International Journal of Grid and Distributed Computing
Vol. 9, No. 9 (2016), pp.137-154
http://dx.doi.org/10.14257/ijgdc.2016.9.9.13

A New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations

Abdelrafe Elzamly[1*], Burairah Hussin[2], Samy Abu Naser[3], Khalid Khanfar[4], Mohamed Doheir[5], and Ali Selamat [6], and Abdullah Rashed[7]

[1]*Department of Computer Science, Al-Aqsa University, Gaza, Palestine*
[2,5]*Information & Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia*
[3]*Faculty of Engineering & Information Technology, Al-Azhar University, Gaza, Palestine*
[4]*Department of Information Security, Naif Arab University for Security Sciences, Saudi Arabia*
[6]*Faculty of Computer Science & Information Systems, Universiti Teknologi Malaysia (UTM), Malaysia*
[*] [1]*E-mail: Abd_elzamly@ {yahoo.com, alaqsa.edu.ps}*

Abstract

Despite much research and progress in the areas of cloud computing project, many cloud computing projects have a very high failure rate when it comes to the banking organizations. The aim of this study is to propose a new conceptual framework modelling for cloud computing risk management in banking organizations. There are the main five stages for a successful cloud computing framework in a banking organization as described in Figure 1: Cloud mobility and cloud banking applications, cloud service models, cloud deployment models, cloud risk management models, and cloud security models. As a future work, we will apply the framework in the real banking world to mitigate and control the security issues. A successful framework modelling for cloud computing risk management will greatly improve the probability of cloud computing success in banking organizations.

Keywords: *Cloud Risk Management, Cloud Service Models, Cloud Deployment Models, Cloud Security Models, Cloud Mobility, Cloud Banking Model*

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. The principles of risk management have been introduced in cloud computing to help document, anticipate certain risks, and manage them to ensure job executions are successful. Clouds are more complex environments with further concerns like risk, trust, eco-efficiency, security [1]. Due to the involvement of cloud risk management in monitoring the success of a software project, analyzing potential risks, and making decisions about what to do about potential risks, the risk management is considered the planned control of risk [2]. In addition, risk is an uncertainty that can have a negative or positive effect on meeting project objectives [3]. Cloud computing contend with computation, software, data access and storage services that may not need an end-user knowledge of the physical location and the configuration of the system that is

[*] Corresponding Author

ISSN: 2005-4262 IJGDC

delivering the services [4]. Moreover, they focused on a mobile cloud computing interaction system consisting of multiple mobile devices and the cloud computing facilities [5]. The goal of cloud risk management is identification and recognition of risks at an early stage and then actively changing the course of actions to mitigate and reduce the cloud computing risk [6]. In the process of understanding the factors that contribute to cloud computing success, risk management is becoming increasingly important. Today, cloud computing risk management has become a common practice amongst leading banking organization 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 project manager and team to make better decisions to mitigate cloud-computing risks. Integrating models of cloud computing risk management are considered a new phenomenon in banking organizations, where it requires cloud computing managers and developers to be involved in a project from the concept phase until the mitigating risk phase.This study present a new framework modelling risk management for successful cloud computing in banking organizations. **The aim of this study** is to propose a new conceptual framework modelling for cloud risk management in banking organizations.

Related Work

The cloud computing bank with a somehow commcerial nature, the non-availability of resources, such as liquidity risk, remains [7]. The banking service registers every member of the cloud and stores their credit balance and all agreements they are participating [8]. Further, they proposed artifact model of the software risk management for mitigating risks. Therefore, it has the five levels to mitigate risks through software project [9]. Banking services organizations have shown a significant interest in the adoption of emerging cloud, mobile, social networks and green computing environments for managing the needs of their complex business processes and systems [10]. 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 [11]. In addition, it explained some of cloud security services such as cost benefits and the trusted cloud platform as a service of reusability that improve the cloud security and information technology capabilities [12].

New Conceptual Framework for Cloud Computing Risk Management in Banking Organizations

Indeed, they introduced the conceptual framework for cloud security banking that included components such as security, privacy, legal, compliance and regulatory issues of banking [13]. Further, the cloud risk management components of framework like user requirement self-assessment, cloud service provider's desktop assessment, risk assessment, third-party agencies review, and continuous monitoring. Further, through the cloud risk management framework, the cloud service suppliers can better understand the user's requirements, and the trust between the users and the suppliers is more easily acquired [14]. Indeed, they proposed the new cloud risk management approach to improve the business process level goals that achieve successful for could computing organization by managing, assessing, and mitigating cloud risks [15]. Electronic Data Interchange (EDI) and e-payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking [16]. Moreover, cloud risk management framework is one of security assessment tool to mitigate of threats and vulnerabilities and security issues [17]. In fact, there are many studies were interestingly and describe risk management theoretically, but we need practical models to assess risk and predict risk in software project [19]. On the other hand, they focused on architectural

of software risk components that include deployment and operation in cloud computing lifecycle [20]. According to previous studies, we have divided the framework modelling of cloud banking environment into five stages and components as cloud mobility and cloud banking applications, cloud service models, cloud deployment models, cloud risk management models, and cloud security models as shown in Figure 1.

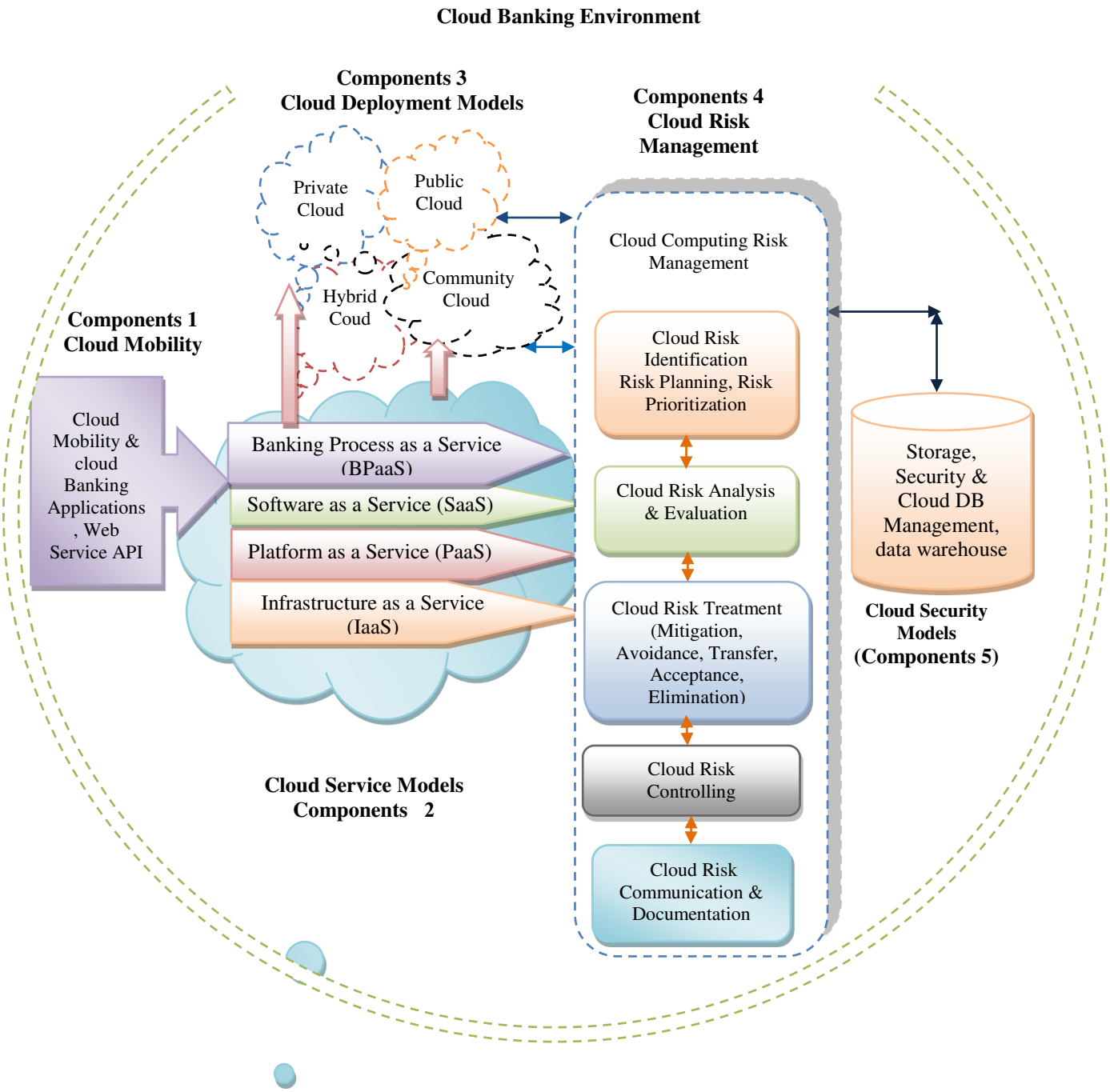


Figure 1. New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations

1.1 Cloud Mobility, Cloud Banking Applications, and Web Service API

Cloud 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 Internet and mobile technologies has led to the popularity of mobile application in different aspects of modern life. Moreover, 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 [21]. The cloud applications are more efficient in decision making process of various organizations but there are several technical factors other than the management perspectives [8]. Furthermore, the banking service manages user and agreement information. The service itself is composed of two associated context services each representing different instance data [22]. Mobile banking (M-Banking) refers to any operation that is related to banking services such as balance check, account transactions, payments. Currently, cloud based M-Banking apps addresses many M-Banking apps issues such as processing speed and storage capacity [21].

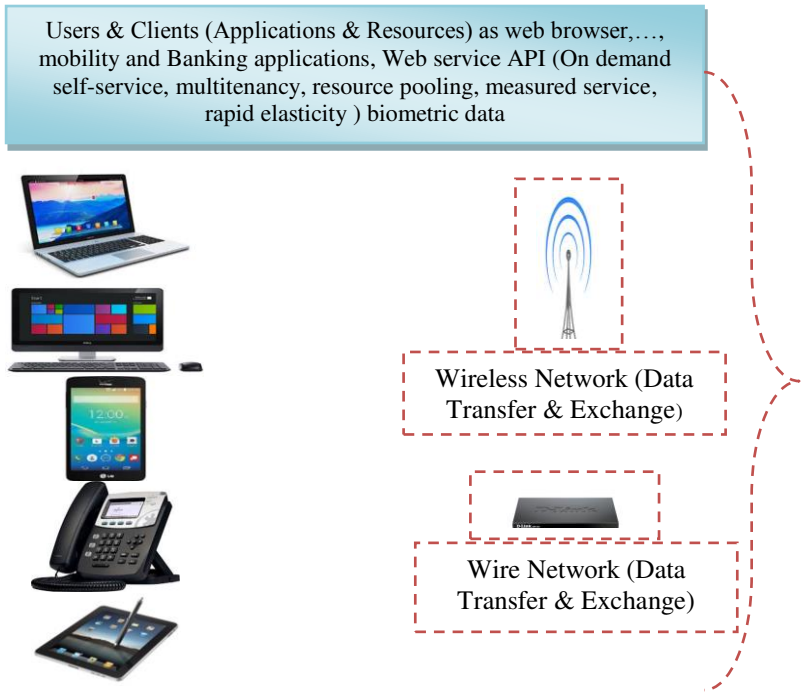


Figure 2. Cloud Mobility, Cloud Banking Applications, and Web Service API

1.2 Cloud Service Models in Cloud Computing

Generally, cloud computing is the new promising technology that enables sharing resources between different enterprises through the Internet in an on-demand manner. Many enterprises are moving toward adopting cloud computing services to gain the benefits of cost reduction of such services [23]. Cloud services are elastic—allowing them to be highly configurable, adaptable and scalable —and require less up-front investment and ongoing operating expenditure than traditional IT models. Based on their business escalation it needs further adoption of modern cloud services if the existing cloud provider fails to offer. Hence the users need interoperability and portability to ship their assets from one cloud to another one [24]. Finally, all four forms of cloud computing can provide computing "on demand" at one or more of four levels. The cloud service model 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 in Figure 3:

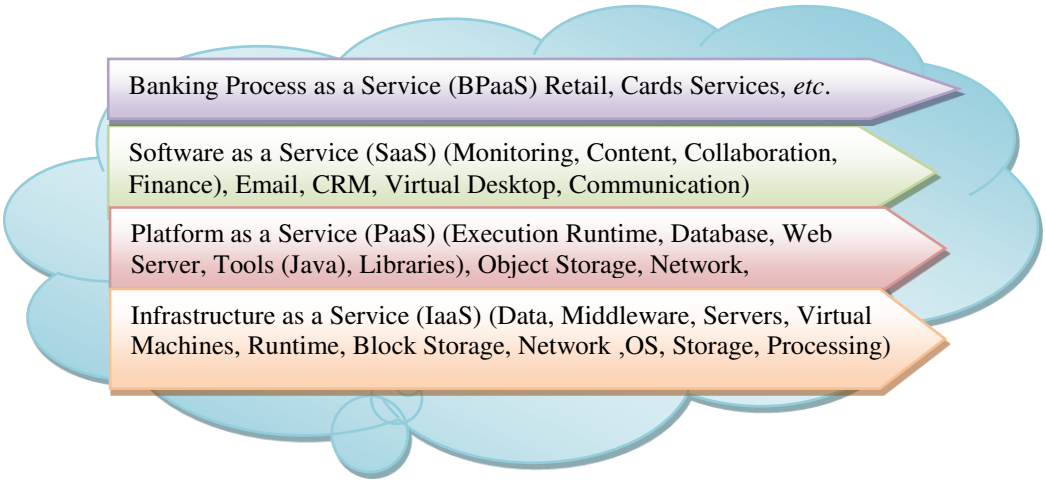


Figure 3. Cloud Service Models

1.2.1 Banking Process as a Service (BPaaS)

The financial establishments such as banks still believe the technology to be connected with many business risks 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 [13]. Therefore, Banking Process as a Service (BPaaS) offers a web-enabled, externally provisioned service for managing business processes. These solutions differ from application clouds by providing end-to-end process support, covering not just software but also people processes such as contact centers [25]. Further, business aspect represents organizations (e.g. banks) that may offer financial or banking services to their customers through mobile banking (e.g. mobile payments). Mobile banking applications can be supported by mobile computing or technology (e.g. 3G, mobile wallet, and mobile payments) [10].

1.2.2 Software as a Service (SaaS)

Software as a service model offers the costumers with the needed software so that the clients need neither to purchase new packages nor to deal with installation, updates, maintenances, and other complexities. The customer makes payment as per use. SaaS solutions are now available for many common business application functions including email [26]. In software as a service model, consumer use hosted application through a web browser. In addition, security and control are services that are the provider's responsibility because the customer has minimal control or extensibility [15].

1.2.3 Platform as a Service (PaaS)

It is based on an environment that supports everything required to complete the lifecycle of building web-based applications or providing cloud applications without the complexity and cost of managing the underlying hardware and software [27]. This enables developers to write and run applications on cloud for quick deployment (Ex: Google app engine *etc.*) [28]. In the PaaS model, the consumer is allowed to write applications that run on the service provider's specific environment. Furthermore, PaaS environment provides you with an infrastructure as well as complete operational and development environments for the deployment of your applications [29].

1.2.4 Infrastructure as a Service (IaaS)

IaaS provides all companies with mostly everything related to computing resources including networks, servers, virtualization, and storage and data center space. This model shares dedicated resources, such as: server, database storage and other peripherals, with contracted clients at pay-and-use cost (Ex: AWS S3, EC2 *etc*.) [28]. In addition, the cloud infrastructure is composed 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 [30]. Currently, IaaS is the main cloud service model. It deals with computers and all other resources like VM (Virtual Machines), server, network and storage. Hence, computers can either be physical or virtual machines, for Example Google compute engine, Amazon EC2, HP Cloud *etc*. Finally, now there is no need to purchase the servers and data centers for application deployment [31].

1.3 Cloud Computing Deployment Models (Delivery Models)

Cloud computing is a model for providing and sourcing information technology services on a "pay-per-use" basis through web-based tools and applications. Cloud computing deployment models generally take one of four forms or a combination of these forms: Private, public, hybrid and community as shown in Figure 4:

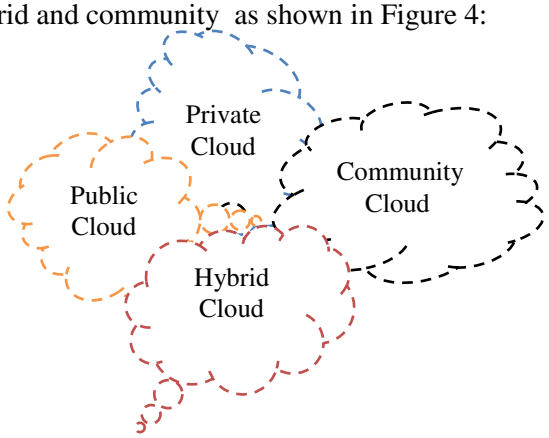


Figure 4 . Cloud Computing Deployment Models

1.3.1 Public Cloud

Public cloud is a type of cloud that is available to everyone; where it is operated and owned by companies to provide quick access to computing resources for other organizations or individuals. In addition, public cloud does not require users to purchase any hardware, software or supporting infrastructure, in which all of these are provided and managed by public cloud providers [4]. Therefore, the advantages of public include [29]: Date availability and continuous uptime, technical expertise, on demand scalability, easy and inexpensive setup, no wasted resources. The outlook on cloud computing services can vary significantly among organizations, because of the inherentence of differences in such things as their purpose, assets held, exposure to the public, threats faced, and tolerance to risk [32].

1.3.2 Community Cloud

Community cloud is usually managed, governed and secured commonly by all the participating organizations and individuals or it can be managed and controlled by a third party service provider. Community cloud is a hybrid form of private cloud designed and operated for a specific group [4]. A community cloud is a public cloud on a smaller scale. It will serve several organizations that support a particular community of users. For example a Linux community cloud would enable developers to share tools common to

Linux development. Currently, the organization would not need to outlay the capital that would otherwise be required to purchase a traditional software license and they would only pay for the use of the software as it was used by the developers. The same risks are associated with community cloud as with public cloud, so consideration of security and privacy are important with community clouds [33].

1.3.3 Private Cloud

It 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]. Private cloud provides more resources control where it works as a self-service interface to control common services, and supports IT staff to quickly deliver and provide on demand IT resources [4]. In this model cloud owner does not share their resources with any other organization. It is set up and maintained by an organization itself [27]. In addition, it is more flexible and reliable to implement fine-grained access control mechanisms to protect the privacy of banking data. In addition, a private cloud provides services to an organization through an intranet [34].

1.3.4 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 [27]. In between these scenarios are hybrid clouds where users complement internal IT resources upon demand with resources from an external vendor [35]. On the other hand, Hybrid cloud is a composition of two, more clouds or multi-clouds (community, private, public) [20]. 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 [36]. Therefore, hybrid clouds offer a greater flexibility to businesses while offering choice in terms of keeping control and security.

1.4 Cloud Computing Risk Management

Historically, the risk is defined as the probability that the real variables and the results may different from those originally measured either positive or the negative impact [37]. Risk of failure is defined as the possibility of suffering harm or loss, or exposure in cloud computing lifecycle [38], [39]. Assessing and managing risk in systems that use cloud services can be a challenge [40]. To the practical extent, the organization should ensure that security controls are implemented correctly, operate as intended, and meet its security requirements. Risk is an uncertainty that can have a negative or positive effect on meeting project objectives [41]. Currently, risk management has become significant for information systems mangers since organizations are spending more on IT projects and becoming more technology-dependent [42]. Integrated framework risk management can be identified as risks and mitigation strategies with the evolving cloud computing paradigm that presents significant opportunities as well as uncertainty [30]. Further, risk management has been proposed as a solution to preserve the quality and integrity of a project by reducing cost escalation [43]. Hence, the success of risk management will greatly improve the probability of software project success [3], [44]–[47]. Risk management is an analytical system to measure risk taking of banks according to predefined regulations. Liquidity management provides comprehensive reports on debts and liquidity that are generated in this system [48]. 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 [48]. Today, cloud computing risk management has become a common practice amongst leading banking organization's success [49]. In the increasing effort to improve development processes and security; recent studies have pointed out to an area of cloud computing risk. There are elements of cloud risk management models for success the project as shown in Figure 5 and Table 1:

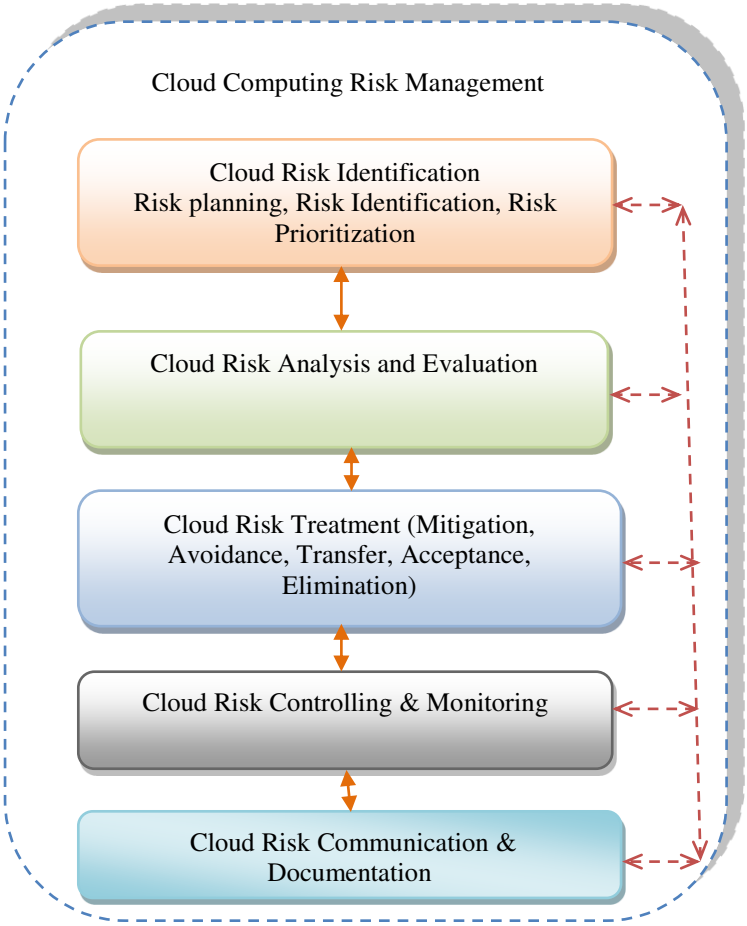


Figure 5. Cloud Risk Management Models

Table 1. Illustrates the conceptual components of Cloud Risk Management Models

Phase	Definition
Cloud Risk Planning	Risk planning includes a set of functions that are identified as continuous activities throughout the software project life cycle [76]. The main inputs to the risk planning according to Taylor [96], are the project charter, guidelines, the contract documents, work breakdown structure (WBS), and network analysis.
Cloud Risk Identification	Risk identification is the process of searching the environment, detecting risks, recognizing their attributes, and estimating their consequences [50]. Techniques that are determined to do caring of the task involve checklists, network analysis, decision trees, examination of decision drivers, cost models, and performance models [51]. However, methods based on qualitative techniques involve checklists of probability risks, questionnaires, interviews and brainstorming, and reviews of plans might also be used.
Cloud Risk Prioritization	Risk prioritization activity considers all aspects of all risk factors and then prioritizes them [52]. One should categorize the software risk factors and select the best strategies based on results analysis to reduce risks after risk planning; identifying software risk factors and risk management techniques have been carried out. The degree of risk depends on two properties: The likelihood and impact on the software project if it works [53]. Risk prioritization makes a ranked ordering of the software risk factors identified and analyzed. Therefore, statistical techniques include risk-exposure analysis, risk-reduction leverage analysis, discriminant analysis (DA), and Delphi [54][55].
Cloud Risk Analysis	According to [56], software project in cloud computing always fail, in order to minimize the impact of risks, risk analysis is required to be carried out. Besides, risk analysis combines exposure and hazard data to analyze the potential for the occurrence of unacceptable adverse effects under real condition [57]. The techniques include performance models, cost models, network analysis, statistical decision analysis, and quality-factor analysis [55].
Cloud Risk Evaluation	Risk evaluation requires a systematic research of random scenarios, including failure rates for the component as well as for the behavior of operator within an evolving environment [58]. Also risk evaluation–decides on risk acceptance by evaluating the risks against an acceptance scale [59]. In addition, the purpose of risk evaluation is to determine the levels of the identified information risks, thus managers can compare them, according to the various levels of information risk, managers will carry out various risk control strategies, and prevent risks from delaying the project [60].
Cloud Risk Treatment (RT)	The nature of the risks within cloud computing will manipulate which of these strategies are suitable to mitigate risk. It is very important to mitigation cloud risks by controls and avoid it [42]. There are four strategies for responding to cloud risks: Mitigation, avoidance, transference, elimination, and acceptance.
Cloud Risk Mitigation	A risk mitigation plan aims to resolve risks as much as potential to reduce the impact of a source of the risk [74].
Cloud Risk Avoidance	Avoidance means taking alternative steps so that the risk likelihood is reduced to zero when using a different types of process [76]. Furthermore, avoidance strategies is applied, if a risk is not accepted and other lower risk choices are available from various alternatives [64].
Cloud Risk	Risk transfer is complete in practice by co-operation teaming project.

Phase	Definition
Transfer	Common examples of risk transfer is also occurred where the insurance is the most practical way of planning for risks [65]. Transference strategies include shifting the management risk to a third party or someone else [63].
Elimination Cloud Risk	When the exposure is unacceptably high or when the cost of elimination is not prohibitive, this is called as elimination of the risk. Usually, risk is eliminated in the case of low cost to respond [62].
Cloud Risk Acceptance	Reasons, impact and consequences of the risk occurrence or exposure are analyzed and understood if risks are accepted [76].
Cloud Risk Controlling (RC)	Controlling–steering the risk reduction is based on the actual effectiveness of the control measures and the levels of risk, deciding on launching of the contingency plans or closing a successfully mitigated risk [59]. Risk is not always avoidable, but it is controllable on software development projects [66]–[68]. Furthermore, risk control in software projects is usually based on constructing a model through synchronization from many developers to manage and prevent conflicts [69].
Cloud Risk Communication & Documentation	According to [65], neither software project managers nor organizations are careful enough to document and archive any lessons learned from the previous project, so that the new future software projects can gain the benefits. Every risk reports and lessons-learned have to be documented and archived, hence software project manager can access software risk file easily.

1.5 Cloud Security Models: Security and Cloud DB Management

Cloud security is a broad topic and can be any combination of policies, technologies, and controls to protect data, infrastructure and services from possible attacks or achieving business objectives. All security domains should work in an effective manner [27]. 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 [20]. In cloud computing technology there is a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others [70]. Further, the primary choice of private cloud is due to its security and in-house management [24]. Security problem is considered as one of the greatest challenges in providing cloud computing service. It's essential for success in cloud services business [71]. Currently, cloud computing security is often an emphasis on the perceived cost and performance benefits of public cloud computing, which tends to overshadow some of the fundamental security and privacy concerns that the organizations and Federal agencies have with cloud computing environments. Determining the security of conjoined complex computer systems [36]. Cloud computing as a resource bank can face similar risks that commercial banks are actually facing, especially liquidity risk or resources and services unavailability [7]. Security issues which are related to the cloud services. Cloud computing supports the distributed service oriented architecture as well as the multi-user and multi-domain administrative system. Hence, that's why cloud computing is more susceptible to the security threats [31]. Security for mobile applications: Presently mobile devices run security checks on devices itself, which costs in terms of computation and power [72]. Security in cloud is a major challenge as many threats and risk are associated with this computing model [73], [74]. When the sensitive data is stored in cloud the main concerns are how it is secured, what are the rules and procedures to protect the data [73]. When customers when migrating to the cloud they trust the third party vendor who ensures the requirements like confidentiality, authenticity and integrity of data. The building blocks of cloud security are [73]: **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.

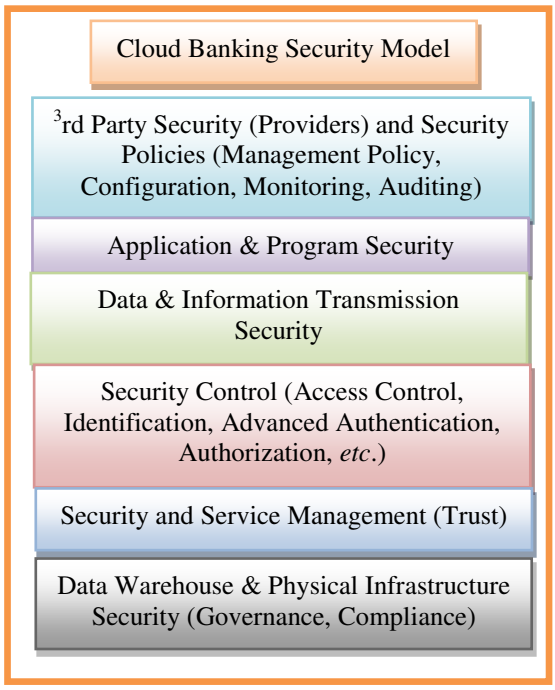


Figure 6 . Cloud Security Models

1.5.1 3rd Party Security (Providers), Security Policies

Indeed, cloud services are accessed and managed by clients via software interface and insecure applications programming interfaces [31]. These, APIs have significant roles in provisioning, monitoring, orchestration and management of the processes running in a cloud computing environment [75]. Some of the security concerns include cyber-attacks and illegitimate control over user accounts [75].

1.5.2 Application & Program Security

Cloud provider should follow a secure development process and also XML signature and XML encryption method should be used to protect applications from XML attacks and web service attacks [27].

1.5.3 Data & Information Transmission Security

Data transmission can be carried as transmission of personal and sensitive data to the cloud server, the transmission of data from cloud server to the client computer. Client's personal and sensitive data may be stored on cloud servers that are not owned by enterprise customers and are remote from the customers. Data stored in the cloud storage resources may be very sensitive data and critical. A cloud security mode should protect these data from loss on damage by providing secure storage servers [76]. Moreover, data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern [32].

1.5.4 Security Control

Traditional access control models that are currently implemented in most cloud solutions are not enough to ensure the security of these environments especially when it is necessary to have a greater flexibility to enable efficient information sharing in critical situations [77]. Authentication is the act of confirming the truth of an attribute of a datum or entity [31]. Information flow control is used to control the information flow from or to cloud becomes very important issue as well, because it's very important to secure the confidentiality of the information that flows from the cloud to the local users.

1.5.5 Security and Service Management

Cloud session management in cloud services are typically hosted on more than one server for increasing the 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, round robin algorithm, *etc.* Management computing resources available on demand Lower cost of new IT infrastructure Payment of use as needed [78]. Furthermore, cloud applications are totally dependent on the ability of cloud users to successfully and securely authenticate themselves for authorized access in a cloud context [36].

1.5.6 Data Warehouse & Physical Infrastructure Security (governance, compliance)

The most prominent issue is the security due to the growing popularity of cloud computing, the security become very important and critical issue. Security is one of the biggest concerns in the cloud, particularly in the case of managing private and confidential data like customer information or credit card information. Compliance in the cloud may also become an issue that may require deploying a private cloud if you do have to secure private data [79]. Therefore, cloud computing moves its application and databases through data centers, while management of data and services are an important security challenges, which have not been fully understood [76]. Regulatory Compliance: By storing data in the cloud, users hand it over to a provider that may have data centres in different geographical locations, countries or even continents. However, organizations that work with sensitive data, such as health records, require complete control over the physical storage location and data access. As a result, storing sensitive data in the cloud complicates adherence to regulatory compliance laws, since such data may fall under different regulations depending on where it is physically stored [80]. 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 [48].

Conclusions

The concern of this study is a framework modelling for cloud computing risk management in banking organizations. Indeed, we have proposed the new conceptual framework modelling for cloud computing risk management that includes five stages: Firstly: Cloud mobility and cloud banking applications; the second model: Cloud service models includes banking process as service (BPaaS), software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS); the third model: Cloud deployment models like public cloud, community cloud, private cloud, hybrid cloud ; the fourth model: Cloud risk management models such as cloud risk planning, cloud risk identification, cloud risk prioritization, cloud risk analysis, cloud risk evaluation, cloud risk treatment, cloud risk controlling and monitoring, cloud risk communication and

documentation; finally, cloud security models include 3rd party security (providers), security policies (management policy, configuration, monitoring, auditing) and privacy, application & program security, data & information transmission security, security control, security and service management (Trust), data warehouse & physical infrastructure security (governance, compliance). As a future work, we will apply the framework modelling for cloud risk management on a real world bank to mitigate and control the security issues by using artificial neural network algorithms and optimal techniques. Furthermore, successful framework modelling for cloud computing risk management will greatly improve the probability of cloud computing success in banking organizations.

Acknowledgements

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

References

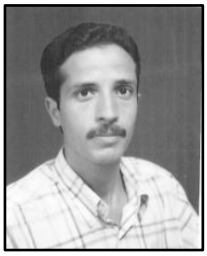
[1] M. Kiran, M. Jiang, D. Armstrong, and K. Djemame, "Towards a Service Lifecycle based Methodology for Risk Assessment in Cloud Computing," in *2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing*, **(2011)**, pp. 450–457.
[2] A. Elzamly and B. Hussin, "Estimating Stepwise and Fuzzy Regression Analysis for Modelling Software Design Project Risks," *Asian J. Math. Comput. Res.*, vol. 3, no. 4, pp. 234–241, **(2015)**.
[3] 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)**.
[4] N. Oktadini and K. Surendro, "SLA in Cloud Computing: Improving SLA's Life Cycle Applying Six Sigma," in *International Conference on Information Technology Systems and Innovation (ICITSI) 2014*, **(2014)**, no. November, pp. 24–27.
[5] Y. Wang, X. Lin, and M. Pedram, "A Nested Two Stage Game-Based Optimization Framework in Mobile Cloud Computing System," in *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, **(2013)**, pp. 494–502.
[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] M. Kefel and B. Mohamed, "Risk Management in Cloud Computing," in *2013 Third International Conference on Innovative Computing Technology (INTECH)*, **(2013)**, pp. 127–131.
[8] K. Chard, S. Caton, O. Rana, and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks," in *2010 IEEE 3rd International Conference on Cloud Computing*, **(2010)**, pp. 99–106.
[9] A. Elzamly, B. Hussin, and N. Salleh, "Methodologies and Techniques in Software Risk Management Approach for Mitigating Risks: A Review," *Asian J. Math. Comput. Res.*, vol. 2, no. 4, pp. 184–198, **(2015)**.
[10] 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.
[11] 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.
[12] 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)**.
[13] 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)**.
[14] F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, and X. Huo, "A Risk Management Framework for Cloud Computing," in *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, **(2012)**, pp. 476–480.
[15] M. Mac, "Toward Business-driven Risk Management for Cloud Computing," in *2010 International Conference on Network and Service Management*, **(2010)**, pp. 238–241.
[16] S. Islam, "An Algorithm for Electronic Money Transaction Security (Three Layer Security): A New Approach," *International Journal of Security and its Applications*, vol. 9, no. 2. pp. 203–214, **(2015)**.

[17] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments," in *10th IEEE International Conference on Computer and Information Technology (CIT 2010)*, **(2010)**, pp. 1328–1334.
[18] M. Su, H. Li, S. Yang, and J. Lu, "A Service Level Agreement for the Resource Transaction Risk based on Cloud Bank Model," in *Proceedings of the 2012 International Conference on Cloud Computing and Service Computing, CSC 2012*, **(2012)**, pp. 198–203.
[19] A. Elzamly, B. Hussin, and N. Salleh, "Top Fifty Software Risk Factors and the Best Thirty Risk Management Techniques in Software Development Lifecycle for Successful Software Projects," *Int. J. Hybrid Inf. Technol.*, vol. 9, no. 6, pp. 11–32, **(2016).**
[20] 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.
[21] 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.
[22] M. Hadi, "Overview of Cloud Computing Towards to Future Networks," *Int. J. Comput. Sci. Innov.*, vol. 2015, no. 2, pp. 68–78, **(2015)**.
[23] 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)**.
[24] 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.
[25] M. Grindle, J. Kavathekar, and D. Wan, "A New era for the Healthcare Industry-Cloud Computing Changes the Game," **(2013)**.
[26] 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.
[27] 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.
[28] 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.
[29] 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).**
[30] C. LLP, W. Chan, E. Leung, and H. Pili, "Enterprise Risk Management for Cloud Computing," **(2012)**.
[31] 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.
[32] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," **(2011)**.
[33] Hitachi, "How to Improve Healthcare with Cloud Computing," **(2012)**.
[34] E. Cayirci, "Modeling and Simulation as A Cloud Service: A Survey," in *Proceedings of the 2013 Winter Simulation Conference*, **(2013)**, pp. 389–400.
[35] 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.
[36] NSTAC, "NSTAC Report to the President on Cloud Computing," **(2012)**.
[37] A. Kamaruddin, "Development of an Early Software Project Risk Assessment Application Using Case-Based Reasoning," Universiti Teknologi MARA, **(2006)**.
[38] J. Dhlamini, I. Nhamu, and A. Kachepa, "Intelligent Risk Management Tools for Software Development," in *Proceeding SACLA "09 Proceedings of the 2009 Annual Conference of the Southern African Computer Lecturers" Association*, **(2009)**, pp. 33–40.
[39] G. Conroy and H. Soltan, "ConSERV, a Project Specific Risk Management Concept," *Int. J. Proj. Manag.*, vol. 16, no. 6, pp. 353–366, Dec. **(1998)**.
[40] A. Elzamly and B. Hussin, "Managing Software Project Risks (Analysis Phase) with Proposed Fuzzy Regression Analysis Modelling Techniques with Fuzzy Concepts," *J. Comput. Inf. Technol.*, vol. 22, no. 2, pp. 131–144, **(2014)**.
[41] A. Elzamly, B. Hussin, N. Salleh, and A. S. Shibghatullah, "Managing and Controlling Design Process Issues by Using Stepwise Approach Modelling," *Res. J. Appl. Sci. Eng. Technol.*, vol. 13, no. 2, pp. 85–97, **(2016)**.
[42] F. Al-Musawi, A. H. Al-Badi, and S. Ali, "A Road Map to Risk Management Framework for Successful Implementation of Cloud Computing in Oman," in *2015 International Conference on Intelligent Networking and Collaborative Systems*, **(2015)**, pp. 417–422.
[43] A. Elzamly and B. Hussin, "Managing Software Project Risks with Proposed Regression Model Techniques and Effect Size Technique," *Int. Rev. Comput. Softw.*, vol. 6, no. 2, pp. 250–263, **(2011)**.
[44] A. Elzamly and B. Hussin, "Mitigating Software Maintenance Project Risks with Stepwise Regression

Analysis Techniques," *J. Mod. Math. Front.*, vol. 3, no. 2, pp. 34–44, **(2014)**.
[45] A. Elzamly and B. Hussin, "A Comparison of Stepwise And Fuzzy Multiple Regression Analysis Techniques for Managing Software Project Risks: Analysis Phase," *J. Comput. Sci.*, vol. 10, no. 10, pp. 1725–1742, **(2014)**.
[46] A. Elzamly and B. Hussin, "Classification and Identification of Risk Management Techniques for Mitigating Risks with Factor Analysis Technique in Software Risk Management," *Rev. Comput. Eng. Res.*, vol. 2, no. 1, pp. 22–38, **(2015)**.
[47] K. Khanfar, A. Elzamly, W. Al-Ahmad, E. El-Qawasmeh, K. Alsamara, and S. Abuleil, "Managing Software Project Risks with the Chi-Square Technique," *Int. Manag. Rev.*, vol. 4, no. 2, pp. 18–29, **(2008)**.
[48] 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)**.
[49] A. Elzamly, B. Hussin, and B. ASH, "Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 8, pp. 137–158, **(2016)**.
[50] C. Pandian, *Applied Software Risk Management: A Guide for Software Project Managers*. Auerbach Publications is an imprint of the Taylor & Francis Group, **(2007).**
[51] 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)**.
[52] P. Jalote, *Software Project Management in Practice*. Addison Wesley, **(2002)**.
[53] J. Hallows, *Information Systems Project Management: How to Deliver Function and Value in Information Technology Projects*, Second. AMACOM, **(2005)**.
[54] A. Elzamly, B. Hussin, S. Naser, and M. Doheir, "Predicting Software Analysis Process Risks Using Linear Stepwise Discriminant Analysis: Statistical Methods," *Int. J. Adv. Inf. Sci. Technol.*, vol. 2015, no. June, pp. 108–115, **(2015)**.
[55] B. Boehm, "Software Risk Management: Principles and Practices," *IEEE Softw.*, vol. 8, no. 1, pp. 32–40, **(1991)**.
[56] M. Holcombe, *Running an Agile Software Development Project*. John Wiley & Sons, Inc., **(2008)**.
[57] R. Layton, J. Smith, P. Macdonald, R. Letchumanan, P. Keese, M. Lema, R. Layton, J. Smith, P. Macdonald, R. Letchumanan, P. Keese, and M. Lema, "Building Better Environmental Risk Assessments," *Front. Bioeng. Biotechnol.*, vol. Jul, **(2015)**.
[58] P. Webern, G. Medina-Oliva, C. Simon, and B. Iung, "Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance Areas," *Eng. Appl. Artif. Intell.*, vol. 42, no. 1, pp. 115–125, Jul. **(2010)**.
[59] J. Miler, "A Method of Software Project Risk Identification and Analysis," Gdansk University of Technology, **(2005)**.
[60] J. Deng and Y. Bian, "Constructing a Risk Management Mechanism Model of ERP Project Implementation," in *International Conference on Information Management, Innovation Management and Industrial Engineering*, **(2008),** pp. 72–77.
[61] A. Zafra-Cabeza, M. Ridao, and E. Camacho, "An Algorithm for Optimal Scheduling and Risk Assessment of Projects," *Control Eng. Pract.*, vol. 12, no. 10, pp. 1329–1338, Oct. **(2004)**.
[62] John Horch, *Practical Guide to Software Quality Management*. Artech House, INC., **(2003)**.
[63] S. Kan, *Metrics and Models in Software Quality Engineering*, Second. Addison Wesley, **(2002)**.
[64] J. Walewski, "International Project Risk Assessment: Methods, Procedures, and Critical Factors," The University of Texas at Austin, **(2003)**.
[65] J. Taylor, *Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware, and Integration Initiatives*. AMACOM © 2004, **(2004)**.
[66] A. Elzamly and B. Hussin, "Evaluation of Quantitative and Mining Techniques for Reducing Software Maintenance Risks," *Appl. Math. Sci.*, vol. 8, no. 111, pp. 5533–5542, **(2014)**.
[67] A. Elzamly and B. Hussin, "Managing Software Project Risks (Planning Phase) with Proposed Fuzzy Regression Analysis Techniques with Fuzzy Concepts," *Int. J. Inf. Comput. Sci.*, vol. 3, no. 2, pp. 31–40, **(2014)**.
[68] 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)**.
[69] N. V and K. Iyakutti, "Bayesian Statistics Software Approach For Risk Control on Complex Software Projects," *Int. J. Eng. Res. Technol.*, vol. 3, no. 12, pp. 1062–1068, **(2014)**.
[70] 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)**.
[71] 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.
[72] 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)**.
[73] 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)**.

[74] M. Doheir, B. Hussin, A. S. H. Basari, and M. Alazzam, "Structural Design of Secure Transmission Module for Protecting Patient Data in Cloud-Based Healthcare Environment Mohamed," *Middle-East J. Sci. Res.*, vol. 23, no. 12, pp. 2961–2967, **(2015)**.
[75] 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.
[76] S. B and M. Siddappa, "A Novel Method of Designing and Implementation of Security Challenges in Data Transmission and Storage in Cloud Computing," *Int. J. Appl. Eng. Res.*, vol. 11, no. 4, pp. 2283–2286, **(2016)**.
[77] D. Ricardo, C. Westphall, and C. Westphall, "A Dynamic Risk-based Access Control Architecture for Cloud Computing," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, **(2014)**, p. 9.
[78] G. Gavrilov and V. Trajkovik, "Security and Privacy Issues and Requirements for Healthcare Cloud Computing," *ICT Innovations 2012 Web Proceedings*. pp. 143–152, **(2012)**.
[79] 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)**.
[80] 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 (Software and Information Systems Engineering) 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 at 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.

Samy Abu Naser, he got a Ph.D. in Computer Science from North Dakota State University, USA in 1993. He received his M.Sc. Degree in Computer Science from Western Kentucky University, USA in 1989. He received his B.Sc. Degree in Computer Science from Western Kentucky University, USA in 1987. He is currently working

as a professor in Al-Azhar University, he is the Dean of the Faculty of Engineering and Information Technology in AL-Azhar University, he worked as Deputy Vice President for Planning & Quality Assurance, and he worked as a deputy dean of the Faculty of Engineering and Information Technology in Al- Azhar University. His research interests are in data mining, artificial intelligent, and risk management.

Khalid Khanfar, He is a professor in Computer Science. He earned his Ph.D. in Computer Science from Illinois Institute of Technology, USA. He served in many administrative positions such as Head of Computer Science Department, Head of Computer Information Systems, Dean of the Faculty of Information Technology, Dean of the Faculty of Science and Information Technology Dean of Scientific Research, Dean of Students Affairs, Deputy Vice President for Academic Affairs, and Vice President for Planning and Development. He published many papers in IT fields. Currently, he is the Head of Information Security Department at Naif Arab University for Security Sciences, Saudi Arabia. His research interests are in Networking, Information and Networking Security, Computer Architecture, and Algorithms Performance.

Mohamed Doheir, he is currently a PhD candidate in Health Care Management in University Technical Malaysia Malaka (UTeM). He received his M. Sc. degree in Internet working Technology from University Technical Malaysia Malaka (UTeM) in 2012. He received his B.Sc. Degree in Educational Computer Science from Al Aqsa University- Gaza, Palestine in 2006. His research interests are in Health care, Cloud Computing and Network Simulation.

Ali Selamat, he is a Professor at Faculty of Computing, University Teknologi Malaysia. Currently, he is a Chief Information Officer (CIO) Director of Information and Communication Technology Center, Universiti Teknologi Malaysia (UTM). He is nominated as a Chair of IEEE Computer Society Malaysia Chapter, 2016 and appointed as a fellow at UTM-IRDA Centre of Excellence in Media and Games technology UTM. He was a Research Dean for a Research Alliance in Knowledge Economy (K-Economy RA) which is currently renamed as Smart Digital Community Research Alliance UTM. He was the Vice Chair of IEEE Computer Society Malaysia, 2014 and 2015, respectively. He was an auditor of IEEE Malaysia Section and a bursary of IEEE Computer Society Malaysia in 2013. Previously, he was an IT Manager at School of Graduate Studies (SPS), UTM. He was a head of Software Engineering Research Group (SERG), K-Economy Research Alliance, UTM, a head of Software Engineering Department and the head of Postgraduate Studies Department, at Faculty of Computer Science & IS UTM from 2005 - 2012. Currently, he is the editor of International Journal of Intelligent Information Database Systems (IJIIDS), Inderscience publisher, International Journal of Digital Content Technology and its Applications (JDCTA) and International Journal of Advancements in Computing Technology (IJACT), which are the SCOPUS indexed

journals. He is currently the editorial board of Vietnam Journal of Computer Science, Springer Publications. His research interests include software engineering, software process improvement, software agents, web engineering, information retrievals, pattern recognition, genetic algorithms, neural networks and soft computing, computational collective intelligence, strategic management, key performance indicator and knowledge management.

Abdullah Rashed, he is got his Ph.D. in Information Systems from degree in Computer Information Systems from the University of Banking and Financial Sciences in 2004. He got his MSc. Information systems from the University of Banking and Financial Sciences in 2000. He got his Bsc. In computer sciences form the Applies Sciences in 1997. He served as Post-Doc fellow with Agoritmi Centre, Portugal from 2009-2014. His research fields include information security, user behavior and acceptance for the new technology.