Information Security and Computer Fraud, 2016, Vol. 4, No. 1, 1-8
Available online at http://pubs.sciepub.com/iscf/4/1/1
© Science and Education Publishing
DOI:10.12691/iscf-4-1-1

Assessment of E-Voting Risks Using AHP Method for the Omani Government Election

Faisal Al Amry*, ChengJack Kie

Faculty of Industrial Management, University Malaysia Pahang, TunRazak Highway, Kuantan, Pahang, Malaysia
*Corresponding author: alamryfaisal@gmail.com

Abstract The purpose of this paper is twofold; to investigate the risks involving with e-voting and to evaluate the risk management of policy of e-voting. In the country of Oman, the Ministry of Interior (MOI) has already implemented an e-voting system making use of the e-Authentication technique, which uses the existing National ID Card to authenticate citizens for voting. This new e-voting system will give solutions that shall allow all citizens to come to election points and get authenticated through their National ID Card before proceeding to the vote. The solution shall be hosted within the current National ID System, taking advantage of the electronic authentication of the cards while enhancing these capabilities with functions specific to the election process, ensuring election rights and introducing vote timestamp storage in the cards. However; review and observation within Ministry of Interior (MOI) of Oman concluded that there is no documented Risk Management Plan that can foresee risks, estimate impacts, and define responses to issues relating with risks involving voting process in the country of Oman. In the context of e-voting systems, risk management is regarded as the characterization of the e- Voting System in Oman; this consists of defining the system for the risk assessment. This is the assessment of system elements, such as hardware, software, system interfaces, data and information, personnel actions, and the mission of the e- Voting system. This is followed by the Identification Threat Sources, Vulnerability Identification, Controls Analysis, Threat Likelihood, performance of impact Analysis and risk level. It is then followed by the Development of Risk Mitigation Strategies and finally the documentation of Results.

Keywords: *risk, e-voting, risk management, parliamentary election, risk modelling, AHP, Ministry of Interior (MOI)*

Cite This Article: Faisal Al Amry, and ChengJack Kie, “Assessment of E-Voting Risks Using AHP Method for the Omani Government Election.” *Information Security and Computer Fraud*, vol. 4, no. 1 (2016): 1-8. doi: 10.12691/iscf-4-1-1.

1. Introduction

The term risk which can be understood as a situation involving exposure to danger or the possibility of suffering harm or loss is in fact an inherent part of business and public life. According to the definition in the Online Business Dictionary [1], risk is “a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action”. While risk management can be defined according to [2]as a continuous process that depends directly on the changes of the internal and external environment of the organization. [3] defines risk management as the process developed under a decision analytical framework, leading to quality decisions with an optimal profile of outcomes associated with uncertain events (desirable or undesirable). [4] defines risk management as the process of identifying risk, planning, assessing the risk and then conducting control measures. There has not been any significant change on the nature of the definition of risk management but it has been extensively used in many areas of science and social studies. Poor or inadequate risk management is the major cause of information technology project failures according to a number of researchers [5,6,7].

Most of the researchers concluded on different time periods of 2007, 2012 and 1999 that problems of budget overruns due to the underestimation of the actual cost during budgeting and project failures are frequently associated with poor risk analysis and management. In this research questionnaires and the Analytic Hierarchy Process (AHP) will be used to quantitatively construct effective tool for the assessment of managing risk involving electronic voting (e-voting) in the country of Oman. Starting with questionnaire for risk assessment that will provide ample analysis of the risks involving e-voting. After achieving sufficient knowledge of the risks relating with e-voting, then we will construct AHP model to find out the best possible way or the optimal technique of choosing appropriate risk mitigation process. AHP is a structured multi-attribute decision method[8], which provides a proven, effective means to deal with complex decision making and allows better, easier, and more efficient weighting and analysis of selection criteria. Every organization has a purpose, and assets, and organizational objectives to be achieved.

Poolsappasit [9] indicates that in recent days all organizations employ the automated information technology (IT) systems to focus greater benefits for their tasks. It is a must that top management of organizational unit to ensure that the organization has the capacity to fulfil its tasks. From the security point of view, the organization needs capabilities to accomplish the maintenance of the required level of safety in the face of real-world threats. Risk management plays a crucial role in determining how to protect the security of information assets of an organizational and carry on its missions from IT-related risks Effective risk management is an essential part of a successful IT project. Risk management is a process that allows IT managers to balance between cost of the protective measures and gains in mission capability. A system administrator has to make a decision and choose an appropriate security plan that maximizes the resource utilization. However, making the decision is not a trivial task. Most organizations have tight budgets for IT security; therefore, the chosen plan must be reviewed as thoroughly as other management decisions.

As shown in Poolsappasit [9] risk management is broken into three components namely risk assessment, risk mitigation, and evaluation. Risk assessment is the practice of shaping the extent of negative impacts associated with the system. The output of this process helps decision maker to identify appropriate controls for reducing the risk in the risk mitigation process. As mentioned by [10] risk mitigation can be either proactive management or reactive risk response. It can be greatly improved if information is readily available, is timely and accurate. Risk mitigation is used to identify measures which when implemented will minimize the risk or even remove it from the system. After risk has been found to be unacceptable then mitigation should provide an appropriate risk-reducing measures, such as: Reducing the severity of potential consequences; reducing the probability of occurrence harmful effects or reducing the exposure to that risk.

The evaluation process includes a process of risk acceptance which requires senior management to sign a statement accepting the residual risk and authorizing the security hardening operation. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities. Traditional risk analysis perceives risk as an inevitable phenomenon that is characteristic of all future events as yet immaterialized. The concept of risk is usually expressed as a function of the uncertainty associated with such events.

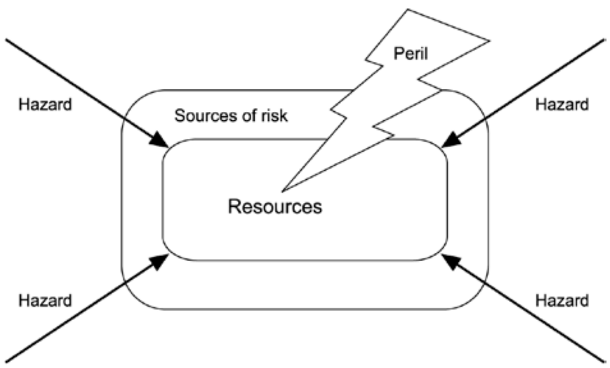

Figure 1. Risk Identification Frame, Adopted from [2]

The severity of loss is measured by the deviation from the expected value of the event's possible outcomes. Risk identification is a process that reveals and determines the possible organizational risks as well as conditions, arising risks. By risk identification the organization is able to study activities and places where its resources are exposed to risks according to Williams [11]. Figure 1 Illustrates risk identification elements which can be described by the following basic components: *sources of risks; hazard factors; perils;* and *exposures to risk.* Sources of risk are elements of the organizational environment that can bring some positive or negatives outcomes. Hazard is a condition or circumstance that increases the chance of losses or gains and their severity. An error of the firm management about the market expansion for a given product is an example for a hazard factor activity that determines the system risk.

Peril is something that is close to the risk and it has negative, non-profitable results. Peril can happen at any time and cause unknown, unpredictable loses. Peril is the cause of losses. Resources exposed to risk are objects facing possible losses or gains. As suggested by Yeo [12] the terms 'risk' and 'uncertainty' are sometimes used interchangeably. However, more often, the concept of risk is expressed in terms of the probability of occurrence (frequency), and the severity of loss (or gain) that will be a consequence of such an occurrence. They will be affected if the risk event occurs.

Nevertheless, Risk Management is becoming a key factor within organizations since it can minimize the probability and impact of information technology project threats and capture the opportunities that could occur during the information technology project life cycle [13]

2. Back Ground of Electronic Voting System (e-voting)

According to [14] the electronic voting (e-voting) system can be defined as is a voting system in which the election data is recorded, stored processed primarily as digital information. As stated by [15] in the recent years, governments have embraced the idea of using information technology (IT) and to recognize e-voting systems a viable method used to replace the paper ballot voting mode in elections. The e-governments is now still considered as mentioned by [16] where it improves many government services; which enables the adoption of electronic voting (e-voting) machines. E-voting is still popular topic worldwide; however the e-voting techniques and systems have not been widely accepted and deployed by society due to various concerns and problems as claimed by [17].

The number of issues associated with many existing e-voting techniques is lack of transparency, security issues (software and hard failures), accessibility (if people can access e-voting e.g. the right to vote), and usability (e.g. ease of use of the e-voting system). These issues create major risks that can hinder the election process. Many of these issues were present since the introduction of the electronic voting; especially with controversial presidential elections and the recent news involving the Secure Electronic Registration and Voting Experiment (SERVE).

According t Schaupp and Carter [18], SERVE were considered insecure by three of its 12 evaluators. SERVE, which was developed by the US Department of Defence (DOD), allows absentee military voters in 50 countries and seven states to cast their votes via the internet. The first use of this new technology occurred in South Carolina's presidential primary on 3rd February, 2004. DOD plans to eventually expand the program to handle the votes of nearly six million US military personnel and civilians living abroad. However, security experts warn that existing internet technology cannot guarantee the integrity of e-voting.

Accenture, who jointly created SERVE with the DOD, stresses that it was only designed to be an experiment to collect data on voter reactions to casting ballots online. The potential consequences can be disastrous such as grand election fraud. Since the opportunities for fraud provided by electronic voting machines surpass all the opportunities available previously. For example, a corrupt insider, working for one of the vendors of widely-used voting machines, could hide malicious code in the software. In attempt to tackles these issues in the USA; the Help America Vote Act (HAVA) was passed by Congress in 2002 mandates reform of the election processes of all states as mentioned by the Verified Voting Organization [19] and also by Schaupp and Carter [18],). HAVA provides funding to replace obsolete voting technologies such as punch cards and lever machines with more modern technologies such as precinct based optical scanners and direct recording electronic (DRE) voting machines. While a survey in the UK voters in 2002 asked them which voting method they would prefer to use in the next general election. Eighty-seven percent said they would like to be able to vote online using their home of office computer [18].

An application to electronic voting is given that matches the features of the best current protocols with significant efficiency improvements by using a mathematical construct which provides a cryptographic protocol [26]. Since there are security concerns that surround internet transaction[18] investigating such questions, are citizens willing to vote online? Would citizens prefer online voting to traditional means of casting a ballot? There are several studies [20,21,22] caution against the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. SERVE is a very good example of the major issues experienced in e-voting and he project was cancelled in 2004 due to its pertaining problems. Vulnerabilities in SERVE occurs because the Internet is independent of national boundaries, an election held over the Internet is vulnerable to attacks from anywhere in the world. A shown in [23], not only could a political party attempt to manipulate an election by attacking SERVE, but so could individual hackers, criminals, terrorists, and even other countries. Some of the core issues were the lack of voter-verified Audit system, insider attacks, Lack of Control of the Voting Environment, lack of privacy etc.

However there are other researchers who have done more studies using computer technologies to improve elections [24,25,26,27]. The issues of transparency, security, accessibility and usability of e-voting have been considerably improved and people achieved a sense of reliance on the e-voting system. A good example of such improvement is the cases of the country of Estonia according to [24] were a successful election by using e-voting was achieved.

3. Oman Government Election System

The country Oman; officially called the Sultanate of Oman is an Arab state in Southwest Asia on the southeast coast of the Arabian Peninsula. The election process starts before one year of election. The steps for participating elections are pretty simple and fair. Any Omani citizens those who reached 21 years within on the 1st January of the election year and possess a valid citizen card or passport can register for vote. The Wally offices are responsible for the registration process. An application designed for the process and the registration recording through this application. A scanned copy of citizens resident card or passport copy and a printed confirmation of registration, keeps for further reference. The election applications running disconnected computers (offline); hence a separate application provides for the Wally officers to back up the local database and write to a CD and send to the ministry for the synchronization of the data.

This activity will take place every week until the last date of voter registration. Every week each Wally offices send the backup CD of their database. The administrators of the ministry will dump all the data to a staging database and crosscheck each name and ID along with the scanned copy provided to them. Once any mismatch found, they rectify the error and to make the database error free. Each of the registered voters needs to cross check with Royal Oman Police (ROP) for their validity of the resident card and name correction. The cross checking are done from the Ministry of Interior (MOI) against the ROP database and with the staging database. This checking will reveal, whether the citizen are using the same card with unique card number issued finally from ROP and the furnished details are matching with ROP database. Once the crosschecking is finished the data will be transferring to the central database and available for updates or remaining process. The grounds solution to the old system problems is to implement the e-voting project in Oman. The problems of the old system are a voter cannot vote using either passport or ID Card (The voter should only use ID Card); it is difficult to tract a person since the electoral ink was used to identify the voted person, while even some of the voters refuses to mark the electoral ink. The non-elected candidates are trying to complaint about the system, like the fraud voting is possible in case that the people could erase the election ink on their nail, and choose second voting centre to vote. And finally the backup servers or PC's increase the cost almost double of actual amount. The new e-voting system uses the E-Authentication technique which uses the existing National ID Card to authenticate citizens for voting in the national elections. The solution shall allow all citizens to come to election points and get authenticated through their National ID Card before proceeding to the vote. The solution shall be hosted within the current National ID System, taking advantage of the electronic authentication of the cards while enhancing these capabilities with functions specific to the election process, ensuring election rights and introducing vote timestamp storage in the cards.

The registered voters should update any changes relating to their Wilayat (meaning Province in Arabic) due to the relocation of the area, relocation of work or marriage can submit the application to the authorities for change or update his voting Wilayat and once the application is approved, the voting Wilayat of the voter can be changed, this process is called as update. This data also need to crosscheck with the Royal Oman Police. Once the voter list is finalized it will announce officially and the list will be published for public access so any complaints related the list can be registered, if found valid a committee will take necessary actions to resolve it. Updating or editing of the details are also possible on this stage. Candidate registration should register any Omani citizen who reaches 21 years, are eligible for applying as candidate in elections. The applications will scrutinizing by higher authorities, once his application approved then his photographs and other details will be recorded in to the ministry database.

After shortlisted the candidates, each Wilayat candidate list will be officially published and any complaints related candidate list can be officially given and necessary actions will betaken by the committee. A change in the candidate list is still possible until the final day of list finalization. After finalizing the candidate list, next step is to proceed for ballet paper printing. Every ballet sprinted with name and photograph of each candidate in Wilayat base. The ballets are highly secured with an embossed water mark for preventing the scanned or photo copying of the ballet. And it carries a barcode to find genuineness of the ballets. Once the ballets reach the counting machine, the machine can read the votes as well the barcode and embossed mark. Any kind of imitation or fake ballets can be found and keep away from counting. Few voters or citizens are unfortunate since they are black listed; they are not able to vote due to some reason; for example those who working for some special department or those who punished for some anti-national activities etc. A list will be populated from Royal Oman Police and that list will be kept separately in database. And the time of voting while entering the user data or card if the voter is black listed it will be displayed. The employees those who working for election and the citizens working for other embassies in GCC countries need to do their votes, so need to conduct other election before the Election Day.

In Oman, the management risk in e-voting system is crucial matter and it is very important to handle it carefully. This is the risk associated with people working with MOI or to individuals associated with the operation election process in Oman. The management of this risk is a key element in the MOI`s information security program and provides an effective framework for selecting the appropriate security controls for the e-voting system.

4. Methodology

The research design is the logical sequence that connects the empirical data produced by research to the study's initial research questions and ultimately to its conclusions (Yin, 1994). One of the principal purposes of the research design is to help avoid the situation in which the collected data does not address the initial research question (Robson, 1993). Much research in the social sciences and management spheres involves asking and obtaining answers to questions through conducting surveys of people by using questionnaires, interviews and case studies (Fellows and Liu, 1997). The aim of this research is to develop a model for e-voting risk assessment for the ministry of interior of Oman. This will be achieved through the use of statistical data analysis and AHP decision making model that will reduce and manage electoral risks.

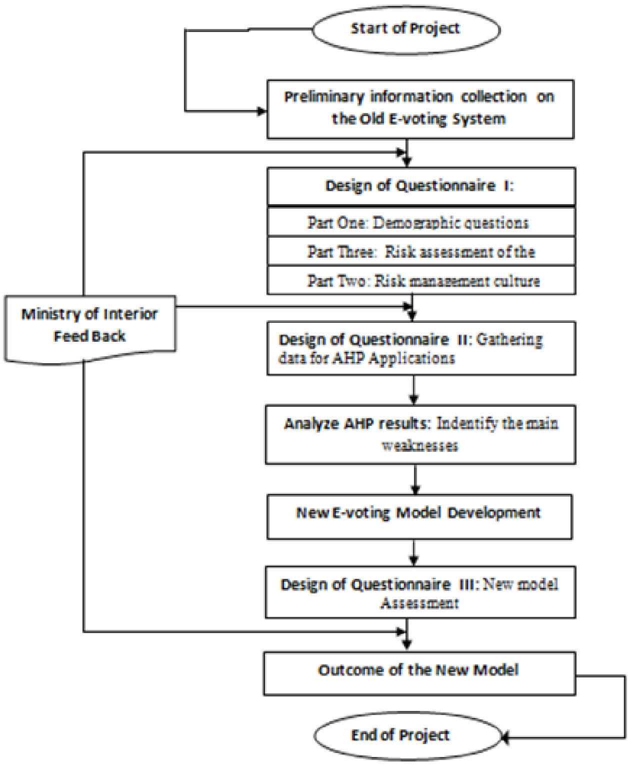

Figure 2. Research Design

To achieve this aim, collecting data for AHP and statistical model is needed to formulate the model. In order to achieve this purpose, one interview session was conducted and three set of questionnaires were distributed. Figure 2 illustrates the research design flow chart.

4.1. Analytical Hierarchy Process(AHP)

The Analytical Hierarchy Process (AHP) and survey method will be used in this research. In this section only AHP will discuss since the survey method is considered not necessarily significant in the literature review.AHP has been largely applied to macro complex and real problem, and the most addressed decision themes are product and process design and, managing the supply chain. As shown in Subramanian & Ramanathan [28], most of AHP application are case study oriented and only a few papers aimed at contributing to AHP modeling before applying to practical problems. The review of the researchers has found that significant research gap exists in the application of AHP in the areas of forecasting, layout of facilities and managing stock [28]. The application AHP in risk management projects is considered modest since there is extensive research indicated strong applications of AHP in risk management. Samvedi et al. [29] proposed a supply chain risk index, which captures the level of risk faced by a supply chain in a given situation. Their work indicates an effort towards quantifying the risks in a supply chain and then consolidating the values into a comprehensive risk index. As concluded by Samvedi et al. [29] in their technique for order preference by similarity to the ideal solution (TOPSIS) a robust risk management method which integrates fuzzy analytical hierarchy process (AHP). Using AHP risk management on various projects such energy managements and of solar-thermal power plant projects, design and selection of public policies, and on construction projects as indicated in [8,30,31]. Aragonés-Beltrán et al. (2014) work reviewed the current state of the art of solar-thermal power plant projects, and then proposed a decision models based on the AHP. As concluded by Aragonés-Beltrán et al. [31], the managing Board can reject unfeasible projects before investing heavily in them. Aminbakhsh [8] proposed a safety risk assessment framework is presented based on the theory of cost of safety (COS) model and the analytic hierarchy process (AHP). The main contribution of the proposed framework is that it presents a robust method for prioritization of safety risks in construction projects to create a rational budget and to set realistic goals without compromising safety [8]. It is very clear that litterateur on AHP applications in e-voting is very limited and modest. The closest AHP application e-voting is the research of Moreno-Jiménez et al. [30] proposing a methodology for the design and selection of public policies based on the cognitive democratic model known as e-Cognocracy.

AHP is employed in resolving two issues of e-Cognocracy as mentioned in [30] one is checking the robustness of the model, do the conclusions remain stable when the hierarchy of the problem is slightly modified and second considering the stability of the solutions when confronted with small changes in the judgments of e-Cognocracy. Therefore, there exists a significant research gap on the applications of AHP in e-voting and in general for all e-government services.

4.2. The Application of AHP for Assessing E-Voting

The analytic hierarchy process (AHP) is a structured technique for organizing and analyzing complex decisions. It was developed by Thomas L. Saaty in the 1970s and has been extensively studied and refined since then. According to [32] the AHP can be defined as structured multi-attribute decision method. The main advantage of AHP is its capability to check and reduce the inconsistency of expert judgments. While reducing bias in the decision making process, this method provides group decision making through consensus using the geometric mean of the individual judgments. Since 1980s the research in AHP still continues according to some recent reviews [8,29,33].

Since AHP is an Eigen value approach to the pair-wise comparisons. It also provides a methodology to calibrate the numeric scale for the measurement of quantitative as well as qualitative performances. The scale ranges from 1/9 for *'least valued than'*, to 1 for *'equal'*, and to 9 for *'absolutely more important than'* covering the entire spectrum of the comparison [28].

4.3. Data Collection for the AHP Model

In this part we raise questions pertaining to AHP method. This questionnaire will finally present the weights for the risk management in e-voting. A questionnaire was created that was specially designed questionnaire for AHP. It is distributed and administered to ten (10) experts. The experts are from the Ministry of Interior. It is anticipated at least three of the following factors will be used: Operator authentication, Reliability, Delectability, Availability of system, Immunity to attack, Integrity of votes, Traceability, Recoverability, Fault tolerance and Isolation.

4.4. Steps of Applying AHP

AHP can help decision makers to: examine a complex problem with a number of possible solutions, evaluate and prioritize alternatives, and organize the information and judgments used in decision making. The analytic hierarchy process allows the relative independent judgments made by people to be used in a more formalized decision making process.AHP derives scales of values from pair wise comparisons in conjunction with ratings and is suitable for multi objective, multi criterion, and multi-actor decisions with any number of alternatives [8]. AHP involves assessing scales rather than measures; hence, it is capable of modeling situations that lack measures (e.g., modeling risk and uncertainty).

AHP is comprised of three main principles: decomposition level of the structure, comparison of judgments, and hierarchical decomposition level (or synthesis) of priorities. Decomposing a decision problem into its constituent parts facilitates building hierarchies of criteria to determine the importance of each criterion. Some key and basic steps involved in AHP methodology are described in Table 1 as shown below.

Table 1. Steps of AHP method

1.	State the problem.
2.	Broaden the objectives of the problem or consider all actors, objectives and its outcome.
3.	Identify the criteria that influence the behavior.
4.	Structure the problem in a hierarchy of different levels constituting goal, criteria, sub-criteria and alternatives.
5.	Compare each element in the corresponding level and calibrate them on the numerical scale. This requires $n(n - 1)/2$ comparisons, where n is the number of elements with the considerations that diagonal elements are equal or '1' and the other elements will simply be the reciprocals of the earlier comparisons.
6.	Perform calculations to find the maximum Eigen value, consistency index CI, consistency ratio CR, and normalized values for each criteria/alternative.
7.	If the maximum Eigen value, CI, and CR are satisfactory then decision is taken based on the normalized values; else the procedure is repeated till these values lie in a desired range.

AHP helps to incorporate a group consensus. Generally this consists of a questionnaire for comparison of each element and geometric mean to arrive at a final solution. In AHP computing the vector of criteria weights is very essential step. The weighting is mainly determined by the decision makers, who conduct the pair wise comparisons, if there are n evaluation criteria, the decision-makers have to conduct $C(n,2)=n(n-1)/2$ pair wise comparisons [32].

In order to compute the weights for the different criteria, the AHP starts creating a *pairwise comparison matrix* A. The matrix A is a $m \times m$ real matrix, where m is the number of evaluation criteria considered. Each entry a_{jk} of the matrix **A**represents[1] the importance of the *j*th criterion relative to the *k*th criterion. If a_{jk}> 1, then the *j*th criterion is more important than the *k*th criterion, while if a_{jk}< 1, then the *j*th criterion is less important than the *k*th criterion. If two criteria have the same importance, then the entry a_{jk} is 1. The entries a_{jk} and a_{kj} satisfy the following constraint:

$$(a_{jk})x\left(a_{kj}\right)=1$$

Obviously, a_{jj}= 1 for all *j*. The relative importance between two criteria is measured according to a numerical scale from 1 to 9, as shown in Table 2, where it is assumed that the *j*th criterion is equally or more important than the *k*th criterion [8]. The phrases in the "Interpretation" column of Table 2 are only suggestive, and may be used to translate the decision maker's qualitative evaluations of the relative importance between two criteria into numbers. Table 2 shows the evaluation hierarchy structure of EC risk factors. There are three evaluation criteria in the objective level of technical, including C/S security risk, physical security risk and requirements risk. Then the evaluation measurement of ratio scale is employed to conduct pair wise comparison to clarity the relative importance of each attribute.

Table 2. Relative Scores.

Value of ajk	*Interpretation*
1	jandkare equally important
3	jis slightly more important than k
5	jis more important than k
7	jis strongly more important than k
9	jis absolutely more important than k

It is also possible to assign intermediate values which do not correspond to a precise interpretation. The values in the matrix **A** are by construction pairwise consistent. On the other hand, the ratings may in general show slight inconsistencies. However; these do not cause serious difficulties for the AHP.

5. Results of AHP Analysis

AHP model was developed using Microsoft Excel as the software tool. This AHP model will carry-out decisions on the identification of the most risky areas of e-voting security. Here the considered risk elements are shown in Table 3. These are in fact considered as the most common factor of security risks of e-voting system. These variables have been constructed from the literature as indicated in Cunha et al. [34].

Table 3. Security risks of e-voting system

SECURITY (S)		100,00%
S1	Operator authentication	11%
S2	Reliability	15%
S3	Detect-ability	8%
S4	Availability of system	14%
S5	Immunity to attack	17%
S6	Integrity of votes	9%
S7	Traceability	5%
S8	Recoverability	8%
S9	Fault tolerance	9%

Considering relevant security, transparency, usability and accessibility and their sub-criterion for an e-voting system used for the Portuguese parliament general elections, [34] then established an auditing procedure based on AHP. Here only five variables have been chosen to use for the AHP analysis as shown in Figure 3. These variables are based on the data from questionnaire for AHP by which 10 experts at the MOI were given to judge the highest and lowest security risks of e-voting system. Three steps will be used to create the complete AHP model using Ms excel and steps are as follow: step one pair wise comparison, step two normalization and step three consistency analyses.

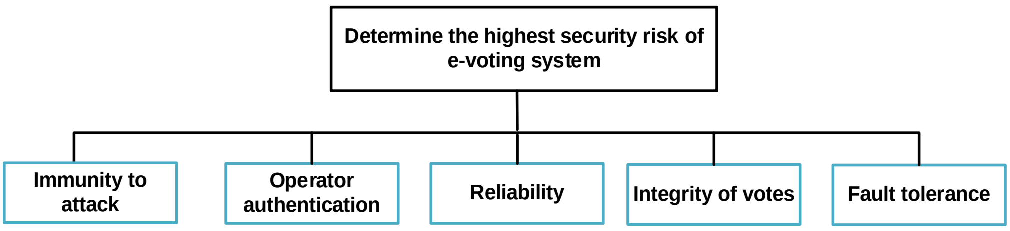

Figure 3. Chosen variables of security

The following excel tables show the detailed process of the AHP modelling. Table 4 below shows the pair-wise comparison of the selected risk factors of the e-voting system. The criteria in the row are being compared to the criteria in the column**.** Table 5 below shows the normalization or the standardized matrix of the selected risk factors of the e-voting system. This step is to normalize the matrix by totalling the numbers in each column.

Table 4. Pair-wise Comparison

	Reliability	Operator authentication	Immunity to attack	Integrity of votes	Fault tolerance
Reliability	1.00	3.00	3.00	5.00	7.00
Operator authentication	0.33	1.00	0.33	3.00	5.00
Immunity to attack	0.33	3.00	1.00	3.00	3.00
Integrity of votes	0.20	0.33	0.33	1.00	3.00
Fault tolerance	0.14	0.20	0.33	0.33	1.00
SUM	2.01	7.53	5.00	12.33	19.00

Table 5. Standardized Matrix

	Reliability	Operator authentication	Immunity to attack	Integrity of votes	Fault tolerance
Reliability	0.50	0.40	0.60	0.41	0.37
Operator authentication	0.17	0.13	0.07	0.24	0.26
Immunity to attack	0.17	0.40	0.20	0.24	0.16
Integrity of votes	0.10	0.04	0.07	0.08	0.16
Fault tolerance	0.07	0.03	0.07	0.03	0.05
SUM	1.0	1.0	1.0	1.0	1.0

Each entry in the column is then divided by the column sum to yield its normalized score. The sum of each column is one, then the eigenvector values are found; which are normalized priority weights of each attribute. These weights are the values that are the most consistent with the pair-wise comparison values. Table 6 below shows the eigenvector values or priority vector. It is very clear that much importance should be given to Reliability, Immunity to attack and Operator authentication.

Table 6. Results of the analysis

Risks	Weight
Reliability	45%
Operator authentication	17%
Immunity to attack	23%
Integrity of votes	9%
Fault tolerance	5%
Total	100%

Table 7 computes the consistency of the AHP method. And the Standard Rule states the following condition: If CR <= .10, consistency is acceptable. To compute consistency ratio (CR): CR = CI / RI. The appropriate Consistency index is called Random Consistency Index (RI).

Table 7. Computing λmax

Risks	SUM	SUM/Weight
Reliability	2.45	5.40
Operator authentication	0.92	5.26
Immunity to attack	1.31	5.62
Integrity of votes	0.46	5.15
Fault tolerance	0.25	5.23
Lambda Max(λmax) ===============>5.33		

The RI is shown in Table 8, the RI = random index (CI of randomly generated pair-wise comparison matrix). The value of RI is based on *n*. A true Consistency Ratio is calculated by dividing the Consistency Index for the set of judgments by the Index for the corresponding random matrix. According to (Saaty, 2003); It is suggested that if that ratio exceeds 0.1 the set of judgments may be too inconsistent to be reliable. However; in practice, CRs of more than 0.1 sometimes have to be accepted.

Table 8. Random Consistency Index

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

$$CI = (\lambda max - n) / (n-1) = (5.33-5)/(5-1) = 0.0825$$

$$\text{Compute consistency ratio(CR)} = 0.0825 / 1.12 = 0.068 \quad .$$

Since the consistency ration is 0.068 and it is less than 0.10. Then the AHP model is acceptable. Nevertheless, risk management is very crucial for e-voting systems, and based the current literature on e-voting risk management on AHP applications in e-voting is very limited and modest. Therefore, there exists a significant research gap on the applications of AHP in e-voting and in general for all e-government services.

6. Conclusion

In spite of the challenges and problems, the trend is clear and firm toward using electronic voting means (E-Voting. CC and Competence Centre for Electronic Voting and Participation), in particular, not only electronic tally, but also electronic vote casting as mentioned in [11,35]. On the other hand, it is also possible that this kind of e-voting system may be significantly helpful for disabled and illiterate citizens. At the same time, the use of electronic voting technologies may reduce the economic and logistic costs of elections and consultations, while enabling geographically distributed citizens to vote as suggested by Williams et al. [12]. Nevertheless, risk management is very crucial for e-voting systems, and based the current literature on e-voting risk management on AHP applications in e-voting is very limited and modest. Therefore, there exists a significant research gap on the applications of AHP in e-voting and in general for all e-government services

Acknowledgements

This paper was supported by the Ministry of Interior (MOI), Oman. Especial thanks for the department of Information Technology at the MOI.

References

[1] BusinessDictionary, "Risk Definition." 2014.

[2] L. Tchankova, "Risk identification–basic stage in risk management," *Environ. Manag. Heal.*, vol. 13, no. 3, pp. 290-297, 2002.

[3] A. A. Filho, "STATE-CONTINGENT INSURANCE AND RISK MANAGEMENT," STANFORD UNIVERSITY, 2006.

[4] E. Sayari, M. Yaghoobi, and M. Ghanaatpishe, "Using Fuzzy Delphi Method in Risk Management (Case Study: Implementation of Fuzzy Delphi Method to Identify Credit Risks in Convert Financial and Credit Institutions into the Bank ," *World Appl. Sci. J.*, vol. 31, no. 5, pp. 759-766, 2014.

[5] R. Nelson, "IT project management: infamous failures, classic mistakes and best practices ," *MIS Q. Exec.*, vol. 6, no. 2, pp. 67-78, 2007.

[6] H. Taylor, E. Artman, and J. P. Woelfer, "Information technology project risk management: bridging the gap between research and practice," *J. Inf. Technol.*, vol. 27, no. 1, pp. 17-34, 2012.

[7] B. Whittaker, "What went wrong? Unsuccessful information technology projects," *Inf. Manag. Comput. Secur.*, vol. 7, no. 1, pp. 23-30, 1999.

[8] S. Aminbakhsh, M. Gunduz, and R. Sonmez, "Safety risk assessment using analytic hierarchy process (AHP) during

planning and budgeting of construction projects.," *J. Safety Res.*, vol. 46, pp. 99-105, Sep. 2013.

[9] N. Poolsappasit, "Towards an efficient vulnerability analysis methodology for better security risk management," Colorado State University, Colorado, 2010.

[10] A. Ghadge, S. Dani, and R. Kalawsky, "Supply chain risk management: present and future scope," *Int. J. Logist. Manag.*, vol. 23, no. 3, pp. 313-339, 2012.

[11] R. Williams, B. Bertsch, B. Dale, T. Van Der Wiele, J. Van Iwaarden, M. Smith, and R. Visser, "Quality and risk management: what are the key issues?," *TQM Mag.*, vol. 18, no. 1, pp. 67-86, 2006.

[12] K. T. Yeo, "Strategy for risk management through problem framing in technology acquisition," *Int. J. Proj. Manag.*, vol. 13, no. 4, pp. 219-224, 1995.

[13] S. Alhawari, L. Karadsheh, A. Nehari Talet, and E. Mansour, "Knowledge-based risk management framework for information technology project," *Int. J. Inf. Manage.*, vol. 32, no. 1, pp. 50-65, 2012.

[14] D. Gritzalis, *Secure electronic voting*. Kluwer Academic Publishers Dordrecht, 2003.

[15] P. Haijun, H. Edwin, and A. Nirwan, "RE-NOTE: An E-voting scheme based on ring signature and clash attack protection," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, 2103, pp. 867-871.

[16] D. P. Moynihan, "Building Secure Elections: E‐Voting, Security, and Systems Theory," *Public Adm. Rev.*, vol. 64, no. 5, pp. 515-528, 2004.

[17] Z. Xukai, L. Huian, S. Yan, P. Wei, and L. Feng, "Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties," in *INFOCOM, 2014 Proceedings IEEE*, 2014, pp. 136-144.

[18] L. C. Schaupp and L. Carter, "E-voting: from apathy to adoption," *J. Enterp. Inf. Manag.*, vol. 18, no. 5, pp. 586-601, 2005.

[19] Verified_Voting.org, "Summary of the Problem with Electronic Voting," 2014. [Online]. Available: http://www.verifiedvoting.org/wp-content/uploads/downloads/revised_summary31.pdf.

[20] R. Gibson, "Elections online: Assessing Internet voting in light of the Arizona Democratic primary," *Polit. Sci. Q.*, vol. 116, no. 4, pp. 561-583, 2001.

[21] D. Mac Namara, J. Gibson, and K. Oakley, "Just Like Paper-a baseline for classifying e-voting usability," *Int. Conf. e-Democracy Open Gov.*, pp. 1-12, 2014.

[22] R. Mercuri, "Electronic Vote Tabulation Checks and Balances," University of Pennsylvania, , Philadelphia, 2000.

[23] D. Jefferson and A. Rubin, "Analyzing internet voting security," *Commun. theACM*, vol. 47, no. 10, p. 59, 2004.

[24] M. Alvarez, T. Hall, and A. Treschsel, "Internet Voting in Estonia," VTP Working Paper, 2008.

[25] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, 2004, pp. 27-40.

[26] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proceedings of the 8th ACM conference on Computer and Communications Security*, 2001, pp. 116-125.

[27] A. H. Trechsel and F. Mendez, "The European Union and e-voting: addressing the European Parliament's internet voting challenge," 2005.

[28] N. Subramanian and R. Ramanathan, "A review of applications of Analytic Hierarchy Process in operations management," *Int. J. Prod. Econ.*, vol. 138, no. 2, pp. 215-241, Aug. 2012.

[29] A. Samvedi, V. Jain, and F. T. S. Chan, "Quantifying risks in a supply chain through integration of fuzzy AHP and fuzzy TOPSIS," *Int. J. Prod. Res.*, vol. 51, no. 8, pp. 2433-2442, Apr. 2013.

[30] J. M. Moreno-Jiménez, C. Pérez-Espés, and M. Velázquez, "e-Cognocracy and the design of public policies," *Gov. Inf. Q.*, vol. 31, no. 1, pp. 185-194, Jan. 2014.

[31] P. Aragonés-Beltrán, F. Chaparro-González, J.-P. Pastor-Ferrando, and A. Pla-Rubio, "An AHP (Analytic Hierarchy Process)/ANP (Analytic Network Process)-based multi-criteria decision approach for the selection of solar-thermal power plant investment projects," *Energy*, vol. 66, pp. 222-238, Mar. 2014.

[32] W. Liu, "A Electronic Commerce Risk Evaluation Method Based on AHP and GRA," in *Information Science and Engineering (ICISE), 2009 1st International Conference on*, 2009, pp. 2791-2793.

[33] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," *Adv. Cryptology—EUROCRYPT 2000*, 2000.

[34] J. F. Cunha, M. J. Leitão, J. P. Faria, M. P. Monteiro, and M. A. Carravilla, "Auditing e-Voting Pilot Processes and Systems at the Elections for the European Parliament and for the Portuguese Parliament," in *Seconfd Internationl Conference on Electronic Voting*, 2006, pp. 145-155.

[35] J. Esteve, "The Certification of E-Voting Mechanisms. Fighting against Opacity.," *Electron. Voting*, 2008.