands in different servers, which is controlled by the load balancer component in the cloud, which routes request to different servers based on server load and round robin algorithm [54].
SI40	**Identity/Access Management**	Cloud applications are wholly dependent on the ability of cloud users to successfully and securely authenticate themselves for authorized access in a cloud context [39]. Accesses to key stores have to be limited to the authorized personnel who require the individual keys. These keys ought to be under policies governing them [53].
SI41	**Quality of Service (QoS)**	Quality of service has some of issues such as congestion, network disconnection, and the signal attenuation can reduce the quality of services significantly [40]. Through, we can estimate the level of service quality, experiences in wireless technologies confirms that QoS in general is hard to maintain, especially the end-to-end ones[19].
SI42	**IT organizational changes**	If cloud computing is based on a significant degree, organizations needs fewer internal IT as infrastructure management, technology deployment, application development, and maintenance. Hence, the morale and dedication of remaining IT staff members could be at risk as a result [38].

4.6 Physical Infrastructure Security Issues

Table 8. Illustrates the Critical Physical Infrastructure Security Issues

No.	Issues	Definition
SI43	**Flexibility Infrastructure**	It can be scaled to maximize investments. Cloud computing allows dynamic scalability as demands fluctuate [63]. The cloud is not dependent on local hardware or software, thus the user gains a new level of flexibility in terms of accessing the solution [8].
SI44	**Single Point to Attack and Failure**	Although the centralization of services increases security by reducing the size of infrastructure to protect, that also creates points of gravitation for cyber and physical attacks. When a system is hacked and/or fails, the impact is much bigger comparing to distributed architecture [64]**.**
SI45	**High-value cyber-attack targets**	The consolidation of multiple organizations operating on a CSP's infrastructure presents a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality and data integrity [38].
SI46	**The multitenancy**	The multi-tenant concept affects how resources are organized and provided to the CSP's customers [38]. Multitenancy is an essential cloud property that enables the share of resources such as the memory, application, networks and data. The hardware

No.	Issues	Definition
		component is shared by different users, while the virtual level is isolated for every user [48].
SI47	**Scalability**	Cloud based systems needs to be designed in such a way that will take advantage of the rapid scalability and deployment capabilities that cloud computing offers [65]. Furthermore, scalability and Performance Scalability is a built-in feature for cloud deployments. The cloud instances are deployed automatically on demand and as a result, users are paid only for the required applications and data storage. The cloud is scaled to meet the required changes in IT system demands [20].
SI48	**Cost**	A core benefit of cloud migration is the potential for cost savings[40]. By migrating banking platform to the cloud, banking organizations can get powerful functionality in the most cost effective manner. Regardless the infrastructure cost, cloud minimizes cost of other services, updating and managing applications and decreases on-site energy costs [19].

5. Empirical Strategy (Analytic Study)

5.1 Methods

Indeed, we used cloud Delphi techniques for data gathering and analysis it in this study. However, we will begin a list of cloud security issues based on secondary data, their experience of the cloud managers and cloud developers. These issues were derived from the cloud models. However, we identified and classified the critical security issues in cloud banking based on interviews, Delphi approach and secondary data. Furthermore, we focused on two groups cloud developers and cloud IT managers in Malaysian banking organizations. Each group will select the highest and most important cloud security issues based on cloud service models (CSM), cloud deployment models (CDM). In addition, we ranked and addressed the cloud security issues. The Delphi method has collected data and aggregated of cloud security issues. Indeed, we are divided the phases cloud Delphi technique into three phases such as identifying, analysis, and evaluating security issues. However, we illustrate the concept of cloud Delphi technique for classifying cloud security issues in Figure 1 as follows:

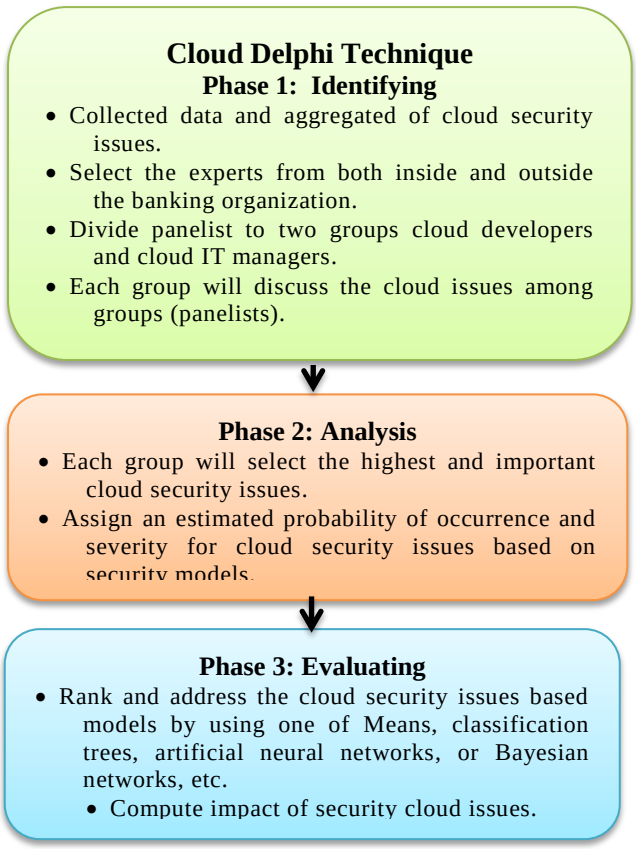

Figure 1. Illustrates the Steps of Cloud Delphi Study

5.2 Data Collection

The cloud Delphi technique use to collect data as qualified informants, so we focused on two groups cloud developers and cloud IT managers in banking organizations. In this regard the cloud Delphi study is modified to three phases like identifying, analysis, and evaluating as described in Figure 1. The data are collected by secondary data and cloud Delphi study. In this study, the samples of 40 panelists were selected from inside and outside Malaysian banking organizations based on their experienced in cloud banking. Indeed, we an estimated probability of occurrence based on a 10 scale (where 1= very low probability of occurrence and 10 = very high probability of occurrence), estimate the severity of the security issue described on a 10 scale (where 1= very low influence risk and 10 = very high influence risk).

5.3 Results and Discussion

Table 9, 10, 11 illustrate all levels of risk for all the security cloud issues in banking organizations. However, after computing the impact of cloud security for the security issues in cloud service models (CSM) and cloud deployment models (CDM), it indicated that the highest risk of "**Trusted cloud**" in 3rd party (providers) and policies security in banking organizations. Furthermore, the highest risk of "**Availability and Mobility**" in application and program (software) security and the highest risk of "**Data Protection**" in data and information Security. In addition, the highest risk of "**Network Security**" in security control and network, the "**Quality of Service (QoS)**" in security and service management, and the "**The multi-tenancy**" in physical infrastructure security. In fact, all respondents indicated that the levels of risks are medium and large except security issue no. 6: Lack of transparency. Indeed, we assigned alert level of risk based on 1- < 4 is

small, 4-7 is medium, greater than 7 is large. For example, we ranked the cloud security issues in 3rd Party (Providers) and Policies Security as SI12, SI2, SI1, SI13, SI4, SI3, SI10, SI11, SI9, SI7, SI8, SI5, and SI6.

Table 9. Classification of Critical Cloud Security Issues based on Security Domains for Cloud Service Models (CSM) in Banking Organizations

BS	Cloud Security Issues Models (CSIM)	Cloud Service Models (CSM)											
		BPaaS			SaaS			PaaS			IaaS		
		P	S	I	P	S	I	P	S	I	P	S	I
3rd Party (Providers) & Policies Security	SI1	7.15	7.15	7.15	7.15	6.7	6.92	6.2	7.02	6.59	6.8	8.4	7.55
	SI2	7.9	8.2	8.04	6.85	7.9	7.35	7.47	7.1	7.28	7.95	7.52	7.73
	SI3	7.3	6.82	7.05	6.07	6.55	6.30	5.52	4.85	5.17	4.52	4.7	4.61
	SI4	5.55	5.12	5.33	6.65	4.95	5.73	5.87	6.1	5.98	5.87	5.7	5.78
	SI5	4.7	4.57	4.63	4.3	4.32	4.31	4.52	4.5	4.51	4.37	4.57	4.47
	SI6	4.7	4.17	4.42	4.25	3.1	3.62	3.22	3.25	3.23	2.9	3	2.94
	SI7	5	5	5	4.65	4.8	4.72	5	5.32	5.15	4.55	4.2	4.37
	SI8	5.25	5.05	5.14	5.02	5.32	5.17	4.6	5.07	4.83	4.67	4.32	4.49
	SI9	5.67	4.9	5.27	5.97	5.3	5.62	5.15	4.8	4.97	4.7	4.75	4.72
	SI10	5.58	5.65	5.61	5.35	5.15	5.24	6.25	5	5.59	5.92	5.6	5.76
	SI11	3.9	4.7	4.28	5.1	5	5.04	5.07	5.12	5.09	4.8	5.65	5.20
	SI12	8.05	8.35	8.19	8.37	8.12	8.24	8.42	8.47	8.44	8.55	8.22	8.38
	SI13	5.32	5.02	5.17	6.05	5.32	5.67	5.42	5.12	5.27	5.45	5.8	5.62
Application & Program (Software) Security	SI14	5.12	5.07	5.09	5.3	6.45	5.84	4.92	4.85	4.88	6.72	5.65	6.16
	SI15	6.05	5	5.5	5.25	5.62	5.43	5.2	6.15	5.65	5.8	5.72	5.76
	SI16	5.45	5.05	5.24	4.9	4.95	4.92	5	5.52	5.25	5.2	5.92	5.55
	SI17	6.65	6	6.31	7.35	5.62	6.42	6.3	7.37	6.81	6.75	6.57	6.66
	SI18	5.25	5.5	5.37	5.9	6.22	6.06	5.92	5.42	5.66	5.6	5.8	5.69
Data & information Security	SI19	7.43	7.78	7.60	8.13	7.9	8.01	8.03	8.43	8.22	8.25	8.23	8.23
	SI20	8.25	8.42	8.33	8.55	8.7	8.62	8.05	8.92	8.47	8.4	8.9	8.64
	SI21	8.82	7.57	8.17	8.05	8.72	8.38	8.75	8.25	8.49	8	8.5	8.24
	SI22	7.77	7.72	7.74	8.05	8	8.02	8.17	8.47	8.32	8.35	8.67	8.51
	SI23	7.48	8.17	7.81	8.12	8.45	8.28	8.47	7.72	8.09	7.57	8.32	7.94
	SI24	8.32	7.9	8.10	8.55	8.3	8.42	8.52	8.3	8.41	8.8	7.92	8.35
	SI25	8.27	8.45	8.36	7.67	7.97	7.82	7.52	7.65	7.58	7.27	7.52	7.39
	SI26	7.6	8.35	7.96	7.9	7.82	7.86	8.12	8.4	8.26	6.72	5.42	6.04
	SI27	5.3	5.47	5.38	7.65	7.62	7.63	7.55	6.15	6.81	7.67	7.82	7.74
Security Control & Network	SI28	6.9	6.23	6.55	6.58	5	5.73	5.83	7.17	6.46	5.28	5.08	5.17
	SI29	4.78	4.68	4.72	4.95	5.08	5.01	6.2	6.65	6.42	5.98	6.18	6.07
	SI30	7.4	6.27	6.81	5.67	7.6	6.56	7.62	5.1	6.23	5.27	5.32	5.29
	SI31	4.92	5	4.96	5.25	4.95	5.09	4.37	4.9	4.63	4.37	4.8	4.58
	SI32	6.72	7.52	7.11	7.4	4.7	5.89	5.15	4.85	4.99	5.8	7	6.37
	SI33	7.58	7.7	7.63	7.53	7.58	7.55	7.8	8.5	8.14	8.1	7.55	7.82
	SI34	7.67	6.22	6.91	6.65	7.45	7.03	7.27	7.35	7.31	7.52	7.62	7.57
	SI35	7.45	7.38	7.41	7.65	7.68	7.66	7.48	7.43	7.45	7.43	7.45	7.43
	SI36	7.5	7.48	7.48	6.95	7.7	7.31	8.13	5.6	6.74	7.73	7.58	7.65

BS	Cloud Security Issues Models (CSIM)	Cloud Service Models (CSM)											
		BPaaS			SaaS			PaaS			IaaS		
		P	S	I	P	S	I	P	S	I	P	S	I
	SI37	7.78	7.53	7.65	7.28	7.5	7.38	7.63	7.55	7.58	6.35	7.37	6.84
	SI38	7.55	7.22	7.38	7.2	7.32	7.26	6.95	7.72	7.32	7.2	6.9	7.04
Security & Service Management	SI39	5.52	7.4	6.39	4.8	7.02	5.80	7.22	4.62	5.78	5.35	4.97	5.15
	SI40	7.8	7.8	7.8	7.47	7.42	7.44	7.47	7.67	7.57	7.85	7.8	7.82
	SI41	8.2	8.45	8.32	8.2	7.62	7.90	7.82	7.95	7.88	8.87	8.32	8.59
	SI42	8.25	7.92	8.08	8.12	8.7	8.40	7.75	8.12	7.93	7.17	7.8	7.48
Physical Infrastructure Security	SI43	7.17	7.25	7.21	8.05	7.95	7.99	7.87	6.97	7.41	7.4	7.82	7.60
	SI44	6.92	7.65	7.27	5.45	7	6.17	7.67	7.47	7.57	6.1	7.57	6.79
	SI45	7.52	7.77	7.64	7.7	7.92	7.81	7.8	8.4	8.09	8.1	7.52	7.80
	SI46	6.92	7.7	7.30	7.77	7.75	7.76	7.62	7.57	7.59	8.2	8	8.09
	SI47	7.62	7.55	7.58	7.5	7.37	7.43	7.47	7.7	7.58	8.05	8.05	8.05
	SI48	5.5	5.77	5.63	4.57	4.3	4.43	7.4	7.15	7.27	7.72	7.82	7.77

P= Probability of occurrence **S**= Severity of risk **I**= Impact of security cloud risk = $\sqrt{P * S}$

Table 10. Classification of Critical Cloud Security Issues based on Security Domains Cloud Deployment Models (CDM) in Banking Organizations

CBS	Cloud Security Issues Models (CSIM)	Cloud Deployment Models (CDM)											
		Public Cloud			Community Cloud			Private Cloud			Hybrid Cloud		
		P	S	I	P	S	I	P	S	I	P	S	I
3rd Party (Providers) & Policies Security	SI1	7.27	7.17	7.22	7.67	7.67	7.67	8.3	7.3	7.78	7.8	7.55	7.67
	SI2	8.3	7.37	7.82	6.9	7.8	7.33	7.1	7.55	7.32	7.25	5.5	6.31
	SI3	7.32	5.32	6.24	6.02	5.47	5.74	5.92	4.97	5.42	5.12	4.67	4.89
	SI4	5.27	7.2	6.16	5.47	6.42	5.93	5.45	7.02	6.18	4.85	4.47	4.65
	SI5	4.7	4.75	4.72	4.35	4.32	4.33	4.07	4.32	4.19	4.2	4.37	4.28
	SI6	2.6	3.55	3.03	3.6	3.32	3.45	3.92	3.1	3.48	3.72	3.5	3.61
	SI7	5	4.65	4.82	4.95	5.5	5.21	5.2	4.97	5.08	4.7	4.7	4.7
	SI8	5.37	5.25	5.31	4.97	4.32	4.63	4.52	4.92	4.72	4.17	4.65	4.40
	SI9	4.9	5.45	5.16	6.17	4.22	5.10	4.52	5.27	4.88	5.17	5.35	5.26
	SI10	4.92	5.5	5.20	5.02	6.02	5.50	6.3	5.77	6.03	4.35	5.52	4.90
	SI11	6.55	5.5	6.00	5.47	6.15	5.80	4.6	6.07	5.28	5.5	4.37	4.90
	SI12	7.72	8.7	8.19	8.45	7.2	7.8	8.55	8.37	8.46	8.15	8.65	8.39
	SI13	5.25	6.32	5.76	6.9	6.17	6.52	6.17	7.4	6.75	6.7	7.82	7.24
Program (Softwa	SI14	5.05	6.62	5.78	6.12	5.47	5.79	6.95	7.22	7.08	6.82	5.6	6.18
	SI15	5.62	7.27	6.39	5.4	5.07	5.23	6.22	5.52	5.86	6.2	6.4	6.29

CBS	Cloud Security Issues Models (CSIM)	Cloud Deployment Models (CDM)											
		Public Cloud			Community Cloud			Private Cloud			Hybrid Cloud		
		P	S	I	P	S	I	P	S	I	P	S	I
	SI16	4.85	5.2	5.02	4.9	4.55	4.72	4.87	5.5	5.17	6	5.37	5.67
	SI17	7.77	6.45	7.08	4.55	4.87	4.70	4.6	4.5	4.54	5	5.22	5.11
	SI18	4.97	5.22	5.09	5.72	5.5	5.61	5.97	4.95	5.43	5.4	5.1	5.24
Data & Information Security	SI19	8.22	8	8.11	8.47	8.65	8.56	7.87	8.62	8.24	8.3	7.25	7.75
	SI20	8.82	8.27	8.54	8.12	7.67	7.89	8.42	8.8	8.61	8.87	8.8	8.83
	SI21	8.8	8.7	8.74	8.47	8.72	8.59	8.97	8.82	8.89	8.72	7.92	8.31
	SI22	8.72	8.9	8.81	7.82	7.92	7.87	7.67	8.35	8.00	8.05	7.95	7.99
	SI23	8.42	8.57	8.49	8.42	8.45	8.43	7.85	8.35	8.09	8.32	8.47	8.39
	SI24	8.72	7.95	8.32	7.92	8.1	8.01	7.92	8.37	8.14	7.92	7.9	7.91
	SI25	7.62	8.02	7.82	8.27	8.35	8.31	7.7	8.22	7.95	7.82	7.92	7.87
	SI26	5.88	6.38	6.12	5.95	8.08	6.93	8.35	7.6	7.96	7.93	8.4	8.16
	SI27	7.92	7.97	7.94	7.3	7.77	7.53	6.57	6.47	6.52	5.1	5.55	5.32
Security Control & Network	SI28	6.53	7.9	7.18	5.9	5.3	5.59	5.33	7.8	6.44	5	6.33	5.62
	SI29	5.2	6.7	5.90	6.18	5.03	5.57	5.15	6.2	5.65	5.9	5.35	5.61
	SI30	6.12	7.55	6.80	7.6	7.5	7.54	7.42	7.32	7.37	7.82	6.35	7.04
	SI31	4.52	4.5	4.51	4.5	4.37	4.43	4.6	5.02	4.80	7.47	7.5	7.48
	SI32	5.97	7.35	6.62	7.6	7.15	7.37	7.2	6.57	6.88	7.45	7.37	7.41
	SI33	7.42	7.42	7.42	7.85	7.72	7.78	7.82	8.07	7.94	7.52	8.6	8.04
	SI34	7.32	7.52	7.42	7.6	7.52	7.56	7.05	7.4	7.22	6.9	6.97	6.93
	SI35	7.65	7.73	7.68	7.53	7.35	7.43	7.78	7.68	7.72	7.75	7.88	7.81
	SI36	7.4	5.65	6.46	5.18	5.53	5.35	4.93	6.08	5.47	7.33	7.53	7.42
	SI37	5.9	6.8	6.33	6.87	7.57	7.21	6.87	6.52	6.69	7.5	7.6	7.54
	SI38	8.05	7.82	7.93	7.77	7.47	7.62	7.3	7.77	7.53	7.87	7.85	7.86
Security & Service Management	SI39	7.55	7.55	7.55	7.15	6.325	6.72	6.17	7.825	6.95	7.25	7.45	7.34
	SI40	7.65	7.8	7.72	7.5	7.32	7.41	7.67	7.57	7.62	7.82	8	7.91
	SI41	8.35	7.82	8.08	8.12	7.87	7.99	8.02	7.85	7.93	8.3	7.925	8.11
	SI42	7.15	7.8	7.46	7.57	7.87	7.72	5.37	5.95	5.65	4.45	4.75	4.59
Physical Infrastructure Security	SI43	7.87	8.27	8.07	7.82	7.8	7.81	7.7	7.75	7.72	5.35	5.45	5.39
	SI44	7.62	7.95	7.78	7.77	4.9	6.17	7.52	7.72	7.62	7.62	7.5	7.56
	SI45	7.57	7.65	7.61	5.45	4.3	4.84	4.75	7.67	6.03	7.6	7.95	7.77
	SI46	7.97	8	7.98	8	7.7	7.84	7.7	7.62	7.66	7.67	7.9	7.78
	SI47	7	7.5	7.24	7.37	7.55	7.46	5.52	5.02	5.26	7.5	7.67	7.58
	SI48	7.57	7.67	7.62	7.57	7.5	7.53	7.73	6.45	7.06	4.4	5.2	4.78

P= Probability of occurrence **S**= Severity of risk **I**= Impact of cloud security risk

$= \sqrt{P * S}$

Table 11. Classification of Critical Cloud Security Issues based on Domain Security in Banking Organizations

CBS	Cloud Security Issues Models (CSIM)	Total CSM			Total CDM			Total			
		P	S	I	P	S	I	P	S	I	R
3rd Party (Providers) & Policies Security	SI1	6.82	7.31	7.06	7.76	7.42	7.59	7.29	7.37	7.33	3
	SI2	7.54	7.68	7.61	7.38	7.05	7.21	7.46	7.36	7.41	2
	SI3	5.85	5.73	5.79	6.1	5.11	5.58	5.97	5.42	5.69	6
	SI4	5.98	5.46	5.72	5.26	6.28	5.74	5.62	5.87	5.74	5
	SI5	4.47	4.49	4.48	4.33	4.44	4.38	4.40	4.46	4.43	12
	SI6	3.76	3.38	3.56	3.46	3.36	3.41	3.61	3.37	3.49	13
	SI7	4.8	4.83	4.81	4.96	4.95	4.95	4.88	4.89	4.88	10
	SI8	4.88	4.94	4.91	4.76	4.78	4.77	4.82	4.86	4.84	11
	SI9	5.37	4.93	5.15	5.19	5.07	5.13	5.28	5.00	5.14	9
	SI10	5.77	5.35	5.55	5.15	5.70	5.42	5.46	5.52	5.49	7
	SI11	4.71	5.11	4.91	5.53	5.52	5.52	5.12	5.32	5.22	8
	SI12	8.35	8.29	8.32	8.21	8.23	8.22	8.28	8.26	8.27	1
	SI13	5.56	5.31	5.43	6.25	6.93	6.58	5.90	6.12	6.01	4
Application & Program (Software) Security	SI14	5.51	5.50	5.51	6.23	6.23	6.23	5.87	5.86	5.87	2
	SI15	5.57	5.62	5.59	5.86	6.06	5.96	5.71	5.84	5.78	3
	SI16	5.13	5.36	5.24	5.15	5.15	5.15	5.14	5.25	5.20	5
	SI17	6.76	6.39	6.57	5.48	5.26	5.37	6.12	5.82	5.97	1
	SI18	5.66	5.73	5.70	5.51	5.19	5.35	5.59	5.46	5.52	4
Data & Information Security	SI19	7.96	8.08	8.02	8.21	8.13	8.17	8.08	8.10	8.09	6
	SI20	8.31	8.73	8.52	8.56	8.38	8.47	8.43	8.56	8.49	1
	SI21	8.40	8.26	8.33	8.74	8.54	8.64	8.57	8.40	8.48	2
	SI22	8.08	8.21	8.15	8.06	8.28	8.17	8.07	8.25	8.16	5
	SI23	7.91	8.16	8.04	8.25	8.46	8.35	8.08	8.31	8.19	4
	SI24	8.55	8.10	8.32	8.12	8.08	8.10	8.33	8.09	8.21	3
	SI25	7.68	7.9	7.79	7.85	8.13	7.99	7.77	8.01	7.89	7
	SI26	7.58	7.5	7.54	7.02	7.61	7.31	7.30	7.55	7.43	8
	SI27	7.04	6.76	6.90	6.72	6.94	6.83	6.88	6.85	6.87	9
Security Control & Network	SI28	6.14	5.87	6.00	5.69	6.83	6.23	5.91	6.35	6.13	9
	SI29	5.47	5.64	5.56	5.60	5.82	5.71	5.54	5.73	5.63	11
	SI30	6.49	6.07	6.28	7.24	7.18	7.21	6.86	6.62	6.74	7
	SI31	4.73	4.91	4.82	5.27	5.35	5.31	5.00	5.13	5.06	10
	SI32	6.26	6.01	6.14	7.05	7.11	7.08	6.66	6.56	6.61	8
	SI33	7.75	7.83	7.79	7.65	7.95	7.80	7.70	7.89	7.79	1
	SI34	7.28	7.16	7.22	7.21	7.35	7.28	7.25	7.25	7.25	4
	SI35	7.50	7.48	7.49	7.67	7.66	7.66	7.59	7.57	7.58	2
	SI36	7.57	7.09	7.32	6.21	6.19	6.20	6.89	6.64	6.76	6
	SI37	7.26	7.48	7.37	6.78	7.12	6.95	7.02	7.30	7.16	5
	SI38	7.22	7.29	7.25	7.75	7.73	7.74	7.48	7.51	7.49	3
Security & Service Management	SI39	5.72	6.0	5.86	7.03	7.28	7.15	6.37	6.64	6.51	4
	SI40	7.65	7.67	7.66	7.66	7.67	7.66	7.65	7.67	7.66	2
	SI41	8.27	8.08	8.18	8.2	7.86	8.03	8.23	7.97	8.10	1
	SI42	7.82	8.13	7.97	6.13	6.59	6.36	6.98	7.36	7.17	3

CBS	Cloud Security Issues Models (CSIM)	Total CSM			Total CDM			Total			
		P	S	I	P	S	I	P	S	I	R
Physical Infrastructure Security	SI43	7.62	7.5	7.56	7.18	7.31	7.25	7.40	7.40	7.40	2
	SI44	6.53	7.42	6.96	7.63	7.01	7.32	7.08	7.22	7.15	5
	SI45	7.78	7.90	7.84	6.34	6.89	6.61	7.06	7.4	7.22	4
	SI46	7.63	7.75	7.69	7.83	7.80	7.82	7.73	7.78	7.75	1
	SI47	7.66	7.66	7.66	6.85	6.93	6.89	7.25	7.30	7.27	3
	SI48	6.3	6.26	6.28	6.82	6.70	6.76	6.56	6.48	6.52	6

P= Probability of occurrence **S**= Severity of risk **I**= Impact of cloud security risk **R**= Rank

= Large Risk = Medium risk mall risk

6. Conclusions

The concern of the study is to classify the critical cloud security issues for banking organizations based secondary and primary data. Indeed, we classified the issues based on the cloud security issues model (CSIM), cloud service model (CSM), and cloud deployment models (CDM). Furthermore, we used the cloud Delphi technique for data gathering and analysis it in this study. The study has been conducted on groups of cloud IT managers and cloud banking developers. We illustrated the level of risk for all the cloud security issues in banking organizations as small, medium, and large risk. For example, we indicated that the highest risk of "**Trusted cloud**" in 3rd party (providers) and policies security issues in banking organizations and the highest risk of "**Availability and Mobility**" in application and program (software) security, *etc*. As a future work, we intend to use the security controls for mitigating issues using artificial intelligence techniques. However, successful classification and identification of critical cloud security issues will greatly improve the probability of cloud banking success rate.

Acknowledgments

This work is financially supported by the Arab Monetary Fund, Bank of Palestine, and Welfare Association in Palestine: Academic Fellowship Program (Zamalah). The authors also would like to thank the Welfare Association, Al-Aqsa University, Gaza, Palestine and Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia.

References

[1] D. Hoang and L. Chen, "Mobile Cloud for Assistive Healthcare (MoCAsH)," in 2010 IEEE Asia-Pacific Services Computing Conference Mobile, **(2010)**, pp. 325–332.
[2] F. Al-anzi, S. Yadav, and J. Soni, "Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance," in 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC), **(2014)**, pp. 1–6.
[3] A. Elzamly and B. Hussin, "Managing Software Project Risks (Implementation Phase) with Proposed Stepwise Regression Analysis Techniques," Int. J. Inf. Technol., vol. 1, no. 5, pp. 300–312, **(2013)**.
[4] A. Elzamly and B. Hussin, "A Comparison of Fuzzy and Stepwise Multiple Regression Analysis Techniques for Managing Software Project Risks: Implementation Phase," Int. Manag. Rev., vol. 10, no. 1, pp. 43–54, **(2014)**.
[5] A. Elzamly and B. Hussin, "An Enhancement of Framework Software Risk Management Methodology for Successful Software Development," J. Theor. Appl. Inf. Technol., vol. 62, no. 2, pp. 410–423, **(2014)**.
[6] J. Miler and J. Górski, "Supporting Team Risk Management in Software Procurement and Development Projects," in 4th National Conference on Software Engineering, **(2002)**, pp. 1–15.
[7] V. Holzmann and I. Spiegler, "Developing Risk Breakdown Structure for Information Technology Organizations," Int. J. Proj. Manag., vol. 29, no. 5, pp. 537–546, Jun. **(2010)**.
[8] J. Mounzer, T. Alpcan, and N. Bambos, "Integrated Security Risk Management for IT-Intensive Organizations," in 2010 Sixth International Conference on Information Assurance and Security, **(2010)**,

pp. 329–334.
[9] K. Beckers, J.-C. Kuster, H. Schmidt, and S. Faßbender, "Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing," in 2011 Sixth International Conference on Availability, Reliability and Security Pattern-Based, **(2011)**, pp. 327–333.
[10] Z. Gao, Y. Li, H. Tang, and Z. Zhu, "Management Process Based Cloud Service," in International Conference on Cyberspace Technology (CCT 2013), **(2013)**, pp. 278–281.
[11] A. Elzamly and B. Hussin, "Modelling and Evaluating Software Project Risks with Quantitative Analysis Techniques in Planning Software Development," J. Comput. Inf. Technol., vol. 23, no. 2, pp. 113–120, **(2015)**.
[12] H. Li, Y. Pu, and J. Lu, "A Cloud Computing Resource Pricing Strategy Research-based on Resource Swarm Algorithm," in 2012 International Conference on Computer Science and Service System, **(2012)**, pp. 2217–2222.
[13] A. Elzamly and B. Hussin, "Quantitative and Intelligent Risk Models in Risk Management for Constructing Software Development Projects: A Review," Int. J. Softw. Eng. Its Appl., vol. 10, no. 2, pp. 9–20, **(2016)**.
[14] A. Elzamly, B. Hussin, S. Naser, and M. Doheir, "Classification of Software Risks with Discriminant Analysis Techniques in Software planning Development Process," Int. J. Adv. Sci. Technol., vol. 81, no. 2015, pp. 35–48, **(2015)**.
[15] Carl Pritchard, Risk Management, Second. ESI International Arlington, Virginia, **(2001)**.
[16] M. Alemu and A. Omer, "Cloud Computing Conceptual Security Framework for Banking Industry," J. Emerg. Trends Comput. Inf. Sci., vol. 5, no. 12, pp. 921–930, **(2014)**.
[17] M. Alhomidi and M. Reed, "Security Risk Analysis as a Service," in 2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013, **(2013)**, pp. 156–161.
[18] A. Alzahrani, N. Alalwan, and M. Sarrab, "Mobile Cloud Computing: Advantage, Disadvantage and Open Challenge," in Proceedings of the 7th Euro American Conference on Telematics and Information Systems, **(2014)**, pp. 4–7.
[19] H. Rajaei and J. Wappelhorst, "Clouds & Grids: A Network and Simulation Perspective," in Conference: 2011 Spring Simulation Multi-conference, SpringSim '11, Boston, MA, USA, **(2011)**, pp. 143–150.
[20] E. Aruna, A. Shri, and A. Lakkshmanan, "Security Concerns and Risk at Different Levels in Cloud Computing," in 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), **(2013)**, pp. 743–746.
[21] A. Gill, D. Bunker, and P. Seltsikas, "An Empirical Analysis of Cloud, Mobile, Social and Green Computing," in An Empirical Analysis of Cloud, Mobile, Social and Green Computing, **(2011)**, pp. 698–705.
[22] G. Arunkumar and N. Venkataraman., "A Novel Approach to Address Interoperability Concern in Cloud Computing," in Procedia Computer Science, **(2015)**, vol. 50, pp. 554–559.
[23] Hitachi, "How to Improve Healthcare with Cloud Computing," **(2012)**.
[24] S. Bouchenak, G. Gheorghe, G. Chockler, H. Chockler, and A. Shraer, "Verifying Cloud Services: Present and Future," ACM SIGOPS Oper. Syst. Rev., vol. 27, no. 2, pp. 6–19, **(2013)**.
[25] S. Goyal, "Public vs Private vs Hybrid vs Community-Cloud Computing: A Critical Review," International Journal of Computer Network and Information Security, vol. 6, no. 3. pp. 20–29, **(2014)**.
[26] T. Saxena and V. Chourey, "A Survey Paper on Cloud Security Issues and Challenges," in Conference on IT in Business, Industry and Government (CSIBIG), **(2014)**, pp. 1–5.
[27] A. Khrisna and Harlili, "Risk Management Framework With COBIT 5 and Risk Management Framework for Cloud Computing Integration," in 2014 International Conference of Advanced Informatics: Concept, Theory and Application (ICAICTA) Risk, **(2014)**, pp. 103–108.
[28] M. Hadi, "Overview of Cloud Computing Towards to Future Networks," Int. J. Comput. Sci. Innov., vol. 2015, no. 2, pp. 68–78, **(2015)**.
[29] M. Kiran, M. Jiang, D. Armstrong, and K. Djemame, "Towards a Service Lifecycle based Methodology for Risk Assessment in Cloud Computing," in 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, **(2011)**, pp. 450–457.
[30] M. Ahmadalinejad and S. Hashemi, "A National Model to Supervise on Virtual Banking Systems through the Bank 2.0 Approach," ACSIJ Adv. Comput. Sci. an Int. J., vol. 4, no. 1, pp. 83–93, **(2015)**.
[31] A. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security Risks and their Management in Cloud Computing," in 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, 2012, pp. 121–128.
[32] M. Kaur and R. Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing," Int. J. Comput. Appl., vol. 70, no. 18, pp. 16–21, 2013.
[33] Y. Sushmitha, V. Reddy, and D. Reddy, "A survey on Cloud Computing Security Issues," Int. J. Comput. Sci. Innov., vol. 2015, no. 2, pp. 88–96, **(2015)**.
[34] M. Carroll, A. Merwe, and P. Kotzé, "Secure Cloud Computing: Benefits, Risks and Controls," in Information Security for South Africa -2011, **(2011)**, pp. 1–9.

[35] B. Al-shargabi and O. Sabri, "A study of Adopting Cloud Computing from Enterprise Perspective using Delone and Mclean IS Success Model," Int. J. Comput. Sci. Inf. Secur., vol. 14 S1, no. February, p. 5500, **(2016)**.
[36] R. Kumar and S. Rajalakshmi, "Mobile Cloud Computing: Standard Approach to Protecting and Securing of Mobile Cloud Ecosystems," in Proceedings - 2013 International Conference on Computer Sciences and Applications, CSA 2013, **(2013)**, pp. 663–669.
[37] A. Tuli, N. Hasteer, M. Sharma, and A. Bansal, "Exploring Challenges in Mobile Cloud Computing: An Overview," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference). p.6, **(2013)**.
[38] C. LLP, W. Chan, E. Leung, and H. Pili, "Enterprise Risk Management for Cloud Computing," **(2012)**.
[39] NSTAC, "NSTAC Report to the President on Cloud Computing," **(2012)**.
[40] M. Irfan, M. Usman, Y. Zhuang, and S. Fong, "A Critical Review of Security Threats in Cloud Computing," in 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), **(2015)**, pp. 105–111.
[41] B. Karabey and N. Baykal, "Attack Tree Based Information Security Risk Assessment Method Integrating Enterprise Objectives with Vulnerabilities," Int. Arab J. Inf. Technol., vol. 10, no. 3, pp. 297–304, **(2013)**.
[42] N. Ahmed and A. Abraham, "Modeling Security Risk Factors in a Cloud Computing Environment," J. Inf. Assur. Secur., vol. 8, no. 2013, pp. 279–289, **(2013)**.
[43] G. Wahlgren and S. Kowalski, "IT Security Risk Management Model for Cloud Computing: A Need for a New Escalation Approach.," Int. J. E-entrepreneursh. Innov., vol. 4, no. 4, p. 19, **(2013)**.
[44] M. Dhingra, "Review on Information Security Management," in International Conference on Futuristic Trends in Engineering, Science, Humanities, and Technolog, **(2016)**, pp. 1–4.
[45] V. Akshaya and T. Purusothaman, "Business Intelligence as a Service in Analysis of Academic Courses," Int. J. Appl. Eng. Res., vol. 11, no. 4, pp. 2458–2467, **(2016)**.
[46] S.-T. Lai and F.-Y. Leu, "A Security Threats Measurement Model for Reducing Cloud Computing Security Risk," in 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, **(2015)**, pp. 414–419.
[47] E. Cayirci, "Modeling and Simulation as A Cloud Service: A Survey," in Proceedings of the 2013 Winter Simulation Conference, **(2013)**, pp. 389–400.
[48] L. Maghrabi, "The Threats of Data Security over the Cloud as Perceived by Experts and University Students," in 2014 World Symposium on Computer Applications & Research (WSCAR), **(2014)**, pp. 1–6.
[49] Microsoft, "Embracing Cloud in Health: A European Risk Assessment Framework," **(2014)**.
[50] P. Senthil, N. Boopal, and R. Vanathi, "Improving the Security of Cloud Computing using Trusted Computing Technology," Int. J. Mod. Eng. Res., vol. 2, no. 1, pp. 320–325, **(2012)**.
[51] A. Singh and P. Singh, "A Hybrid Security Model for Distributed Cloud Management," Int. J. Comput. Sci. Mob. Comput., vol. 5, no. 2, pp. 39–45, **(2016)**.
[52] K. Jakimoski, "Security Techniques for Protecting Data in Cloud Computing," Int. J. Grid Distrib. Comput., vol. 9, no. 1, pp. 49–56, **(2012)**.
[53] M. Bamiah, S. Brohi, and S. Chuprat, "Cloud Implementation Security Challenges," in Proceedings of 20l21ntemational of Cloud Computing, Technologies, Applications & Management, **(2012)**, pp. 174–178.
[54] P. Hazarika, V. Baliga, and S. Tolety, "The Mobile-Cloud Computing (MCC) Roadblocks," in 2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN), **(2014)**, pp. 1–5.
[55] A. Mxoli, M. Gerber, and N. Mostert-phipps, "Information Security Risk Measures for Cloud-based Personal Health Records," in International Conference on Information Society (i-Society 2014), **(2014)**, pp. 187–193.
[56] CA Technologies, "Healthcare Security Solutions: Protecting your Organization, Patients, and Information," **(2014)**.
[57] P. Srivastava, "Multiple Key Based Architecture to Secure Cloud Database," vol. 4, no. September, pp. 1–7, **(2015)**.
[58] P. Rohmeyer and T. Ben-zvi, "Managing Cloud Computing Risks in Financial Services Institutions," in 2015 Proceedings of PICMET '15: Management of the Technology Age, **(2015)**, pp. 519–526.
[59] P. Laplante, Real-Time Systems Design and Analysis, Third. A John Wiley & Sons, INC., **(2004)**.
[60] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hubsch, and I. Paraskakis, "PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services," in 5th International Conference on Cloud Computing and Services Science (CLOSER 2015), **(2015)**, no. MAY, pp. 206–213.
[61] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," **(2011)**.
[62] P. Anand, J. Ryoo, H. Kim, and E. Kim, "Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection," in IMCOM '16, **(2016)**, p. 8.
[63] G. Gavrilov and V. Trajkovik, "Security and Privacy Issues and Requirements for Healthcare Cloud Computing," ICT Innovations 2012 Web Proceedings. pp. 143–152, **(2012)**.

[64] D. Bernardo, "Utilizing Security Risk Approach in Managing Cloud Computing Services," in 2013 16th International Conference on Network-Based Information Systems, **(2013)**, pp. 119–125.
[65] A. Michalas, N. Paladi, and C. Gehrmann, "Security Aspects of e-Health Systems Migration to the Cloud," in 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom) Security, **(2014)**, pp. 212–218.

Authors

Abdelrafe Elzamly, he got a Ph.D. in Information and Communication Technology from the Technical University Malaysia Melaka (UTeM) in 2016 with a record of about 20 publications. He received his Master degree in Computer Information Systems from the University of Banking and Financial Sciences in 2006. He received his B.Sc. degree in Computer from Al-Aqsa University, Gaza in 1999. He is currently working as Assistant Professor at Al-Aqsa University as a full time. Also, from 1999 to 2007 he worked as a part time lecturer at the Islamic University in Gaza. Between 2010 and 2012 he worked as a Manager in the Mustafa Center for Studies and Scientific Research in Gaza. His research interests are in risk management, software and information systems engineering, cloud computing security, and data mining.

Burairah Hussin, he received his Ph.D. degree in Management Science- Condition Monitoring Modelling, from the University of Salford, UK in 2007. Before that, he received a M.Sc. degree in Numerical Analysis and Programming from the University of Dundee, UK in 1998 and a B.Sc. degree in Computer Science from the University of Technology Malaysia in 1996. He currently works as a Professor at the Technical University Malaysia Melaka (UTeM). He also worked as the Dean at the Faculty of Information and Communication Technology, Technical University of Malaysia Melaka (UTeM). His research interests are in data analysis, data mining, maintenance modelling, artificial intelligence, risk management, numerical analysis, and computer network advising and development.

Abd Samad Hasan Basari, he received a Bachelor degree in Mathematics from the Universiti Kebangsaan Malaysia (UKM) in 1998, Master of Science (IT-Education) from the Universiti Teknologi Malaysia (UTM) in 2002 and a Doctoral degree from the Universiti Teknikal Malaysia Melaka (UTeM) in 2009. He also a certified HTML5 Developer and RapidMiner Analyst. He joined the Faculty of Information and Communication Technology, UTeM in 2003 and became an associate professor in 2013. His current research interests are in computational modeling, decision support system and artificial intelligence.