Volume 6, Issue 2
April 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations

Abdelrafe Elzamly[1], Burairah Hussin [2], Samy S. Abu Naser[3], Tadahiro Shibutani[4], and Mohamed Doheir[5]

[1]*Department of Computer Science, Al-Aqsa University, Gaza, Palestine*
[2,5] *Information & Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia*
[3]*Department Information Technology, Al-Azhar University, Gaza, Palestine*
[4]*Institute of Advanced Sciences, Yokohama National University, Yokohama, Japan*
***E-mail**: [3]abunaser@alazhar.edu.ps*

ABSTRACT

The aim of this study is to predict critical cloud computing security issues by using Artificial Neural Network (ANNs) algorithms. However, we proposed the Levenberg–Marquardt based Back Propagation (LMBP) Algorithms to predict the performance for cloud security level. Also LMBP algorithms can be used to estimate the performance of accuracy in predicting cloud security level. ANNs are more efficiently used for improving performance and learning neural membership functions. Furthermore, we used the cloud Delphi technique for data gathering and analysis it in this study. In this study, the samples of 40 panelists were selected from inside and outside Malaysian banking organizations based on their experienced in banking cloud computing. However, we have indicated that the LMBP is nonlinear optimization models which used to measure accuracy of the prediction model, the Mean Square Error (MSE) are measured to determine the performance. The performance is goodness, if the MSE is small as shown in Table 1. This work has been conducted on groups of cloud banking developers and IT managers. As future work, we intend to combine another optimal technique with ANNs algorithms to predict and mitigate critical security cloud issues. Though, positive prediction of critical cloud security issues is going to surge the probability of cloud banking success rate.

Keywords: C*loud banking organization, Cloud Computing, Cloud Security Issues, , Artificial Neural Network, Levenberg Marquardt Algorithm, Back Propagation Algorithm,.*

1. NTRODUCTION

Although much research and progress in the area of cloud computing project, a lot of cloud computing projects have a very high failure rate particularly when it is related to the banking area. However, several serious cloud security issues like data protection and integrity, quality of services(QoS), Portability and Interoperability, and mobility need to be controlled and mitigated before cloud computing able to apply adoptive widely [1]. In addition, cloud computing has several advantages but cloud computing in banking organizations is suffering from a lot of cloud security issues. The aim of cloud risk management is identification and evaluation of cloud security issues at an early stage to predict the cloud computing security level [2]. Today, cloud computing risk management became a mutual practice amongst leading banking organization success. In the increasing effort to improve development processes and security; new studies have led to cloud computing risk area. Risk management aids software project manager and team to do improved decisions to mitigate cloud-computing risks. The objective of this study is predicting performance for cloud computing security issues using Levenberg–Marquardt based Back Propagation (LMBP) algorithms.

2. LITERATURE REVIEW

Cloud computing risk management consists of computing processes, methods and techniques that are useful to mitigate cloud computing risk failure. Security risk management is increasingly becoming significant in a diversity of areas linked to information technology (IT), for example: telecommunications, banking information systems, cloud computing[3]. Moreover, the cloud banking model is a resource management modeling founded on economic philosophies. Its function like commercial banks in loan and deposit business [4]. Cloud security is a general subject and any grouping of policies, controls, and technologies to safeguard data, services and infrastructure from conceivable attacks. Additionally, current researches focused on providing security technologies, instead of business features such as services stability, availability and continuity [5]. This study is going to predict the critical cloud issues in Malaysian banking organizations. Actually, they presented the conceptual framework for cloud security banking that involved components for example security, legal, privacy, compliance and regulatory issues of banking [6]. As stated by previous studies we split the framework modeling cloud computing to five phases as mobility and banking application, Cloud Deployment Models (CDM), cloud risk management models (CRMM), Cloud Service Models (CSM), and cloud security model (CSM) as follows: Firstly, mobility related to the possibility of moving and taking place in diverse locations and through multiple times using any kind of portable devices like smart phones, Personal Digital Assistants (PDAs) and wireless laptops. Nonetheless, mobile banking related to any operation that linked to banking services like balance check, payments and receiving banking SMS via a mobile device, and account transactions [7]. Secondly, CSM depend on

Volume 6, Issue 2
April 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

some state of the art of web technologies like Application Programming Interface (API), Web Services, Web 2.0, and etc. [8]. Also, CSM is split into four categories that are offered from a cloud provider: Software as a Service (SaaS), Platform as a Service (PaaS), Banking Process as a Service (BPaaS), and Infrastructure as a Service (IaaS). Thirdly, CDM can be split into four dissimilar types: Public cloud is made obtainable to the general public or a huge industry group and are possessed by a third party selling cloud services [9]. Private Cloud is functioned and possessed by a single organization or company that focuses on controlling the mechanism of virtualizing resources and automating services those are used and tailored by many lines of business and essential groups [4]. Community cloud falls among public and private clouds with regard to the target set of consumers [10]. Community cloud, this model is used by a specific group of community within an organization that has the same worry, objectives or security necessities [11]. Hybrid cloud uses both public and private cloud methods, where it smears the strategic notions of the services of public cloud with the basis of the private cloud. Fourthly, Cloud Risk Management (CRM): in Cloud computing, risk required to be taken into consideration in all phases of interactions and investigated at every service stage in relation to the possessions that should be protected [12]. Besides, there are diverse types of risks that bank management should be protected against. For numerous banks, the main risk is credit risk but there are several other risks that supervising authorities must notify banks about connected criteria and require them to follow [13]. There are eight phases for effective cloud risk management like Cloud Risk Planning Phase (CRPL), Cloud Risk Analysis (CRA) phase, Cloud Risk Identification(CRI) phase, Cloud Risk Prioritization(CRP) phase, Cloud Risk Evaluation(CRE) phase, Cloud Risk Treatment(CRT) phase includes four strategies for responding to cloud risks: cloud risk mitigation, cloud risk avoidance, cloud risk transfer, cloud risk elimination, cloud risk acceptance, Cloud Risk Controlling(CRC) phase, and Cloud Risk Communication & Documentation (CRCD) phase. Finally, Cloud Security Issues Models (CSIM): cloud security is a very common topic and any grouping 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 [14].

3. CLOUD SECURITY ISSUES

Though, classification of critical security issues in cloud banking is needed to be highlighted in this section [15]: 3rd Party (Providers) and Policies Security Issues: Lack of standards, Service Level Agreement (SLAs), Governance, Legally and policy, Dependency, Lack of transparency, Cloud service provider viability, Malicious insiders, Regulatory compliance & requirements, Shared technology issues, Unknown risk profile, Trusted cloud, Abuse cloud computing; Application and program (software) security issues: Authentication, Authorization, Insecure Interfaces API's, Availability and Mobility, Portability and Interoperability; Data and Information Security Issues: Privacy, Confidentiality, Data Protection, Data Limitations and Segregation, Data integrity and scavenging, Data Location, Data Loss/Leakage, Detection and Recovery, Hijacking of Account or Service & Traffic; Security Control & Network Issues: Information flow Controlling, Intrinsic Constrains of Wireless Network, Network Access Schemes, Bandwidth, Anonymity and Network Traffic Analysis, Network Security, Virtual Network Protection, Limited control, Distributed Denial of Service (DDoS), Heterogeneity in Mobile cloud Devices, Platform Reliability and Latency; Security and Service Management Issues: Session Management, Identity/Access Management, Quality of Service (QoS), IT organizational changes; Physical Infrastructure Security Issues: Flexibility Infrastructure, Single Point to Attack and Failure, High-value cyber-attack targets, the multi-tenancy, Scalability, Cost.

4. EMPIRICAL STRATEGY

The Delphi technique use to collect data as qualified informants, so we focused on two cloud developers groups and cloud IT managers in banking organizations. In this regard the Delphi study is modified to three phases like identifying, analyzing, and evaluating as described in Figure 1. The data are collected by secondary data and Delphi study. In current study, the population samples of forty panelists were chosen from inside and outside Malaysian banking organizations according to their experienced in cloud banking. Actually, we measure the probability of occurrence according to a 10 scales (1= "very low probability of occurrence risk" and 10 = "very high probability of occurrence risk"), and the brutality of the cloud security issues described on a 10 scales (1= "very low influence risk" and 10 = "very high impact risk". Actually, we used 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, experienced of cloud managers and cloud developers. The Delphi method is collected data and aggregated of cloud security issues. In fact, we divided the phases of cloud Delphi technique into three phases such as identifying, analyzing, and evaluating. However, we illustrate the concept of Delphi technique for identifying and classifying cloud security issues in Figure 1 as follows:

Cloud Delphi Technique

Phase 1: Identifying

- Collected data and aggregated of cloud security issues.
- Select the experts from both inside and outside the banking organization.
- Divide panelist to two groups cloud

Volume 6, Issue 2
April 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Figure 1: Illustrates the steps of cloud Delphi study of collecting data [16]

5. METHODOLOGY (MATERIALS & METHODS)

However, the data gathered for this study to be used in the modelling is getting from the managers and cloud developers in banking organizations. We propose Artificial Neural Network (ANNs) for predicting cloud security issues in banking organizations. In order to manage and predict performance of cloud computing security level, we can use artificial neural networks methods. In order to establish the intelligent approaches, first we need to model the relationship between cloud computing issues. In addition, artificial neural networks modelling are used as nonlinear statistical data model to predict cloud-computing issues. Of course, IT managers and cloud developers must use practical approaches, methods, and tools to predict cloud security issues in banking organization. Indeed, the back-propagation algorithm is used in layered feed- forward ANNs where the artificial neurons are structured in layers, and lead their signals "forward", and then the errors are transmitted backwards. The neural network gets input from input layers and yields the output to the output layer and the processing can be done in hidden layers. There must be only one input and output layer, however, there may be an arbitrary number of hidden layers [17-19]. Additionally, the BP algorithm should minimize these errors, till the ANN learns the training data. Typically the training initiates with random weights, and the learning objective is to modify them so that the error is reduced [17-19]. The design of procedures for predicting cloud security issues using Levenberg-Marquardt (LM) Based Back Propagation (BP) Algorithm as follows:

1. Collect and prepare the data for cloud security issues based on Cloud Delphi Technique.
2. Assign an estimated probability of occurrence and severity of cloud security issues based on security models.
3. Build a network analysis
4. Train the network: It generates the neural network from a Cloud Delphi dataset with known output data cases.
5. Test the network: A trained neural networks are used to test how well it does at prediction of known and new output values.
6. Predict cloud security issues based models by using artificial neural networks for evaluating the performance impact of CSI. A trained neural network is used to predict unknown output value.

6. RESULTS AND DISCUSSION

Indeed, we used the Levenberg–Marquardt based Back Propagation (LMBP) Algorithms, as nonlinear optimization to predict the performance. So we illustrate the mean square error and Regression (R) values for the Training, Validation and Testing as in Table 1.

Table 1 Illustrates the MSE and Regression values for the three types

Types	Samples	Training data (input)%	MSE	R
Training	28	70%	4.94160×e-7	9.95213×e-1
Validation	6	15%	8.75807×e-6	9.79262×e-1
Testing	6	15%	1.95378×e-5	9.49600×e-1

Table 1 shows that the overall Mean Square Error which measure the average squared errors between the output data and targets data and Regression (R) which measure correlation between the actual outputs data and targets data for training, validation and testing samples.

The accuracy of prediction is observed, when the values of R are closest to 1. Hence, if the dataset was trained by using (LMBP) Algorithms, the performance obtained was in 3 epochs with 10 hidden neurons yields. The results indicated that the LMBP algorithms are very efficiently for testing and training networks. Although, a two-layered feed forward network hidden neurons and networks are trained using LMBP Algorithms as shown in Figure 2.

Volume 6, Issue 2
April 2017

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

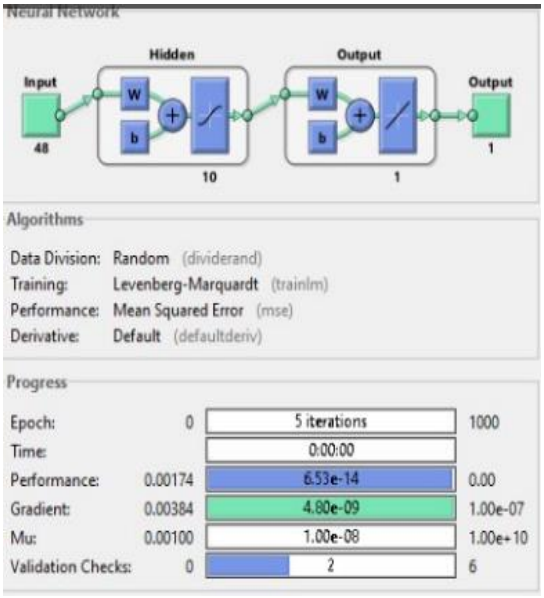

Figure 2 architecture and algorithms and progress of ANN system

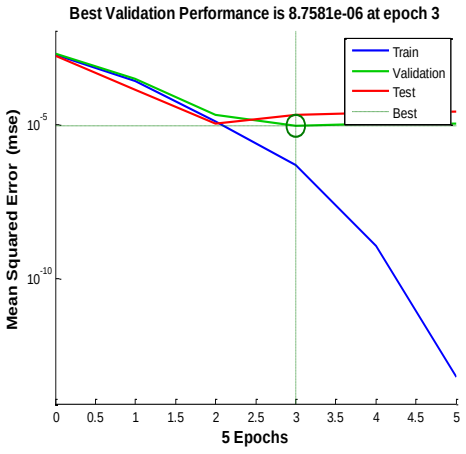

Figure 3 Performance of LMBP Algorithm (MSE vs. Epochs)

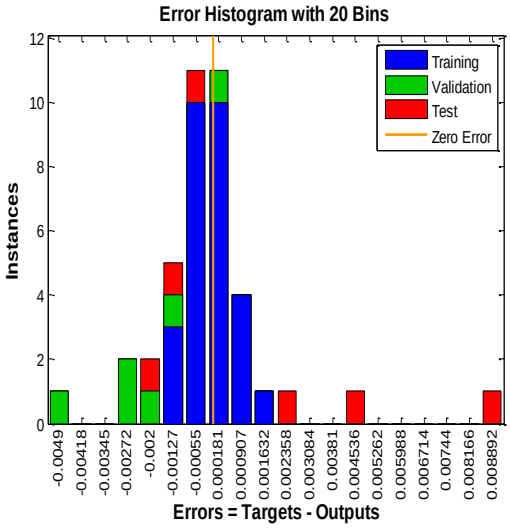

Figure 4 error histogram with 20 bins based LMBP

Indeed, it is trained to measure the performance of networks by using LMBP algorithms in Matlab R2013b. Furthermore, we estimated the best validation performance 0.0000087581 at epoch 3 in Figure 3 and the error histogram with 20 bins is illustrated in Figure 4. Therefore, regression R values are measured the correlation between outputs and targets. Hence, the results in the regression analysis plot are perfect correlation between the outputs and targets as in Figure 5. In addition, the one mean a close relation between outputs and targets, zero a random relationship. LMBP is nonlinear optimal models which used to measure accuracy of the prediction model, the Mean Square Error (MSE) are measured to determine the performance. The performance is goodness, if the MSE is small.

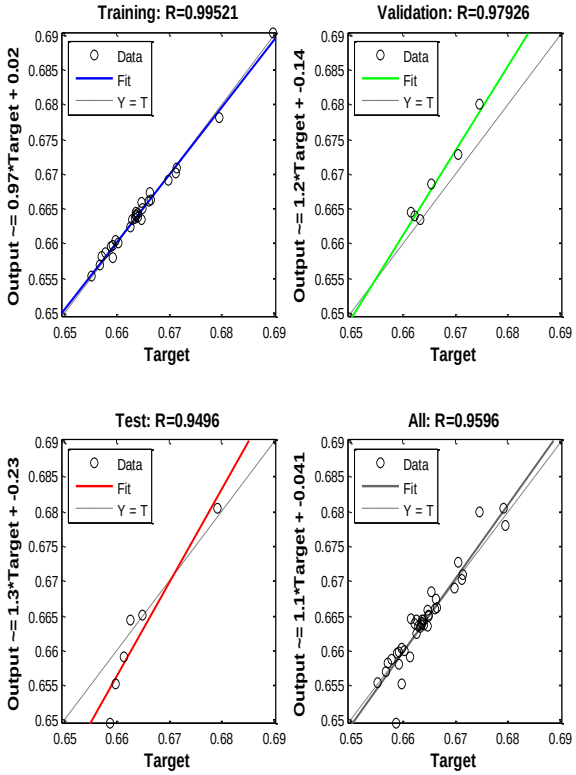

Figure 5 Regression Analysis Plot - Levenber g-Marquardt Backpropagation Algorithm

7. CONCLUSIONS

The concern of the study is to predict critical cloud computing security issues using Artificial Neural Network (ANNs) algorithms. However, we presented the Levenberg–Marquardt based Back Propagation (BP) Algorithms to predict the performance for cloud security level. Also LMBP algorithm is applied to

estimate and test the performance of accuracy for predicting cloud security level. ANNs are more efficiently used for improving performance and learning neural membership functions. Indeed, the performance of cloud security is analyzed by using LMBP to give the best performance in the predicting models. Furthermore, we used the cloud Delphi technique for data gathering and analyzing it in this study. In this study, the samples of 40 panelists were selected from inside and outside Malaysian banking organizations based on their experienced in banking cloud computing. However, we have indicated that the LMBP is nonlinear optimal models which used to measure accuracy of the prediction model and to reduce the error between the actual outputs and targets for training process, the Mean Square Error(MSE) are measured to determine the performance. The performance is goodness, if the MSE is small as shown in Table 1. As future work, we intend to use another optimal technique with Artificial Neural Network algorithms to predict and mitigate critical security cloud issues.

8. 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] 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] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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)**.

[7] 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.

[8] 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.

[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] 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)**.

[11] 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.

[12] 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.

[13] 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)**.

[14] 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.

[15] A. Elzamly, B. Hussin, S. A. Naser, K. Khanfar, M. Doheir, A. Selamat, and A. Rashed, "A New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 9, pp. 137–154, **(2016)**.

[16] 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)**.

[17] B. Ibrahim and A. Shanavas, "An Approach to Predict SOA Security Vulnerabilities using Feed Forward Artificial Neural Networks," *SIJ Trans. Comput. Networks Commun. Eng.*, vol. 3, no. 4, pp. 54–58, **(2015)**

[18] S. Abu Naser, "Predicting learners performance using artificial neural networks in linear programming intelligent tutoring system." International Journal of Artificial Intelligence & Applications vol. 3, no. 2, pp.65-73, **(2012)** .

[19] S. Abu Naser, et al. "Predicting Student Performance Using Artificial Neural Network: in the Faculty of Engineering and Information Technology." *International Journal of Hybrid Information Technology*, vol. 8 no. 2, 221-228**,(2015)**

Authors' information

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 in 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.

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 worked as 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.

Tadahiro Shibutani, He received the Ph.D. degree in mechanical engineering from Kyoto University, Kyoto, Japan, in 2000. He was a Visiting Scholar with the Center of Advanced Life Cycle Engineering, University of Maryland, in 2007. He is currently Associate Professor of Center for Creation of Symbiosis Society with Risk with Yokohama National University, Yokohama, Japan. His research interests include physics of failure, health monitoring, and risk management for engineering systems.

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.