CHALLENGES IN IMPLEMENTIG DATA CONSISTENCY RULES FOR ONLINE PAYMENT INFASTRUCTURE

Nihad Ibrahim Abdullah [1], Abdul Karim Bin Mohamad [2],
Abd Samad Hasan Basari[3] , Ali Jalil Ibrahim[4]

[1,2,3]Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia
[1]Computer Science Institute,Sulaiman Polytechnic University -Iraq
[4]Chamchamal Technical Institute, Sulaimani Polytechnic University, Sulaimanyah 46001, Iraq
*Corresponding author: Nihad Ibrahim Abdullah (nihadib@ yahoo.com)

ABSTRACT: *Data consistency issue in payments has to consider as new and at the same time familiar challenge for management due to the massive amount of data. Thus, a major concern for payments is to reduce any risks related to data consistency in the online system to ensure system effectiveness and efficiency. Despite the development of security software and applications, questions remain about the competence depending on just technology solutions to manage data consistency risks. This study analyzed the current situation of data consistency risks which aims to address the factors that lead to such risks. Besides, it elaborated challenges that encounter with current techniques to reduce data consistency risks in the online payment system.*

1. INTRODUCTION

In recent years, the emergent role of online payments systems has been increasing due to the availability of distinctive and instant services. The terms "Online payments" or "Internet payments" are both synonyms refer to the capability to perform payment services via the Internet such as fund transfer, bill payment, loan services, credit card request and many other services which might be varied from one payment to the other. Due to this, there are many aspects of opportunties and challenges encountered in online payments systems. One of the major challenges faced online payments is represented by risk [1]. The risk is an expression indicates various aspects of danger that effect on wide organizational functionality [2]. Regarding this study, the aspects of technical risks will be discussed and elaborated further to highlight the associated areas of risks that related to Information Technology in the payments industry. The technical risks have been discussed widely in previous researches which can lead to various aspects of negative outcome including. (a) system implementation failure, (b) inadequate IS\IT strategies, (c) poor data consistency, (d) systems inconsistency, and (e) poor security and reliability.

As noticed, the problem of data consistency becomes particularly challenging for payments in which many attacks attempt to modify and alter data. The term 'Consistency' means "an unimpaired or unmarred condition applied to entire messages of a representation with an original condition" (Webster's Third New International Dictionary). So, data consistency means the representative of trusted, consistent, and complete data in order to obtain benefit from it. Due to this, threats to data consistency take many forms such as data can be copied, modified or stolen [1]. It was accepted by many literatures that payments are spent significant efforts to retain their users through the Internet. Thus data consistency risks can have impact on: less customer satisfaction increased running costs, inefficient decision-making processes, lower performance and lowered employee job satisfaction [3]. In addition, the sound of poor data consistency can affect on payments reputation to build trust internally and externally, which may imply resistance on user's acceptance to use\depend online paymenting system. In association with payment business process, data consistency risks can affect critically in many ways such as: duplicate payment made to vendors, payment might be applied to wrong customer account, and many errors might obstruct decisions to develop paymenting systems [4].

This can imply that data consistency risk if it is not identified or reduced can have negative economic and social impacts on organizations [5]. As noticed, the problem of data consistency becomes particularly challenging for payments in which many attacks attempt to modify and alter data. Despite the consequence of the problem, many technical/theoretical solutions available nowadays are still limited [6]. The main reason is due to technical focus to ensure the security programs are installed to detect unauthorized access, viruses, network attacks and other aspects of risks. In this study, the efforts will be guided towards explore the current situation and factors of data consistency risks in online paymenting systems, besides determine the current issues and challenges faced techniques that can be used to control data consistency risks in online paymenting systems.

2. FACTORS OF DATA CONSISTENCY RISKS

As noticed from previous discussions, data consistency risks can affect straightforward on the coherence and effectiveness of paymenting systems. This is because any breach of data consistency might be the first step in a successful attack against system availability or confidentiality [7].

The data consistency risks in online paymenting can be easily generated. This is because "open architecture of the Internet", it allows the opportunity for those with specific knowledge and tools to alter data in online paymenting system during transfer, store, update, and create data in user\server side [8]. Furthermore, potential risk to data consistency has been increasing in online paymenting because:

● Payments are increasing dependence on IS\IT using Internet to retain their clients, the transactions are exposed to the added threat of data corruption and inaccurate transaction recording therefore a continues enhancement to the process of data consistency is highly demanded due to this expansion and modernism of online system [9,10].

● With the wide use of web services technologies to solve the problem with processes of data consistency, in fact most of these technologies are having problems in exacting information and lack of creative strategy [11].

Therefore, the process of identifying the factors is necessary to perceive the trends of data consistency risks in online paymenting which aims to avoid them later. Relating to this, there are many studies have shown the various factors of data consistency risks in general. As argued by [12] data consistency is considered as one of basic criteria of data quality. For this reason, they provided a descriptive classification of causes of data consistency risk in data warehousing. These factors comprised numerous elements such as: (a) use of different representation formats in data sources, (b) lack of business ownership, policy and planning of the entire enterprise data contribute to data quality problems, (c) Lack of validation routines at sources causes data quality problems, and (d) data sources do not comply to business rules.

Whereas [13] noted that issues faced system design, data entry errors, and incomplete data are considered as major causes of data consistency risks. Nevertheless, in order to address the factors of data consistency risks in online paymenting systems, there are relatively limited studies have discussed factors of data consistency risks in this context.

Among these studies, a study conducted by [10] which justified increasing the data consistency risks is because of most online paymenting platforms are based on new platforms which utilize complex interfaces to link with legacy systems. As result, this can lead to increase the transaction errors, and invalid data. For this reason there is a demand to coordinate various activities of online paymenting activities with risk management concept in order to cover these risks.

3. CURRENT TECHNIQUES USED TO CONTROL DATA CONSISTENCY RISKS

In order to reflect the efforts that have been contributed in previous literatures, many academic literatures claim that data consistency risks relating to business comprise significant influences for financial institutions (refer to Table 1). The reason behind reviewing these studies is due to their recent involvement and contribution in assuring data consistency. A model of trust proposed by [14] for ensure data consistency in grid environment. The main function of this model is the utilization of hybrid reputation system which produces gradients that detect desirable from undesirable behavior. As noticed, there are many benefits from this approach which can determine the trustworthiness of an entity in grid environments. The main limitation in this approach embedded in the result which can send feedback for the situation of data good, bad, or neutral. Here, when the result shows 'neutral' the respondents do not know which action they can take to ensure data is valid.

Another study conducted by [13] who suggested a conceptual risk framework in e-Commerce that needs to be performed by internal auditors. The major concern of this framework around information and data. As [13] revealed that any information cannot be accurate nor integrated if it is resulted from system that have partial reliability. Hence, the schema that proposed by [13] investigate about identifying, analyze, and managing risk through control strategies. This schema has discussed obvious steps to manage data and information, and it mentioned in this method the communication as important component for system consistency. However, this method is lack of focus to determine with whom staffs are communicating, and what the objectives of this communication about. These steps are necessary to ensure the overall system consistency because risks can be identified clearly, but through communication it can be manipulated again since there is no such consistency monitor. The third approach is developed by [6] which discussed the policy-based approach for assuring data consistency in database management systems (DBMS). Here, the researchers specify robust data consistency policies based on DBMS. For this purpose, they developed consistency policy language which was embedded in software for specifying and enforcing consistency policies based on access control, data validation, and metadata management function. As obvious, this approach is considered as high technical solution for data consistency. However, as estimated from data consistency risk factors the solution of data consistency risks cannot be evolved from merely technical solution, instead it is the issue of reliability of information and data not just technology.

Table 1. Summary of Current Techniques that Used to Control Data Consistency

	Previous Studies in Data Consistency		
	Lim, Dai, and Bertino (2010)	Pathak(2005)	Gilbert, Abraham, and Paprzycki (2006)
Model	A policy based approach for assuring data consistency in DBMSs.	Conceptual Risk Framework for Internal Auditing in e Commerce.	Model for Trust to Ensure Data Consistency in Grid Environments.
Process	● Develop consistency policy language embedded	● Identifying, analyze, and managing risks Through control strategies	● Utilization of hybrid reputation system which

	in software • The software will specify and enforce consistency		produce gradients that detect desirable from undesirable behavior.
Scope	Database Management System	e-Commerce	Grid environment
Findings	Provide practical solution for assuring data consistency in collaborations.	This approach offered a structured assessment used by auditors	Provide a solution for exchangeable identities through weighted hybrid system
Limitation	Solution is merely technical software	Inability to define the objectives, task of Communication components	Feedback of data in reputation system.

4. DISCUSSION

As noticed previously, there are extensive literatures on the impact of data consistency risks, but only limited researchers have shown the suitable procedures to manage these risks in online paymenting. Payments should adopt robust risk management process to enable the reliability and consistency in their online system. As result, it will enhance system performance and effectiveness which might be return with many benefits for both users and management.

For this reason, managing risks and set measurement to data consistency are considered as one of the multiple efforts could be presented to improve the payment's combined performance as payments should ensure that appropriate measures are in place to ascertain the accuracy, completeness and reliability [1]. The current techniques to control data consistency risks have elaborated in this study. As well as, many benefits and limitation have been shown with these techniques. In the light of these considerations, there are numerous challenges to control data consistency risks in online paymenting. These challenges can obstruct payments to observe, review and analysis online paymenting system [15,16]. The challenges that have identified in this research with current techniques summarized by:

4.1. Setting security controls

The first challenge represented by setting security controls. There are measurements and methods need to be taken in order to assure that security controls in online paymenting system are working as planned. These measurements are subject to handle security control issues for such as: data consistency, authorization, authentication...etc.

Due to the demand of online system that sound trustful and practical. It has noticed in academic and government guidelines that payments should ensure there are appropriate controls to protect data consistency in online paymenting transactions, records and information [17]. Besides, data consistency should always be observed to ensure outcome of given data is sufficient and meet online system demand.

4.2. Ability to support the infrastructure

The second challenge for risk management techniques in online paymenting is to be applicable due to "inability to support the infrastructure" [18]. The current techniques contain a set of general rules that could be applicable in any organization, while for online paymenting and due to Internet environment have demanded a constant change and care that payments should noticed while operating online systems [9].

4.3. Assign people

In addition, the third challenge is 'assign people' which is a difficult task for payments. [21] Argues that risks in online paymenting is supposed to be managed as "pure" business issue, and it will be "dangerous" to leave risk management to "IT management" to manage it. On other hand, [1] noted the most critical issue for payments is the ability to involve technical people in risk management in order to ensure the consistency and effectiveness of the solutions. [17] implement a RACI model which is considered as an essential model to estimate people responsibility for certain function inside enterprise. Technical staff contribution can be described as 'functional' to manage payment risks, because their knowledge and solutions increasing in paymenting transactions.

4.4. The issue of when and where should be applied

The fourth challenge represented by 'when and where the proposed techniques should be applied for online paymenting systems'. As [19] noted the necessity to establish continues risk management once the systems developed. Related to this, [20] suggested that payments should proactively inquire about system life-cycle cost, business risks, and business value whether it will supply enterprises with new opportunities to operate IS\IT wisely.
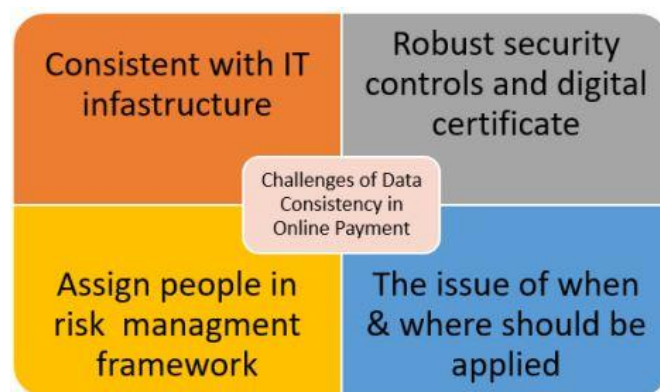

Fig. 1. Current Challenges to Control Data Consistency Risks in Online Paymenting.

5. CONCLUSION

This study have commenced with definitions of two key areas which are online paymenting systems and risks. It was

noticed that importance of data consistency risks in online paymenting, and they have become one of the critical issues since the emergent trends of cyber-attacks.

Due to this, this study have explored certain factors which can generate data consistency risks. The main reason behind identifying these factors is because it can lead to discover similar events, besides it will determine what can be used to handle the source of data consistency risks. As drawn from discussions above, the importance of data consistency have widely acknowledged. However, there are limited practices have shown in previous studies to cover data consistency risks in online paymenting systems.

ACKNOWLEDGEMENT (ACKNOW)
The acknowledgements come at the end of an article after the conclusions and before the references

REFERENCES

[1] Basel Committee on Paymenting Supervision, "Risk Management Principles for Electronic Paymenting", 2001, available at http://www.bis.org/publ/bcbs98.pdf . Accessed 9 June 2017.

[2] Geiger, H. "Regulating and Supervising Operational Risk for Payments",1999, available at www.bf.uzh.ch/publikationen/pdf/publ_850.pdf. Accessed on 1- June 2017.

[3] Kahn, B. Strong, D. & Wang, R. Information quality benchmarks: Product and service performance. Communications of the ACM, 45, 184-192, 2003.

[4] NIE J. and MA F. , "Network Security Risks in Online Paymenting", Wireless Communications, Networking and Mobile Computing p.1183, 2005.

[5] Ballou, D. P. Madnick, S. & Wang, R. Assuring information quality. Journal of Management Information Systems, 20, 9–11, 2004.

[6] Hyo-Sang, L. Chenyun, D. & Bertino, E." A policy-based approach for assuring data consistency in DBMS". 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 2-3, 2010.

[7] Stoneburner, G. Goguen, A., & Feringa, A. "Risk management guide for information technology systems (Special Publication 800-30)". US Department of Commerce, National Institute of Standards and Technology. USA, 2002.

[8] SCN Education B.V. "Electronic paymenting: the ultimate guide to business and technology of online paymenting, First edition, Birkhäuser, 2001.

[9] Monetary Authority of Singapore ."INTERNET PAYMENTING &TECHNOLOGY RISK MANAGEMENT GUIDELINES.", 2008. Retrived 15 May 2017 From http://www.mas.gov.sg/resource/legislation_guidelines/risk _mgt/I BTRMV3.pdf

[10] Ganesh, R. "Risk Management for Internet Paymenting." ISACA journal. 6. 2-3, 2001. Accessed on 15-May-2017. From. http://www.isaca.org/Journal/Past-Issues/2001/Volume-6/Pages/Risk-Management-for-Internet-Paymenting.aspx>.

[11] Ewald, T. & Wolk, K., "A Flexible Model for Data Integration", 2006. Accessed on 3-July – 2017 from http://msdn.microsoft.com/en-us/library/bb245674.aspx

[12] Ranjit S., and Kawaljeet S. "A Descriptive Classification of Causes of Data Quality Problems in Data Warehousing", International Journal of Computer Science Issues, Vol. 7, Issue 3, No 2, May 2010.

[13] Doheir, M., Kadhim, A., Samah, K. A. F. A., Hussin, B., & Basari, A. S. H. (2014). Extension of NS2 framework for wireless sensor network. Advanced Science Letters, 20(10-12), 2097-2101. doi:10.1166/asl.2014.5638

[14] Jagdish, P. , A conceptual risk framework for internal auditing in ecommerce, Managerial Auditing Journal, pp. 1-4, 2005.

[15] Austin, G., Ajith, A. & Marcin. "P. A System for Ensuring Data Consistency in Grid Environments". Proceedings of the International Conference on Information Technology: Coding and Computing, vol. 14 pp. 1-3, 2006.

[16] Caalin G. "Online paymenting in transition economies: the implementation and development of online paymenting systems in Romania", International Journal of Payment Marketing, Vol. 20 Issue: 6, pp.285 – 296, 2002.

[17] Chris, M. " Top Challenges in Enterprise Risk Management", 2010. Available at http://blogs.forrester.com/chris_mcclean/10-03-22 top_challenges_enterprise_risk_management.. Accessed on 4- October 2017

[18] ISACA, The Risk IT Practitioner, 2009, Available at. www.isaca.org/KnowledgeCenter/.../RiskIT_PG_30June20 10_Res earch.pdf Accessed on 14-July-2017.

[19] Doheir, M., Basari, A. H., Elzamly, A., Hussin, B., Yaacob, N., & Al-Shami, S. S. A. (2019). The new conceptual cloud computing modelling for improving healthcare management in health organizations. International Journal of Advanced Science and Technology, 28(1), 351-362.

[20] Peter, H." Payments at Risk: Global Best Practices in an Age of Turbulence", First edition, Singapore: Wiley, 2011.

[21] Williams, T. "A classified bibliography of recent research relating to project risk management", European Journal of Operational Research, vol. 85, no. 1, pp. 18-38, 1995.

[22] Coles, R. & Moulton, R. , 'Operationalizing IT risk management', Computers & Security, vol. 22, no. 6, pp. 487-93, 2003.

[23] Yaacob, N.M., Basari, A.S.H., Salahuddin, L., Ghani, M.K.A., Doheir, M., Elzamly, A. Electronic personalized health records [E-Phr] issues towards acceptance and adoption (2019) International Journal of Advanced Science and Technology, 28 (8), pp. 1-9.

[24] ASLI YÜKSEL, M. , "Customer's Perspectives and Risk Issues on E-Paymenting in Turkey; Should We Still be Online?" Journal of Internet Paymenting and Commerce, 2010.