A Compliant Assurance Model for Assessing the Trustworthiness of Cloud-based E-Commerce Systems

Thembekile O. Mayayise
School of Computing, College of Science, Engineering and Technology, University of South Africa
Pretoria, South Africa
Tmayayise@gmail.com

Isaac O. Osunmakinde
School of Computing, College of Science, Engineering and Technology, University of South Africa
Pretoria, South Africa
osunmio@unisa.ac.za

***Abstract*— Many cloud-based e-commerce stores aim to attract and retain customers in order to be competitive. However, they are all faced with a challenge regarding gaining and maintaining consumer trust in a volatile cloud-based e-commerce environment where risks pertaining to information security, privacy of information and inadequate monitoring of compliance to applicable laws are prevalent. The pervasiveness of these risks has indirectly propelled the development of web assurance models, which were designed in an attempt to encourage online consumer trust. Regrettably, many of these models have been inadequate in certain areas, such as being unable to provide online real-time assurance on a comprehensive set of attributes, which include a check of compliance to the applicable e-commerce legislation or standards in a cloud-based environment.**

The aim of this research was to examine whether the integration of the attributes of adaptive legislation, adaptive ISO standards, policies, advanced user security and website availability can be used to develop a compliant assurance model. The model uses an intelligent cooperative rating based on the analytical hierarchy process and page ranking techniques to improve the level of cloud-based trustworthiness. We illustrated in an empirical explanatory survey conducted with 15 test samples from IEEE, Science Direct databases and real life data captured from E-commerce sites that the proposed compliant model strongly contributes to the improvement of cloud-based sites, as well as enhancing the trustworthiness of these websites. The findings of this research study can be used as a reference guide to understand the effectiveness of cloud-based e-commerce assurance models, as well as to enhance the trustworthiness of these models.

***Keywords*— *cloud, assurance, model, seal, trustworthiness, e-commerce* .**

I. INTRODUCTION

The internet has revolutionized the way in which companies do business or render services to customers globally. However the issue of trust over the internet between buyers and sellers remains paramount, since it determines the success of the adoption of e-commerce. The internet as a business enabler has numerous advantages, such as providing businesses with a technological platform to conduct business without experiencing any geographical boundaries. On the other hand, business organizations that conduct business over the internet are faced with numerous challenges, which if not addressed, could hinder the adoption of e-commerce; these relate to information security and privacy risks and other general website-related attacks.

The advent of cloud computing in the late 1990s has made it possible for online businesses such as Amazon to provide cloud-based services, which include storage services, among others [7]. Cloud computing is an emerging technology that offers a range of technology services, such software as a service, as depicted in figure I. According to [22], cloud computing can be defined as well-packaged services that satisfy the following conditions: the services offered through the cloud must be delivered through the telecommunications network; users are dependent on the service to gain access and process data; the user retains the legal control over the data; some of the resources on which the cloud service depends are virtualised, implying that a user may not necessarily know the physical location of the hosting device, and lastly in a cloud there is a flexible contractual agreement between the service provider and client with regard to the quantum used.

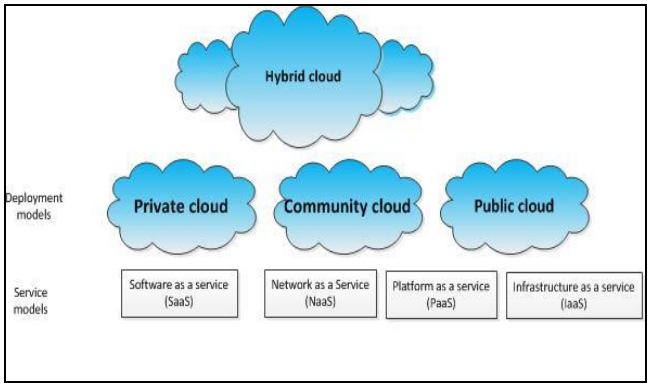

Figure I. Cloud computing services (adapted from [6])

Cloud computing has many potential benefits, such as taking away the responsibility of managing the technology infrastructure, allowing business owners to focus on their core business. On the other hand, there are some risks that the cloud service providers need to address in order to minimize data breaches in the cloud. According to [17], many cloud service providers claim to have high systems availability capabilities,

yet fail to produce the evidence to support the claim. As a result, customers are likely to experience service disruption or even data losses or theft, as depicted in the case of Google in Table I (adapted from [18] and [25]). It is thus imperative for trust relationships between parties doing business via the internet as a channel of communication to be strong.

Table I: Specific e-commerce losses as a result of online transactions

Date	Country	Company	Cause	Impact
Feb 2010	Global	VeriSign	The systems were hacked	Undisclosed information was stolen
Apr 2011	Global	Sony	Security and privacy breach	An estimated 77 million play station accounts were hacked and confidential information such as credit card information was exposed
Jul 2011	China	Alibaba	Inadequate gold supplier verification measures where goods that customers ordered were never received	This resulted in financial losses estimated at $1.94 million
Jul 2011	South Korea	ESTsoft	Information system security breach by hackers	35 million people's personal information was exposed
Oct 2012	Global	Google	Cloud service outages that resulted in slow responses and server unavailability, which affected various other vendor websites	Loss of productivity as a result of slow response of systems

E-commerce assurance models, such as policy statements on an online vendor's site or a third party assurance seal, have been devised in an attempt to promote online consumer trust. Unfortunately, there are some short-comings that need to be addressed by future web seal designers. One of the shortcomings is that assurance models do not seem to provide the desired assurance, but only perceived assurance, to consumers [4]. Another challenge is that e-commerce assurance models are static and do not provide continuous compliance assessments to applicable legislation and standards by online vendors or cloud service providers. In an environment where the changes to the technology platform and configuration may be frequent, such as the cloud, continuous assurance would be more beneficial [15].The cloud has numerous challenges, such as failure to disclose how the data collected via the cloud will be used and continuous availability of the cloud resources [14]. A cloud assurance model should be designed in such a way that these challenges are addressed in order to encourage online consumer trust. The objective of this paper is to present a comprehensive survey of a cloud-based e-commerce assurance model and to propose a compliant cloud-based assurance model for e-commerce. The major contributions of this paper are as follows:

- Development of a compliant cloud-based assurance model based on cooperative intelligent rating (analytical hierarchy process [AHP] and page ranking) for e-commerce trustworthiness
- Knowledge generation as a reference guide to understand e-commerce trustworthiness in general and cloud-based e-commerce assurance models in particular detail.

This paper is arranged as follows: section II discusses the cloud-based assurance models, section III proposes the compliant cloud-based assurance model, section IV, descriptive deployment analysis, lastly the conclusion is presented in section V.

II. CLOUD-BASED ASSURANCE MODELS AND ASSOCIATED CHALLENGES

A. Cloud-based e-commerce assurance models

Cloud-based assurance models are in the form of certifications or manual compliance checks achieved by the cloud service provider to numerous standards and even laws such as privacy laws. Reference [1] is an example of a cloud service provider that provides its customers with an assurance model that lists the type of certification received by the service provider, such as International Organization for Standardization (ISO) 27001 and Payment Card Industry certification. The declaration of certification by [1]'s web services team is aimed at encouraging trust among its clients or merchants to use its technology platform. In a nutshell, the main objective of assurance models is to reduce fear to transact among

consumers and rather encourage online customers to trust the process. Sections 1 to 3 discuss the different types of assurance models that can be found in cloud-based e-commerce environments.

1) Cloud-based policy assurance models

The policy assurance models are provided as self-assurance measures in a cloud-based environment by the online vendor or the cloud service provider. Policy statements are normally displayed at the bottom of the website home page, hyperlinked to the policy detail. The advantage of a policy assurance model is that it is a common form of e-commerce assurance. The disadvantage is that in a cloud-based e-commerce environment policy assurances may not entail all the information pertaining to the applicable privacy laws [22] and this is an area that needs to be improved. Examples of policy assurance models can be found in [1] and [5].

2) Static cloud-based assurance models

A static assurance is a seal that is displayed on a certified cloud service provider's site; it requires a user to click on the website to read the detail. The Trusted Cloud Data security certification is an example of a cloud-based assurance model for service providers within the European Union domain, where both the company and the service provider are regulated by the European Union Safe harbor principles [23]. While this type of assurance model can be useful in providing assurance to countries that are EU-resident, it eliminates non-EU countries because it is not adaptive to accommodate the laws of other countries. The disadvantage of this type of seal is failure to provide continuous assurance in a dynamic cloud-based e-commerce environment.

3) Continuous assurance models

A continuous or variable seal assurance model provides regular online updates on information concerning the assurance status of a particular website. An example of a cloud-based assurance model is the [14] web seal. This has been designed to provide security assurance in the cloud environment where it scans the website for any known vulnerabilities. The advantage of this model is that it provides online real time assurance. What needs to be done to improve these seals is to factor in compliance to best practice standards and regulatory laws for the users to trust the system, since providing assurance on known vulnerabilities may not always be sufficient.

B. Challenges of Current Assurance Models

In the cloud-based computing environment, there are numerous challenges, which must be addressed in order to encourage online consumer trust. One of the ways in which these challenges can be addressed is by providing e-commerce assurance, which will encourage online consumer trust. Reference [22] has identified some of the key assurance challenges in the cloud environment and these are discussed in sections 1 to 4 below.

1) Risk of unauthorized use of personal information as an assurance challenge

The cloud presents a challenge to customers regarding privacy of their information. particularly on how the data that customers divulge will be used or stored by the cloud service provider. In the event of a data privacy breach, it often becomes very difficult to ascertain which laws are applicable, more especially if it was not specified at the time of concluding the agreement between the online vendor and the cloud service provider [9]. In order to address this challenge, the proposed cloud-based assurance model assesses adaptive laws on which the vendor and the cloud service provider agree to be applicable in the event of a breach.

2) Security of the data as an assurance challenge

Information security in the cloud is paramount. When a security breach occurs, the impact of that breach is huge, since it is likely to affect more than one website affiliated to that cloud service provider. Amazon is an example of a cloud service provider that prides itself on its ability to provide a secure website environment for business purposes. However that does not mean that every website that is affiliated to Amazon will be protected by a standard seal program. To illustrate this fact, we examined the assurance status of the different websites affiliated to Amazon, such as [3], which has two assurance seals, i.e. Norton Secured and Bizrate, whereas [19] has no seal displayed, notwithstanding the different business types. The proposed model would assist in ensuring that the cloud service providers provide standard assurance levels for areas such as information security and compliance with specific laws and security standards.

3) Availability of cloud services as an assurance challenge

Many online vendors who are using cloud services rely on the service provider to keep the e-commerce environment available. The impact of system unavailability in the cloud environment is serious, since it affects more than one vendor, as in the case of Google, where its cloud services became unavailable and multiple vendors were affected [25]. In order to create a trustworthy environment, users need to be aware that the website they are transacting from is a true vendor site which can be accessible on demand. The proposed cloud-based e-commerce assurance model checks the cloud environment servers, reports on the availability status and provides an aggregated rating, which takes into account other website attributes. A site that is constantly available will yield a positive rating, marked with a green status on the website.

4) Descriptive survey on laxities of assurance models

This section discusses the weaknesses of some of the existing e-commerce assurance models and how they are perceived in terms of trustworthiness. Figures II (a) and (b) provide a summary of the findings of the research that was conducted by [8]. The research was conducted to determine whether seal-accredited websites were more trustworthy than unaccredited sites. A tool was used to check for policy compliance issues on the certified websites. The findings revealed that on the accredited websites, 4% of the sites were not trustworthy because of failure to meet certain requirements as expected by the seal accreditation bodies. The findings revealed that for the Truste accreditation [24] and the BBB online seal, not all the websites displaying the seals were in actual fact trustworthy.

This finding raises some doubt in terms of the credibility of seal accreditation bodies because when an analysis was done of uncertified sites, only 3% of the sites were found untrustworthy, which is less than 4% of the certified sites that were found untrustworthy (refer to figure II (a) and (b). The challenge presented by these findings is that it raises the possibility that some untrustworthy sites are posing as trustworthy sites because they display web seals.

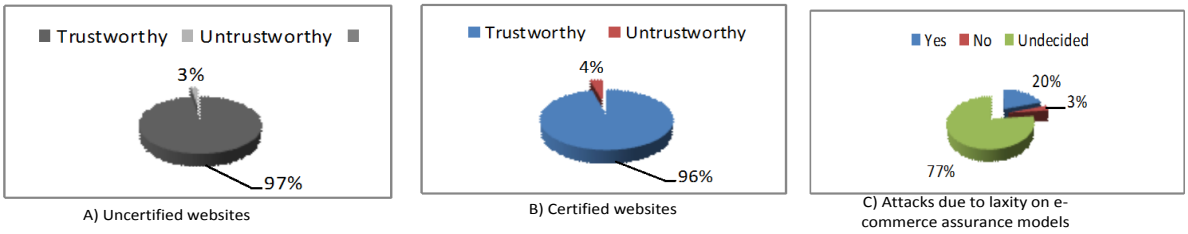

Figure II. Do existing e-commerce assurance models require improved trustworthiness?

These results highlight a need for more work to enhance the existing e-commerce assurance models, including the cloud-based e-commerce assurance models.

III. PROPOSED COMPLIANT CLOUD-BASED ASSURANCE MODEL

The proposed model consists of the following assurance measures: adaptive legislation, adaptive ISO standards, policies and advanced security login and website availability. The term "adaptive" is used show that the attribute is not fixed but rather flexible in such a way that it accommodates revised legislation or different legislation, provided it is specific to the e-commerce environment. Figure III presents the proposed cooperative assurance rating model based on page ranking and AHP techniques.

The mathematical model deals with the level of e-commerce assurance based on PageRank modelling by [20] as an e-commerce assurance rating (EAR).

Our EAR model is shown in equation (1).

$$\text{EAR (A)} = (1\text{-}d) + d\left(\frac{EAR(_{t1})}{c(_{t1})}\right) + \ldots\ldots + \left(\frac{EAR(_{tn})}{c(_{tn})}\right) \quad (1)$$

Where t1, . . . , tn are websites linking to website A, C is the number of outgoing links from a website (out degree) and d is a damping factor, usually set to 0.85 this value avoids accidental infinite series of websites linking infinite number of other sites. Since PageRank assigns a high score to a node, if it is pointed by highly ranked nodes, it is highly applicable in advancing website trustworthiness based on e-commerce assurance. The AHP [12] is a technique that is used in environments where complex decisions need to be made. For the purpose of this study AHP is used to reach clear decisions on the state of every attribute of the proposed assurance model. AHP is used to impart some structure to the unstructured assurance model attributes, such as policy, legislation and the ISO standard [21] and package these attributes in a manner that makes it feasible to make a decision on the website's overall state of trustworthiness. The technique firstly aims to classify the attributes into distinct groups with the aim of constructing a hierarchy of attributes where the lower hierarchy is limited by the upper one specifically; pairwise comparison matrices are generated with respect to our attributes for first rating. One of the important decision steps in AHP is shown in equation (2).

$$Z = \{z_{ij}\} = \left(\begin{bmatrix} z_{11} & \ldots . z_{1n} \\ \vdots & \vdots \\ z_{n1} & \ldots . z_{nn} \end{bmatrix} \right) \quad (2)$$

Where Z=comparison matrix. The basic principle of our method is cooperative usage or parallel activation of the AHP and page ranking techniques in order to use the strength of the second to the benefit of the first. This provides an accurate rating and instils trust in customers in cloud-based e-commerce environments. The cooperative assurance rating status is as follows: green is for a trustworthy site, yellow denotes a risky site and red a completely untrustworthy site; these indications guide the customer in transacting from a site or not doing it.

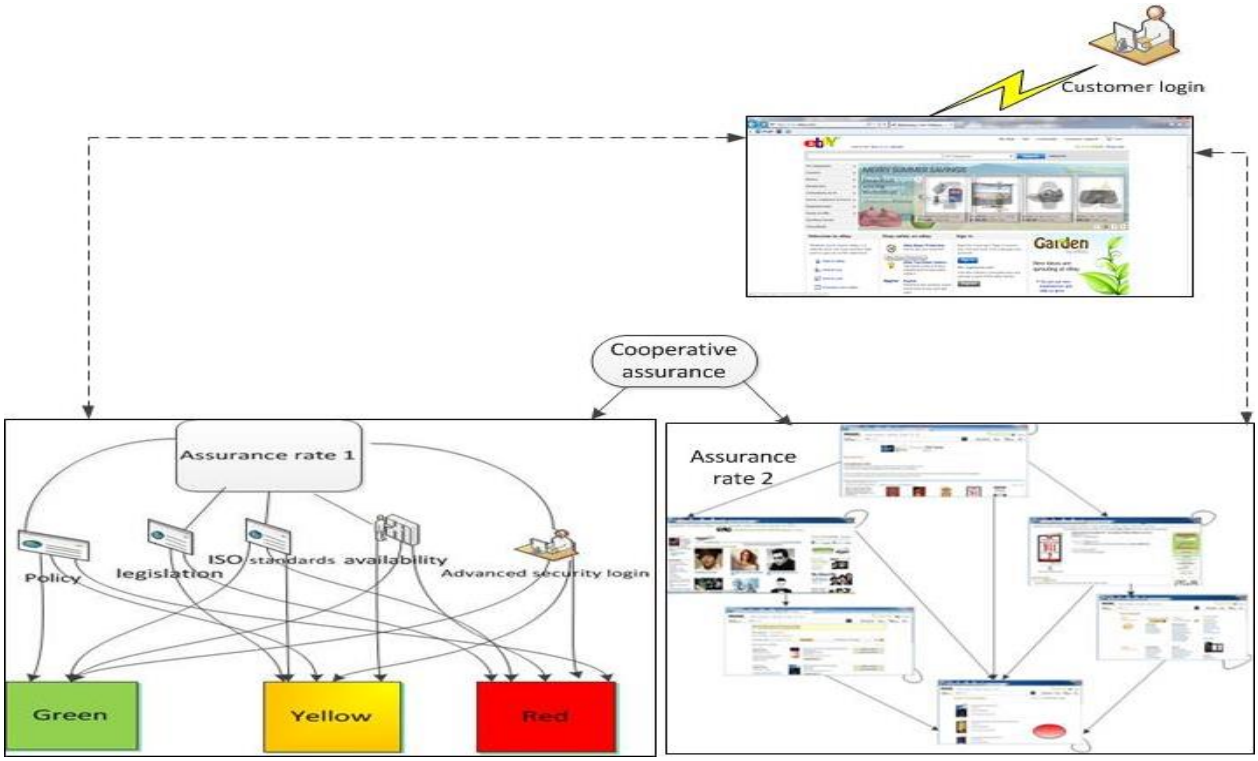

Figure III: Cooperative intelligent rating model for cloud-based e-commerce assurance

The proposed model is aimed at providing useful information for decision-making to a customer concerning the website's trustworthiness. In order to transact from a website, the proposed model (as shown in figure III) requires the creation of strong online login credentials. Thereafter, a customer provides input through a short survey, to determine if the customer has read the policies displayed and secondly if the customer has experienced a bad or good shopping encounter through the website in the past or not. The model aggregates the user's input together with the following attributes: policies, legislation, ISO standard and website availability. The model checks the presence of the policies and the last policy review date to determine currency and provide a rating. Furthermore, a check for compliance to Electronic Communications and Transactions (ECT) legislation will be conducted to produce overall website rating. Adoption of the ISO standard, specifically the ISO 27001, will be confirmed by the model on the security of online transactions, specifically encryption. An online check to determine if the website is consistently available and has the latest anti-virus software and latest patch is conducted to ensure that it is not vulnerable to online attacks. The model combines all the attribute information using the cooperative rating based on AHP and page ranking to strengthen the assurance level. A trustworthy site flashes green and an untrustworthy one flashes red. The proposed model's benefits are as follows:

a) It is comprehensive and interactive in that it assesses compliance to legislation and also does online checking of technological compliance in terms of checking for the latest anti-virus software and website availability.
b) It is interactive and visible through the colour display on the website.
c) A dashboard (green, yellow, red) is provided as a result of a cooperative rating, which strengthens the assurance level.

The detailed discussions of the model attributes are presented in sections A to E. One can see that the proposed model has more beneficial enhancements than the existing ones such as the trusted cloud data security certification and the KYPLEX model [14]

A. Adaptive legislation as assurance measures

In the trans-border cloud environment the application of laws gets very complex in the event of a privacy or security breach if the applicable laws have not been specified from the onset [11]. In terms of providing e-commerce assurance, laws have been found to be an assurance measure [13]. Different e-commerce laws that are specific can be used with the model. For the purposes of this study, South African legislation [9] will be used because of its specific provisions in terms of e-commerce environments. The ECT Act provisions will be used as measures for aggregation in the e-commerce environment, where the final rating will alert the customer if the website that is hosted in a cloud environment is safe to transact from or not. A testable null directional correctional hypothesis that is set for this attribute is:

H_0^1: *The level of adaptive legislation of a country is not positively associated with other assurance measures*

In testing this proposition, explanatory research is required, as shown in table IV.

B. Adaptive ISO security standard as an assurance measure

According to [10], the ISO 27002 standard is regarded as the e-commerce international benchmarking standard for information security, which is thus suitable for inclusion in the cloud-based environment. As a result, sections 10.9.1 to 10.9.3 of ISO 27001 have been identified as vital for inclusion in the proposed model. The model checks for the security of transactions in an online environment by checking for the encryption of transactions on the website. This check, together with the other attributes, will be assessed and aggregated in order to show the final website assurance rating. A testable null directional correctional hypothesis that is set for this attribute is:

H_0^2 *: The level of adaptive ISO standards and other assurance measures is negatively associated*

In testing this proposition, explanatory research is required, as shown in table IV.

C. Policies as an assurance measure

Policies have often been used by various websites to provide assurance to prospective customers concerning privacy of information and other related practices. In terms of the South African ECT Act, certain policies are required by law to be displayed on vendor websites. These include policies such as privacy and refund policies, which must appear on the online vendor's site. Policies in a cloud environment are critical so that consumers can know and understand how their personal information will be handled in terms of privacy and to know which laws will apply in the event of a breach. Specifying the laws applicable to policy statements will be an improvement on existing policy models. A testable null directional causal hypothesis that is set for this attribute is:

H_0^3*: The level of policies of a business enterprise does not positively influence other assurance measures*.

In testing this proposition, explanatory research is required, as shown in table IV.

D. Advanced security features as an assurance measure

Information security in a cloud-based e-commerce environment is crucial in order to gain and maintain online customer trust. Cloud service providers need to provide leading edge security and auditing capabilities to keep up with meeting the customer's assurance needs. Customers need to feel secure from the login phase to check out. A testable null directional causal hypothesis that is set for this attribute is:

H_0^4 *: The level of strength of advanced user security does not influence other assurance measures*

In testing this proposition, explanatory research is required, as shown in table IV.

E. Site availability as an assurance measure

Website availability is crucial in the cloud-based environment. Service disruptions ought to be minimal for customers to gain and maintain trust in an online vendor store. A testable null directional correctional hypothesis that is set for this attribute is:

H_0^5 *: The level of e-commerce site availability and other assurance measures is negatively associated*

In testing this proposition, explanatory research is required, as shown in table IV.

IV. DESCRIPTIVE AND DEPLOYMENT ANALYSIS

A. Descriptive analysis and results

Table IV contains statistical data, which were arrived at by conducting a survey of journals from the IEEE, Science Direct databases based on the criteria of whether they were an E-commerce transacting site or not. The survey was conducted to determine if the following attributes had been identified as assurance measures in any of the sampled journals and e-commerce websites: adaptive legislation, adaptive ISO standards, policy, availability and advanced security logon. The sampling frame is October 2012 to March 2013 and the journals were sampled based on their relevance to the subject of this article where specific keywords were used. The main aim was to determine the number of articles in support of or against the proposed attributes as assurance measures.

Table IV Sampled dataset from journal articles and real life data from e-commerce sites

Sample no	Sampled Cases	Legislation		ISO		Policies		Security		Availability	
		Y	UND	Y	UND	Y	UND	Y	UND	Y	UND
1	Sample size 8;db1, wrt legislation	63%	37%	0%	100%	63%	37%	100%	0%	0%	100%
2	Sample size 10;db2, wrt legislation	30%	70%	10%	90%	80%	20%	30%	70%	0	100%
3	Sample size 15;db3,wrt legislation	7%	93%	7%	93%	93%	7%	100%	0%	85%	15%
4	Sample size 5;db1, wrt ISO	0%	100%	0%	100%	0%	100%	100%	0%	0%	100%
5	Sample size 10;db2, wrt ISO	0	100%	10%	90%	0%	10%	100%	0%	0%	100%
6	Sample size 10;db3,wrt ISO	20%	80%	10%	90%	100%	0%	100%	0%	0%	100%
7	Sample size 5;db1, wrt Policy	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
8	Sample size 10;db2, wrt Policy	10%	90%	0%	100%	100%	0%	100%	0%	0%	100%
9	Sample size 15;db3,wrt Policy	7%	93%	0%	100%	93%	7%	100%	0%	0%	100%
10	Sample size 5;db1, wrt Security	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
11	Sample size 15;db2, wrt Security	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
12	Sample size 15;db3,wrt Security	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
13	Sample size 10;db1, wrt Availability	0%	100%	0%	100%	90%	10%	90%	10%	50%	50%
14	Sample size 10;db2, wrt Availability	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
15	Sample size 15;db3,wrt Availability	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%

Keys:db1=IEEE database,db2=Science direct database,wrt=with respect to,Y=Yes,UND=Undecided.

The Pearson's correlation coefficient (R) in [16] was implemented and confirmed with excel macro to compute the relationships in Table IV. Any two attributes are chosen at random to test for possible relationships as shown below:

1) H1: The level of adaptive legislation of a country is not positively associated with other assurance measures

FINDINGS: The result of the macro implemented implies: Corr(Legislation: ISO) = 0.2;
DECISION: Since the correlation result> 0,Corr (Legislation: ISO) = **0.2;** The above proposition is rejected, which implies that the level of adaptive legislation of a country is positively associated with any other assurance measure

2) H2: The level of adaptive ISO standards and other assurance measures is negatively associated

FINDINGS: The result of the macro implemented implies: Corr(ISO: Availability) = **0.1769;**
DECISION: Since the correlation result > 0, the above proposition is rejected, which implies that the level of adaptive ISO standards and other assurance measures is positively associated.

3) H3: The level of policy of a business enterprise does not positively influence other assurance measures

FINDINGS: The result of the macro implemented implies: Corr(Policies: Availability) = **0.12;**
DECISION: Since the correlation result > 0 suggests the rejection of the above proposition. This implies that the level of policy of a business enterprise does positively influence other assurance measures.

4) H4: The level of strength of advanced user security does not influence other assurance measures

FINDINGS: The result of the macro implemented implies: Corr(Security : Availability) = **0.0353;**
DECISION: Since the correlation result > 0 suggests the rejection of the above proposition. This suffices to prove that the level of strength of advanced user security does influence other assurance measures. The correlational graph that emerged from these direct or indirect interrelationships is shown in figure IV (a).

Figure IV(a): Emerged correlational graph of the assurance measures

The results above suggest necessary or supporting conditions to say that the assurance measures could serve as the building blocks of the intelligent model in figure III and are compliant for accessing the trustworthiness of cloud-based e-commerce sites.

B. Deployment scenario of the cloud-based assurance model

1) Scenario 1 –Untrustworthy e-commerce website

As shown in figure IV (b) Joyce is considering making a book purchase through a cloud-based e-commerce website. She has created an online account. Following logging in, Joyce is asked through a short survey whether she has seen the policies (privacy and refund) on the website and she responds positively. Joyce had no previous shopping experience through the website and the system does not ask questions concerning her last shopping experience. Unfortunately, soon thereafter, a red button starts flashing at the bottom right-hand corner of the screen, signalling to her that the website is untrustworthy. Joyce clicks to read more information and it is highlighted that the website has been unavailable for an extended period of time and is not compliant with cloud-based e-commerce legislation. As a result, Joyce abandons the sale and signs out because the website is not trustworthy. In a nutshell the model interacts with Joyce through a short survey on the attributes whilst the model simultaneously carries out background checks on the site based on the assurance attributes to come up with an overall website rating.

The proposed model could be used to address this scenario.

Figure IV (b). Red website rating

V. CONCLUSION

E-commerce assurance is an area that has not been thoroughly researched, more especially cloud-based e-commerce assurance. As a result, very few journals discuss cloud-based e-commerce assurance models and propose robust models. In this research work, the focus was on examining the existing e-commerce assurance models and placing particular focus on cloud-based assurance with the aim of identifying gaps and addressing them by proposing a cloud-based e-commerce assurance model. The proposed cloud-based assurance model consists of the following assurance attributes: policy, adaptive legislation, adaptive ISO standards and advanced user security login. The AHP and page ranking techniques are used to achieve cooperative ranking of the attributes, which is displayed on the website for customer guidance regarding the website's trustworthiness, as shown in figure IV(b).The major improvement in the proposed model is to have an intelligent cloud-based assurance rating, which the existing e-commerce assurance models do not have. The proposed cloud-based e-commerce assurance model can be used by online customers, vendors, cloud service providers and also law enforcers.

REFERENCES

[1] Amazon. (2012). *E-commerce applications*. Retrieved from http://aws.amazon.com/ecommerce-applications/

[2] Better Business Bureau. (2012) BBB accredited business seal for the web. Retrieved from http://www.bbb.org/us/bbb-online-business/

[3] Bookwork. (2013).Home. http://www.bookworm.com/.

[4] Boulianne, E., & Cho ,C. H.(2009).The rise and fall of WebTrust, International Journal of Accounting Information Systems, 10(4), 229-244.

[5] Business Report. (2012). *News in brief*. Retrieved from http://www.iol.co.za/business/business-news/news-in-brief-1.1213090?showComments=true

[6] Cloud computing. (2013). Wikipedia. Retrieved from http://en.wikipedia.org/wiki/Cloud_computing

[7] Computer Weekly (2013). A history of cloud computing. Retrieved from *http://www.computerweekly.com/feature/A-history-of-cloud-computing*

[8] Edelman, B. (2011). Adverse Selection in online "trust" certifications and search results. *Electronic Commerce Research and Applications*, 10 (1), 17-25

[9] *Electronic Communications and Transactions Act,* (2002), s.43.1. (SA.).

[10] Gerber, M. & Von Solms, R. (2008) Information security requirements – Interpreting the legal aspects, *Computers and Security*, 27(6), 124-135.

[11] Gray, *A. (2013).* Conflict of the laws and the cloud. *Computer law and security review, 29, 58-65.*

[12] Goh, H.H., & Kok,B.C.(2010). Application of Analytic Hierarchy Process (AHP) in load shedding scheme for electrical power system. Environment and Electrical Engineering (EEEIC), 2010 9th International Conference(pp.225-235).Retrieved from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5489942&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5489942

[13] Hosein, I & Whitely, E. (2002).The regulation of electronic commerce: learning from the UK's RIP act. *Strategic Information Systems*, 11(1), 31-58.

[14] KYPLEX.(2013). *Keep your website clean from malware*. Retrieved from http://www.kyplex.com/security-seal.html#domain=http://www.kyplex.com/

[15] Mauldin, E.G, Nicolaou, A.I., & Kovar, S.E. (2005). The influence of scope and timing of reliability assurance in B2B e-commerce, *International Journal of Accounting Information Systems*, 7(2), 115-129

[16] Neto, A.M, Rittner, L., Leite, N., Zampieri, D. E, Lotufo, R & Mendeleck, A. (2007). Pearson's Correlation Coefficient for Discarding Redundant Information in Real Time Autonomous Navigation System. 16th IEEE International Conference on Control Applications.p.426-431

[17] Network world. *(2013.) News*. Retrieved from *http://www.networkworld.com/news/2012/111412-gartner-cloud-security-264268.html*

[18] PC advisor. (2013).The 15 worst data security breaches of the 21st century. Retrieved from *http://www.pcadvisor.co.uk/news/security/3338236/15-worst-data-security-breaches-of-21st-century/*

[19] Shop Bop. (2012).Shop Bop home. Retrieved from http://www.shopbop.com/

[20] Sidiropoulos, A & Manolopoulos, Y. (2006) Generalized comparison of graph-based ranking algorithms for publications and authors, *The Journal of Systems and Software*, 79, 1679-1700.

[21] South African National Standard, (2005), Security techniques - Code of practice for information security management, ISO 27001: *International Organization for standardization*, Switzerland

[22] Svantesson, D & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law and Security Review*, 26, 391-397.

[23] Trusted Cloud. (2013) *Cloud Privacy Certification*. Retrieved from http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-cloud

[24] Trusted websites. (2012). *Web site privacy services*. Retrieved from http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-websites

[25] Yahoo Finance. (2013). Google's cloud goes down affecting lots of websites. Retrieved from *http://in.finance.yahoo.com/news/googles-cloud-goes-down-affecting-173151695.html*