VOL 1 (2017) NO 4 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Multilayered Framework to enhance management information systems decision on sensitive data in cloud computing environment

Haifaa Jassim Muhasin[# **] Rodziah Atan[# *] , Marzanah A.Jabar[#], Salfarina Abdullah[# *], Shahreen Kasim[***]

[#] *Department of Software Engineering & Information System, Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM), Malaysia*

[*] *Halal Research Products Institute, University Putra Malaysia, Malaysia*

[**] *College of Education for Pure Science Ibn-Al-Haitham, Department of Computer Science, University of Baghdad, Iraq*

[***] *Soft Computing and Data Mining Centre, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn, Malaysia*

E-mail: haifaajassim@yahoo.com, rodziah@upm.edu.my, marzanah@upm.edu.my, salfarina@upm.edu.my, shahreen@uthm.edu.my

Abstract— **The purpose of this research is defining the main factors influencing on decision of management system on sensitive data in cloud. The framework is proposed to enhance management information systems decision on sensitive information in cloud environment. The structured interview with several security experts working on cloud computing security to investigate the main objective of framework and suitability of instrument, a pilot study conducts to test the instrument. The validity and reliability test results expose that study can be expanded and lead to final framework validation. This framework using multilevel related to Authorization, Authentication, Classification and identity anonymity, and save and verify, to enhance management information system decision on sensitive data in cloud.**

Keywords— **Cloud computing, privacy, security, confidentiality, integrity, availability.**

I. INTRODUCTION

A new conception generates between users, organizations with their information when using cloud. This need existence another party to control and manage relations. This party is cloud service provider in cloud. Many problems related to information security generate as result to these relations.

The cloud is different from existing technology and approaches through five essential characteristics (self-service on-demand, access to an extensive network, the pooling of resources, rapid flexibility, and measuring service1. Cloud security is the development of the sub-domain of network security, information security and computer security. And it indicates to the deployment of a wide range of technologies, controls, and policies to protect information, applications and infrastructure related with cloud computing [1]. To overcome customers' concerns about the security of applications and data, the vendors have to address these issues. A framework is proposed to enhance management information system decision on sensitive data saved in cloud environment. This paper was organized as follows: first, the data security and privacy requirements and review related works to the study were explained, second, the proposed framework was explained, fourth, design of experiment. Lastly, the results and discussion, and conclusion and future work.

II. DATA SECURITY AND PRIVACY REQUIREMENTS

Access to data using varied resources need validation control model and access the integrated administration with control in cloud environments. The services of cloud vary according to the security policies due to variation in the authorization rights of access between users and service providers. Access to data using varied resources needs authentication of user and access control model for the incorporated management and control in the cloud environment. In particular, the access control model is a technique most commonly used to detect and prevent intrusions from the inside [2]. The analysis of the existing research works on technologies used in cloud computing for data security includes confidentiality, integrity, availability, authentication and authorization. In general, security professionals are taking into account aspects of important security measures such as confidentiality, where the customer or user of cloud computing is responsible for any operation

carried out that may cause for data loss or the possibility of data changes by other users within the same cloud [3].

Integrity is when confidential data is exposed to many risks, including the mistakes that get through the process of sending data from one place to another or from one computer to another. Integrity is one of serious issues related to cloud security [3]. Availability enables cloud service providers to provide services, sources of devices to users as optimum as possible [4]. Authentication is the service for the classification of individual user accounts. It performs setup an account, saving, storing, delete and manage individual user account. It uses simple log in or different token identifier for each user [3]. Other measures are such as authorization and access control [5]. Security issues of sensitive data in cloud environment is still shadowed by obstacle of adoption of cloud computing in companies and government agencies4. Cloud service must ensure data integrity and provide privacy of all stored information.

Many research deals with security weakness by propose schemes can effectively strength the security through authentication in cloud computing. Furthermore, these designs introduce many solutions to provide novel mechanisms for cloud security related to the requirements are used to produce authentication, data security and validation simultaneously. The challenges and problems in the cloud computing environment and possible solutions to overcome these problems presented. Also, a new observing technique identified along with virtualization. This assists the supplier to achieve complete security of the virtual machine [6]. This work improved secure cloud service. Others are seeking to achieve the goal of two points; first to identify security requirements to assess the security of the cloud, and secondly trying to find a possible solution to minimize potential threats [3]. A security framework related to platform for cloud suggested, the processes in this framework are working according to the request from customer, and making connect security form assist safe transmit of the data model [7]. Characteristics knowledge of cloud and data privacy protection are explained in [8]. Some authors suggested authentication method for SaaS management in cloud computing. the researchers believe that this proposed method S3 can improve the security of the cloud through authentication in cloud computing with the cost calculating and contacts acceptable [9]. Various issues related to integrity and security such as access control, integrity checks, and key management discussed in [10]. Others argue on how to develop a cloud computing by addressing the security problems that are related to privacy and reliability. And fundamental factors that affect the security risk, and also made proposals and recommendations on certain places, and to clarify the correlation between cloud computing and information security [11]. Some authors focused on the application of security for the region, for example, security applications, information security, infrastructure security and control security through giving private security model [12]. Others explain privacy and the confidentiality of information in cloud touched. And introduced a model- named multi cloud databases (MCDB) by Alzain et al.[13]. Other studies conform on the proposed solution to focus on two main issues that are the general verification and availability of data at the same time. And highlighted the limitations of security in the solitary cloud and advantage of using Multi – clouds strategy to decrease security risks by using DepSky which is a virtual storage system that guarantee preferable availability and top secrecy of data [4], [14]. Many models presented to achieve security; a new trust cloud model, and also suggested a new security framework based on an independent trust management model in the cloud environment. Also, presented a model of the control of access depends on the security policy thinking in cloud computing [2],[15].

III. The Proposed Framework

The new proposed framework contains four entities and three levels. The entities are: user party, cloud manager party, security auditor party, and cloud provider [16]. The three levels named: Authorization level, security and privacy level, save and verify level [16].

1. Authorization level: The level between manager and user of cloud. The main task of this level is to check the identity of the authorized user and the definition of login time which is used to calculate the cost of use and also used to generate the encrypted code for entering the cloud [16].
2. Security and privacy level: The level between security auditor party and user. The processes of authentication and classification of data to access sensitive information are done. These processes help to enhance data privacy protection and reduce the cost of data protection calculations [16].
3. Save and verify level: The level between the service provider and the user. This level provide service and required data after verification of the identity of the user by cloud manager and audit the type of required data by the auditor party in order to protect the privacy and security of data, and avoid internal intruders and increase the speed of data access. All levels operate according to policy among all parties for the proposed framework [16]. This framework is multi-level licensing framework (M2LF) is shown in Figure 1.

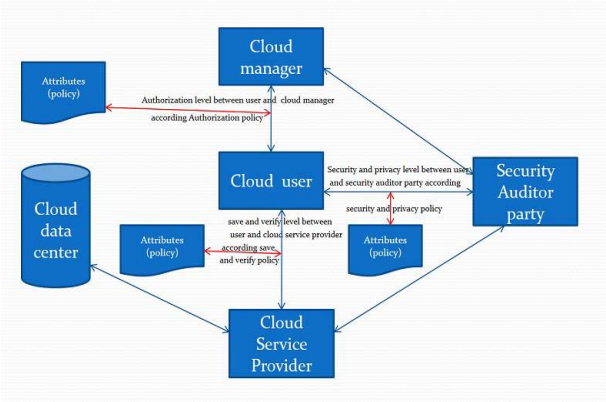

Fig 1. The proposed Framework (M2LF) [16]

IV. Design of Experiment

This study attempts to find if some of the factors influencing sensitive data security and privacy protection have to do with Authorization, Authentication, classification and Identity Anonymity, and Save and Verify. A pilot study was conducted to test the instrument for validity after investigate the main

objective of proposed framework and suitability of instrument by interview with various security experts working on cloud computing security. The structured interview conducted and the results was analyzed. The proposed framework was revised according to the experts' feedback. Then the questioner was developing according to the revised framework. This pilot study is conducted with potential participants who fit the IT professional population being studied and working in IT department. The sample size to pilot test is normally small, ranging from 15-30 respondents but it can be increased if the test requires several stages. So, a total of 32 copies of questionnaire was sending by using online survey (Google Drive) and 29 were completed the questionnaire, the results were analyzed by SPSS 20. The processes of the experiment design shown in Figure 2. The process was achieved within three months (February, March, and April 2017).

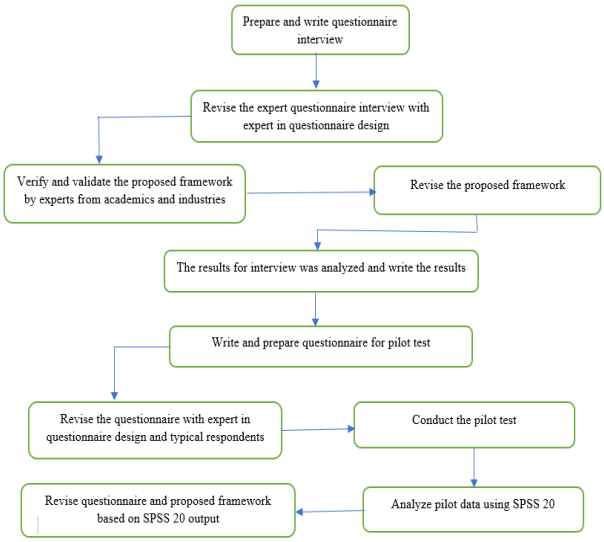

Fig 2. Design of experiment

V. The Proposed Framework Validity Measurement

5.1 Structured Interview Measurement

Structured interviews were conducted with nine experts in cloud computing security from academics and industries. Five experts from academics and four from industries. Structured interview use 12 questions; 3 questions to verify the proposed framework feasibility enhance data confidentiality, privacy and improve the quality of security for public cloud, 2 questions to verify the proposed framework have appropriate confidentiality, integrity, and availability measures and include privacy-enhancing solutions for sensitive data protection, 2 questions to verify the proposed framework applicability and the procedure of access control and the procedures by the parties of framework support the protection of sensitive data, 3 questions to verify the proposed framework understandability, correctness, prevents data leakage, data loss, and providing protection of customer assets from unauthorized access, 2 questions to verify comprehensive of framework, the description of responsible parties and roles and security policies that used by the parties of framework enhance the protection of sensitive data. The data gathering in interview in office face-to-face. The interviews took place in personal offices and lasted between 30 to 45 minutes.

5.2 Measurement using pilot study.

The Likert scales were utilized for measuring the security and privacy processes and procedures in framework (M2LF) towards factors influencing sensitive data security and privacy [17]. Examining factors that influencing sensitive data security and privacy by requesting from user to give the judgments value that is relevant to these factors and using in survey with the Likert scales to measure opinions, attitudes, and behaviors. The questionnaire consisting of multiple choice-questions. The instrument using a five-point Likert scale with values ranging from 1 Strongly Disagree to 5 for Strongly Agree. And used scale with values ranging from 1 Unimportant at all to 5 for Very Important to evaluate the important of activities. The questionnaire of the study is consisted from eight sections from 70 questions. Section 1: is a group of questions related to personal information about the respondents such as: name, job, country and the demographic information is included in this section. Section 2: is a group of nine questions for measuring Authorization Activities efficiency. Section 3: is a group of twelve questions for measuring Authentication Activities efficiency. Section 4: is a group of seven questions which aim for measuring the Classification and Identity Anonymity Activities efficiency. Section 5: is a group of four about Save and Verify Activities efficiency. Section 6: is a group of twelve questions which are target for measuring efficiency of activities according to objectives. Section 7: is a group of seven questions for measuring Activities Efficiency of framework. Section 8: is a group of ten questions for measuring Security Technologies Activity of framework.

VI. Results and Discussion

6.1 The results of proposed framework validity

After the structured interviews undertook the results of interviews was analyzed. The results explain that there is 92.59% among experts agree with the proposed framework feasibility and the framework enhance data confidentiality, privacy and improve the quality of security, 94.45% among experts agree with the measures used by the proposed framework and the framework have appropriate confidentiality, integrity, and availability measures and include privacy-enhancing solutions for sensitive data protection, 94.44% among experts agree on the proposed framework applicability and the procedures used by the parties of framework support the protection of sensitive data, 92.59% among experts agree on the proposed framework understandability. Also 83.33% among experts agree on comprehensive and the description of responsible parties, roles and security policies that used by the parties of framework enhance the protection of sensitive data.

6.2 Content and face validity

In order to ensure the validity of content the questionnaire sent to expert in questionnaire design. The process of checking the content validity was completed within two weeks' period. The face validity requiring distributed the questionnaire to a sample of typical respondents or specialist to judgment on the instrument is appropriate to use18,19,20. The process of taking the samples respondents opinion was finished through two weeks' period. After that, the researchers revised the instrument to improved.

6.3 Reliability test

A pilot study was conducted to test the instrument for validity after investigate the main objective of proposed framework and suitability of instrument by interview with various security experts working in cloud computing security. There are many types of reliability tests. The most common test is Cronbach's alpha20. The reliability of the survey instrument was computed with Cronbach's alpha (a) to illustrate the mean versus the median and rank for the research hypotheses. After the data are executed using SPSS 20, it was found that all the measures from 0.762 to 0.872. The pilot test results indicate that the values of Cronbach's alpha for all variables are greater than 0.7 as seen in Table 1. therefore, there was no need to delete any item21,22. The Cronbach's alpha for all coefficients ranged from (a=0.762) for Authorization Activities, (a=0.812) for Activities Efficiency of framework, (a=0.824) for save and verify Activities, (a=0.859) for Efficiency of Activities according to objectives (The objectives ranged from (a=0.713) for prevent data breach and loss, (a=0.788) for prevent Malicious insiders, (a=0.825) for reduce high cost of calculation and storage time and space), (a=0.866) for Authentication Activities efficiency, (a=0.872) for Security Technology Activity, (a=0.893) for Classification and Identity Anonymity Activities efficiency. With an overall reliability of (a=0.959).

The reliability measurements of the scales examined using Cronbach's alpha (a) gave a strong reliability result with (a=0.959) for alpha. This finding indicates that all the instruments are valid. All the factors loading values are above 0.7 and suitable to proceed with the empirical study later, the results shown in Table 1.

Table 1. Statistics of Reliability Coefficients 1

	Scale	N of Items	Cronbach's alpha	Results
1	**Authorization Activities efficiency**	**9**	**0.762**	Acceptable
2	**Authentication Activities efficiency**	**12**	**0.866**	**Good**
3	**Classification and Identity Anonymity Activities efficiency**	**7**	**0.893**	**Good**
4	**Save and Verify Activities efficiency**	**4**	**0.824**	**Good**
5	**Efficiency of Activities according to objectives**	**12**	**0.859**	**Good**
	a- Reduce high cost of calculations and storage time and space	4	0.825	**Good**
	b- Prevent Malicious insiders	4	0.788	Acceptable
	c- Prevent Data Breach and Data Loss	4	0.713	Acceptable
6	**Activities Efficiency of framework**	**7**	**0.812**	**Good**
7	**Security Technologies Activity of framework**	**10**	**0.872**	**Good**
	All Items	**61**	**0.959**	**Good**

N= Number of items

We do another analysis for the reliability of survey instrument according the hypotheses for (M2LF) framework. The reliability of the survey instrument was computed with Cronbach's alpha (a) to illustrate the mean versus the median and rank for the research hypotheses23,24. After the data are executed using SPSS 20, it was found that all the measures from (a=0.825) to (a=0.912). The pilot test results indicate that the values of Cronbach's alpha for all variables are greater than 0.7 as seen in Table 2. Therefore, there was no need to delete any item. The Cronbach's alpha for all coefficients ranged from (a=0.825) for Data Confidentiality, (a=0.846) for Data Integrity, (a=0.859) for Data Availability, (a=0.912) for Data Privacy. With an overall reliability of (a=0.959).

The reliability measurements of the scales examined using Cronbach's alpha (a) gave a strong reliability result with (a=0.959) for alpha. This finding indicates that all the instruments are valid. All the factor loading values are above 0.7, the results shown in Table 2.

Table 2. Statistics of Reliability Coefficients 2

	Scale	N of Items	Cronbach's alpha	Results
1	**Data Confidentiality**	**13**	**0.825**	**Good**
	a- User Authorization	7	0.702	Acceptable
	b- Data Authentication	3	0.713	Acceptable
	c- Data Anonymity	3	0.710	Acceptable
2	**Data Integrity**	**9**	**0.846**	**Good**
	a- User Authorization	3	0.730	Acceptable
	b- Data Authentication	3	0.704	Acceptable
	c- Identity anonymity	3	0.748	Acceptable
3	**Data Privacy**	**28**	**0.912**	**Good**
	a- Defining the responsibilities	10	0.771	Acceptable
	b- Identity Management	15	0.848	Good
	***b1**- User Authorization*	5	0.704	Acceptable
	***b2**- Data authentication*	4	0.717	Acceptable
	***b3**- Identity anonymity and Data classification*	6	0.724	Acceptable
	c- Data anonymity	3	0.748	Acceptable
4	**Data Availability**	**11**	**0.859**	**Good**
	a- Authorization mechanism	2	0.726	Acceptable
	b- Authentication mechanism	3	0.739	Acceptable
	c- Storage mechanism	6	0.750	Acceptable
	All Items	**61**	**0.959**	**Good**

N= Number of items

The validity and reliability tests results reveal that empirical study can be expanded and lead to final framework validation. Results shows the validity of the proposed framework and instrument reliability and validity.

VII. CONCLUSIONS

To ensure the security and privacy of sensitive information a Multi-Level Framework (M2LF) was proposed. This study attempts to find if some of the factors influencing on decision of management information system on sensitive data security and privacy protection have to do with Authorization, Authentication, classification and Identity Anonymity, and Save and Verify. A pilot study was conducted to test the instrument for validity after investigate the main objective of proposed framework and suitability of instrument by interview with various security experts working on cloud computing security. The structured interview conducted and the results was analyzed. Then the questionnaire was developing according to the refined framework. The validity and reliability tests results expose that study can be expanded and lead to final framework validation. This pilot study is conducted with potential participants who fit the IT professional population being studied and working in IT department. A total of 32 copies of questionnaire was sending by using online survey (Google Drive) and 29 were completed the questionnaire, the results were analyzed by SPSS 20.

REFERENCES

[1] Kumar S, Vajpayee A. A Survey on Secure Cloud: Security and Privacy in Cloud Computing. Am J Syst [Internet]. 2016 [cited 2017 Jun 24]; Available from: http://pubs.sciepub.com/ajss/4/1/2/

[2] Choi C, Choi J, Kim P. Ontology-based access control model for security policy reasoning in cloud computing. J Supercomput [Internet]. 2014 [cited 2017 Jun 24]; Available from: http://link.springer.com/article/10.1007/s11227-013-0980-1

[3] Zissis D, Lekkas D. Addressing cloud computing security issues. Futur Gener Comput Syst [Internet]. 2012 [cited 2017 Jun 24]; Available from: http://www.sciencedirect.com/science/article/pii/S0167739X10002554

[4] Tebaa M, Hajji S. From Single to Multi-clouds Computing Privacy and Fault Tolerance. IERI Procedia [Internet]. 2014 [cited 2017 Jun 24]; Available from: http://www.sciencedirect.com/science/article/pii/S2212667814001476

[5] Wang Z. Security and privacy issues within the Cloud Computing. Inf Sci (ICCIS), 2011 Int … [Internet]. 2011 [cited 2017 Jun 24]; Available from: http://ieeexplore.ieee.org/abstract/document/6086163/

[6] Loganayagi B, Sujatha S. Enhanced cloud security by combining virtualization and policy monitoring techniques. Procedia Eng [Internet]. 2012 [cited 2017 Jun 24]; Available from: http://www.sciencedirect.com/science/article/pii/S1877705812009216

[7] Xiaoping X, Junhu Y. Research on cloud computing security platform. Comput Inf Sci [Internet]. 2012 [cited 2017 Jun 24]; Available from: http://ieeexplore.ieee.org/abstract/document/6300744/

[8] Cheng F, Lai W. The impact of cloud computing technology on legal infrastructure within internet—focusing on the protection of information privacy. Procedia Eng [Internet]. 2012 [cited 2017 Jun 24]; Available from: http://www.sciencedirect.com/science/article/pii/S1877705811065386

[9] Xu L, Cao X, Zhang Y, Wu W. Software Service Signature (S3) for authentication in cloud computing. Cluster Comput [Internet]. 2013 [cited 2017 Jun 24]; Available from: http://link.springer.com/article/10.1007/s10586-013-0262-y

[10] Zhou M. Data security and integrity in cloud computing. University of Wollongong Thesis Collection. 2013.

[11] Daniel W. Challenges on privacy and reliability in cloud computing security. Inf Sci Electron Electr [Internet]. 2014 [cited 2017 Jun 24]; Available from: http://ieeexplore.ieee.org/abstract/document/6947857/

[12] Al-Anzi F, Yadav S, Soni J. Cloud computing: Security model comprising governance, risk management and compliance. Data Min Intell [Internet]. 2014 [cited 2017 Jun 24]; Available from: http://ieeexplore.ieee.org/abstract/document/6954232/

[13] AlZain M, Soh B, Pardede E. A new model to ensure security in cloud computing services. J Serv Sci Res [Internet]. 2012 [cited 2017 Jun 24]; Available from: http://www.springerlink.com/index/F37003R856QP8656.pdf

[14] Jogdand R, Goudar R, Sayed G, Dhamanekar P. Enabling public verifiability and availability for secure data storage in cloud computing. Evol Syst [Internet]. 2015 [cited 2017 Jun 24]; Available from: http://link.springer.com/article/10.1007/s12530-013-9095-4

[15] Li W, Ping L, Pan X. Use trust management module to achieve effective security mechanisms in cloud environment. Electron Inf Eng ([Internet]. 2010 [cited 2017 Jun 24]; Available from: http://ieeexplore.ieee.org/abstract/document/5559829/

[16] Muhasin H, Atan R. Cloud computing sensitive data protection using multi layered approach. Sci Inf [Internet]. 2016 [cited 2017 Jun 24]; Available from: http://ieeexplore.ieee.org/abstract/document/7852610/

[17] Likert R. A technique for the measurement of attitudes. Arch Psychol [Internet]. 1932 [cited 2017 Jun 25]; Available from: http://psycnet.apa.org/psycinfo/1933-01885-001

[18] Gorondutse A, Hilman H. The influence of Business Social Responsibility (BSR) on Organizational Performances: A pilot Study. Int J Bus [Internet]. 2012 [cited 2017 Jun 25]; Available from: https://www.researchgate.net/profile/Abdullahi_Hassan_Gorondutse/publication/274138061_The_Influence_of_Business_Social_Responsibility_(BSR)_on_Organizational_Performances_A_Pilot_Study/links/5516eeef0cf2f7d80a39d219.pdf

[19] Hair J, Anderson R, Babin B, Black W. Multivariate data analysis: A global perspective. 2010 [cited 2017 Jun 25]; Available from: http://library.wur.nl/WebQuery/clc/1924429

[20] Sekaran U, Bougie R. Research methods for business: A skill building approach [Internet]. 2016 [cited 2017 Jun 25]. Available from: https://books.google.com/books?hl=en&lr=&id=Ko6bCgAAQBAJ&oi=fnd&pg=PA19&dq=Sekaran+U,+Bougie+R.+Research+methods+for+business:+A+skill+building+approaches+(5th+ed.).+Chichester:+John+Willey+%26+Sons+Ltd.,+2010.&ots=2A6TW0L-mQ&sig=IfaeTzx9PvofmNuF3CEXTx4NoTE

[21] Vogt W. Quantitative research methods for professionals. 2007 [cited 2017 Jun 25]; Available from: https://scholar.google.com/scholar?q=Vogt%2C+W.+P.+Quantitative+research+methods+for+professionals.+Boston%2C+MA%3A+Pearson+Education%2C+Inc.%2C+2007&btnG=&hl=en&as_sdt=0%2C5

[22] Wikman A. Reliability, validity and true values in surveys. Soc Indic Res [Internet]. 2006 [cited 2017 Jun 25]; Available from: http://www.springerlink.com/index/K67014H37778685X.pdf

[23] Soja P. Examining the conditions of ERP implementations: lessons learnt from adopters. Bus Process Manag J [Internet]. 2008 [cited 2017 Jun 25]; Available from: http://www.emeraldinsight.com/doi/pdf/10.1108/14637150810849445

[24] Walpole R, Myers R, Myers S, Ye K. Probability and statistics for engineers and scientists [Internet]. 1993 [cited 2017 Jun 25]. Available from: http://imse.statler.wvu.edu/files/d/9656f528-f87e-4d33-94bf-1fb7c10f0e38/ieng213.pdf