A CONCEPTUAL MODEL TO CONTROL DATA INTEGRITY RISKS IN IRAQ PAYMENT GATEWAY

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: *This aim of this study is to highlight the problem of data integrity as one of the major risk aspects related to IT operational risks in the central bank of Iraq (CBI), where most of the payment services utilize all possible solutions to sustain in the market by presenting robust data integrity. However, we believe that in certain developing countries in the Middle East specifically in the region of Kurdistan-Iraq, it is highly needed to make use of the most recent development and advancement in Information and Communication ICT infrastructure, this development came after an unfortunate decade of war that acted as an obstacle on the track towards developing the ICT infrastructure, the end of this war and the settlement of governmental and social affairs in Iraq increased the potentials opportunities to implement a best practice which is available in developed or other developing countries. In this study, we studied the factors that influence the issue of data integrity in financial institutions within the central bank of Iraq (CBI) and investigated the significance of those factors. To do this, a total of 400 questionnaires were distributed for the survey, 374 questionnaires were returned and 26 questionnaires unreturned, reliability tests and factor analysis methods were used to investigate the significance of study factors. The analysis concluded that all the factors studies were significant.*

Keywords: Data integrity, Central bank of Iraq, Risk controls, Risk triggers.

1 INTRODUCTION

The past decade has witnessed an explosive growth in the generation, transformation and utilization of unstructured data, much of which has, by necessity, begun to evolve into a more structured form, From the perspective of financial institutions FIs including baking organizations, parsing unstructured data for investment decisions can consume vast amounts of IT infrastructure and organization's network elasticity, and involve considerable manual intervention from staff keeping in mind the imposed need for risk management as well, While risk systems take advantage of ever more unstructured data to generate deeper insights to support financial operations, manual intervention, reconciliation, matching and statistical techniques are required to provide much-needed structure [1]. For financial institutions, Data is considered to be an increasingly valuable asset to be managed and protected. Over the course of the summit, data was referred to as the new oil and the new currency, The centrality of information to financial institutions requires boards to treat the integrity of the data they acquire, create, use, and monetize as a primary strategic issue (Services and Summit, 2018)[2]. Indeed, as one participant stated, "Collecting, safeguarding, and analyzing data is a core competency for banks. How we do that in the future is a key question [3].

The need for financial institutions to store large amounts of data for long periods of time creates problems in that it is necessary not only to preserve this information, but also to ensure the integrity and authenticity. Moreover, over long periods of time, the data may be subject to a number of threats, including, for example, potential damage by software and/or hardware failure, accidental and/or intentional removal or modification. This introduces the need for an extremely necessary principle known as data integrity or consistency [3].

Data integrity refers to the accuracy and consistency (validity) of data over its lifecycle. Compromised data, after all, is of little use to enterprises, not to mention the dangers presented by sensitive data loss. For this reason, maintaining data integrity is a core focus of many enterprise security solutions, the practical meaning of data integrity can be compromised in several ways [4]. Each time data is replicated or transferred, it should remain intact and unaltered between updates. Error checking methods and validation procedures are typically relied on to ensure the integrity of data that is transferred or reproduced without the intention of alteration [5].

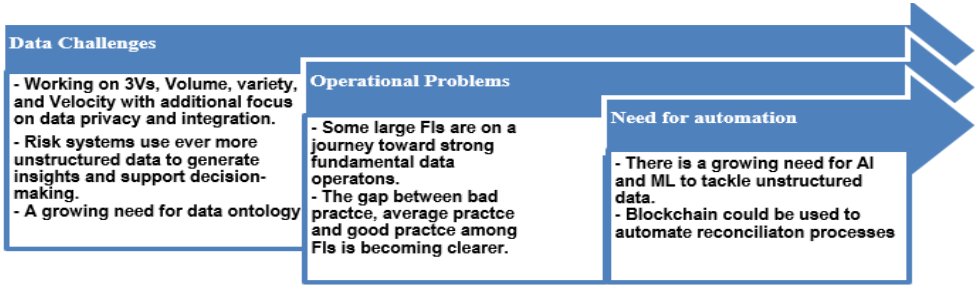
Data Challenges
- Working on 3Vs, Volume, variety, and Velocity with additional focus on data privacy and integration.
- Risk systems use ever more unstructured data to generate insights and support decision-making.
- A growing need for data ontology
Operational Problems
- Some large FIs are on a journey toward strong fundamental data operatons.
- The gap between bad practce, average practce and good practce among FIs is becoming clearer.
Need for automation
- There is a growing need for AI and ML to tackle unstructured data.
- Blockchain could be used to automate reconciliaton processes

Figure 1: Data integrity key demands

2 Issues and challenges of existing techniques of payment systems

As noticed previously, there is an extensive literature on the impact of data integrity risks, but only limited researchers have shown suitable procedures to manage these risks in online payment. Payments should adopt a robust risk management process to enable reliability and consistency in their online system [6]. As a result, it will enhance system performance and effectiveness which might be returned with many benefits for both users and management, for this reason, managing risks and set measurement to data integrity 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 [7]. The current techniques to control data integrity risks have elaborated in this study. As well as, many benefits and limitation have been shown with these techniques. In light of these considerations, there are numerous challenges to control data integrity risks in online payment. These challenges can obstruct payments to observe, review and analysis online payment system, the challenges that have identified in this research with current techniques can be faced with challenges to implement in developing countries can be summarized by:

2.1 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 the online payment system are working as planned. These measurements are subject to handle security control issues for such as data integrity, authorization, authentication...etc [8].

2.2 Ability to support the infrastructure

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

2.3 Assign people

In addition, the third challenge is 'assign people' which is a difficult task for payments. Risks in online payment are supposed to be managed as "pure" business issue, and it will be "dangerous" to leave risk management to "IT management" to manage it. On the other hand, it was noted the most critical issue for payments is the ability to involve technical people in risk management in order to ensure the integrity and effectiveness of the solutions.

2.4 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 payment systems. As scholars noted the necessity to establish continues risk management once the systems developed. Related to this, other scholars 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 [10].

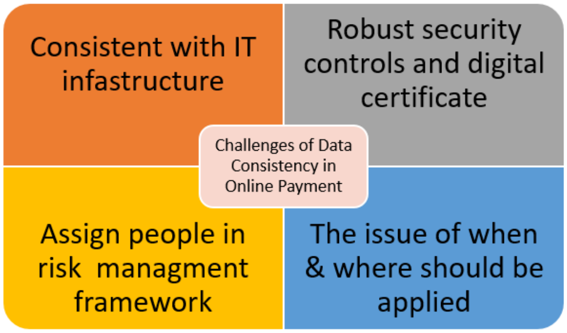
Consistent with IT infastructure
Robust security controls and digital certificate
Challenges of Data Consistency in Online Payment
Assign people in risk managment framework
The issue of when & where should be applied

Figure 2: Current Challenges to Control Data Integrity Risks in Online Payment.

3 Popular Payment Gateways And Integrity Risks

Gateways are responsible for handling various transactions amongst a client and his/her web browser. Payment is authenticated and routed by a PG. An e-commerce-based PG is a basic component to guarantee that transactions occur without any problems and in a secure fashion over the electronic systems. This section illustrates a number of popular payment gateways from perspective of integrity risks management and handling, these systems are widely used [111], and implemented worldwide, we also study the features of these systems to examine whether they consider risk management or not, the popular payment systems that are examined are as:

1. CCAvenue.
2. PayPal.
3. DirecPay.
4. EBS.
5. ABC Payments.
6. HDFC.
7. ICICI Payseal.
8. Transecute

Using an in-depth analysis of these Payment gateways, the criteria based on which our examination is performed involves features such as security, cost, customer support, Realtime transaction time, support of multiple banks and risk management [12].

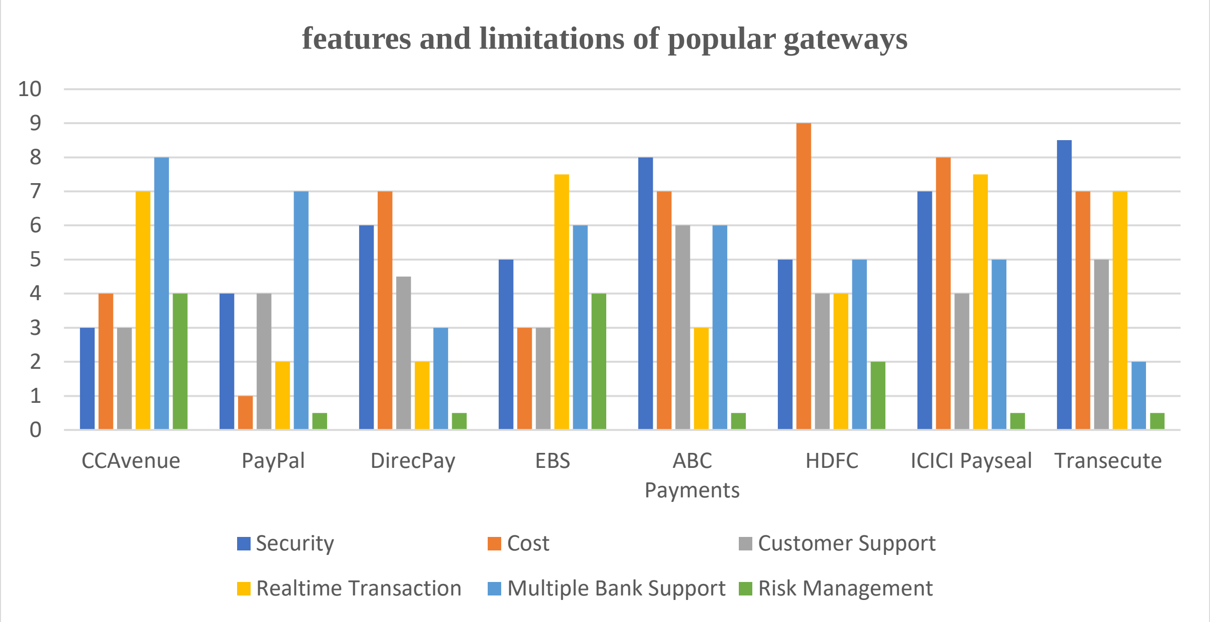

Figure 3: features and limitations of popular gateways. Source:[5]

The analysis provided in Figure 3 clearly shows that risk management is an important issue for popular gateways that still needs to be addressed and considered, few popular gateways locally consider the issue of data integrity from perspective of data security, while data integrity is evolving to cover global networks and communication systems resulting in data integrity issues all over the payment networks not only on a local basis. This made the most popular payment gateways worldwide vulnerable to certain security threats and breaches as will be illustrated in the next section [5].

4 Factors influencing data integrity

The data integrity risks in online payment 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 payment system during transfer, store, update, and create data in the user\server side 13]. Furthermore, the potential risk to data integrity has been increasing in online payment because :

i Payments are increasing dependence on IS\IT using the 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 integrity is highly demanded due to this expansion and modernism of the online system [14].

i) With the wide use of web services technologies to solve the problem with processes of data integrity, in fact, most of these technologies are having problems in exacting information and lack of creative strategy [13].

Therefore, the process of identifying the factors is necessary to perceive the trends of data integrity risks in online payment which aims to avoid them later. Relating to this, there are many studies have shown the various factors of data integrity risks in general. As argued by Weerasinghe, Erfani, Alpcan and Leckie [10], data integrity is considered as one of the basic criteria of data quality. For this reason, they provided a descriptive classification of causes of data integrity risk in data warehousing. These factors comprised numerous elements such as:

i) Using different representation formats in data sources.

ii) Lack of business ownership, policy and planning of the entire enterprise data contribute to data quality problems.

iii) Lack of validation routines at sources cause data quality problems.

iv) Data sources do not comply with business rules.

In the era of financial organizations and banking system models, many professionals and specialists have explored the factors influencing the concept of data integrity within the organizations data repositories and came up with various thoughts, results and conclusions. In an effort to explore these variables and decide which of them directly influences the achievement of data integrity in different payment gateways, many financial and commercial institutions network issues using the resource-wide network [21]. While the utilization of E-payment solutions by financial institutions or E-government systems has many benefits, many issues and difficulties still need to be resolved [15]. This section introduces the factors that will be considered in different dimensions, these dimensions are to be examined from the perspective of their influence on achieving data integrity best practices and risk management. Table 1 summarizes the factors that influence the data integrity in FIs.

Table 1: factors influencing data integrity.

1.	Organizational Factors	Technology Readiness
		Top Management Support
		Quality System and Services
		Facilitating Conditions
2.	Technological Factors	Compatibility
		Complexity
		Availability
		Confidentiality
		Reliability
		Cost Efficiency
		Perceived Security and Privacy
		Relative Advantage
		Quality of Internet Connection
3.	Risk controls	User Awareness
		User Attitude
		Hedonic Motivation
		E-Trust
		E-Satisfaction
4.	Technology Acceptance Factors	Perceived Usefulness
		Perceived Ease of Use

5 Data integrity risks

The term data integrity risk can be defined as the risk that the data stored and processed by organizations' ICT infrastructure is incomplete, inaccurate or inconsistent across different ICT system infrastructure, for example as a result of inadequate data processing controls during the different phases of the data processing life cycle (i.e. designing the data architecture, building the data model and/or data dictionaries, verifying data inputs, controlling data extractions, transfers and processing, including rendered data outputs), impairing the ability of an institution to provide services and produce (risk) management and financial information in a correct and timely manner [16], the data integrity risks may arise due to the following operational reasons:

5.1 Dysfunctional data processing or handling

The failure of the organization to process or control their data is one of the data integrity risks, it may occur due to system, communication or application errors or failures, during data extraction, transfer and load (ETL) process, this causes data to be corrupted or lost [17].

5.2 Data validation controls

The design of data validation controls may encounter operational or logical errors relating to missing or insufficient automated methods for data input and acceptance, data transfer, data processing and output in the ICT infrastructure of the organization, this normally occurs when the organization utilizes third party data [1].

5.3 Data architectures

The data architecture specifies the organization of data within an organization including the relationship between different data repositories for efficient retrieval of data, the design of data architectures, data flows or data dictionaries may result in producing multiple versions of the same data across the organizations [1]

5.4 Data lifecycle

An FI may face challenges in keeping the integrity of their data due to attributes of their data regardless of all data processing procedures and operations [18].

5.5 Controlled data changes

The importance of data for financial organizations inspire the management of these organizations to continuously manipulate and reformat their data repositories to guarantee their data integrity, this in turn may cause data errors resulting from lack of controls on the correctness and justified nature of data manipulations performed during the deployment of ICT infrastructure, examples for issues related controlled data changes include [19]:

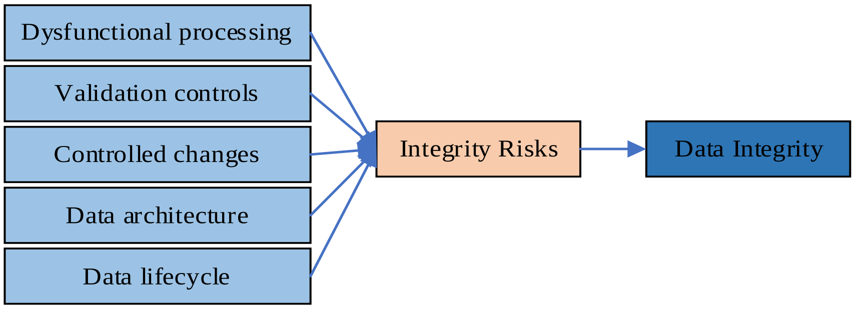

Figure 4: Data integrity risks framework.

7 The proposed model i

After studying the factors that influence the data integrity within an FI earlier in this chapter, and after specifying the data integrity risks that emerge due to the factors that influence data integrity, the proposed model is to be designed considering both dimension:

i) Factors that influence data integrity.

ii) Data integrity risks emerge due to factors influencing data integrity.

The proposed model will highlight the impact of both the dimensions on data integrity, considering the factors in (1) and the risks in (2), the model will be designed so that it utilizes the data integrity risk controls mentioned in previous section to overcome the issue of data integrity risks within payment gateways in Iraq as follows:

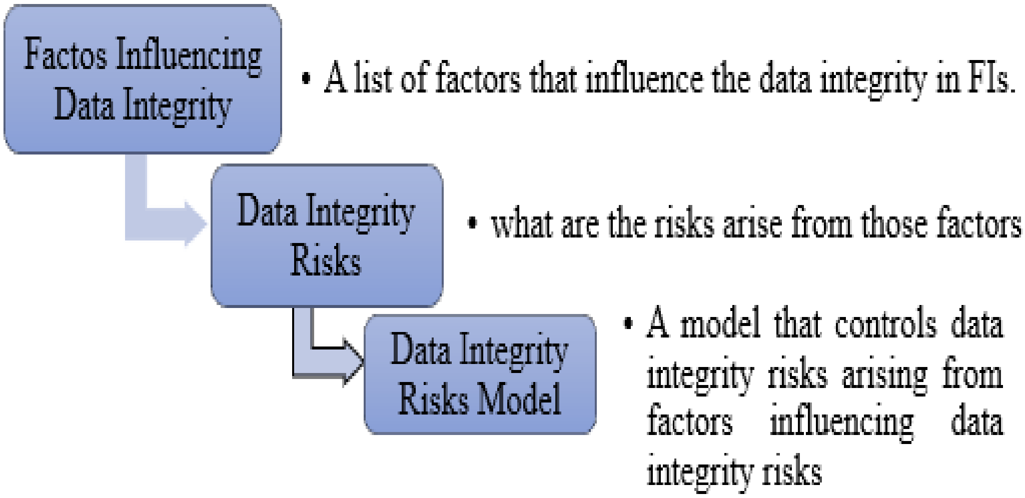
Factos Influencing Data Integrity
• A list of factors that influence the data integrity in FIs.
Data Integrity Risks
• what are the risks arise from those factors
Data Integrity Risks Model
• A model that controls data integrity risks arising from factors influencing data integrity risks

Figure 5: The proposed Model Flowchart.

8 Research Questions, Objectives and Hypotheses

In order to answer the questions of the study and achieve its objectives, the validity of the study's hypotheses was verified. And, the study questions, objectives and related hypotheses were clarified, as shown in Table 1. The following is a detailed explanation of the study's hypotheses and the extent to which its objectives were achieved:

Table 2: Research Questions, Objectives and Hypotheses.

Question	Objectives	Hypothesis
1. What is the status of data integrity risk controls implementation in Iraq payment gateway?	**1.** To investigate the current status of data integrity risk controls implementation in Iraq payment gateway.	H1, H2, H3, H4
2. What are the factors influencing data integrity that influence a successful implementation of data integrity in Iraq payment gateway?	**2.** To identify the factors influencing data integrity that influence the implementation of data integrity in Iraq payment gateway.	H5, H6, H7, H8, H9, H10, H11, H12, H13, H14, H15, H16, H17,
	3. To correlate factors influencing data integrity of data integrity risk controls implementation to data integrity in Iraq payment gateway.	
3. How to develop a best practice conceptual model for the implementation of control data integrity risks in Iraq payment gateway?	**4.** To develop a conceptual model of control data integrity risks best practices in Iraq payment gateway.	

9 Methodology

The study will be conducted using a qualitative research method using a series of semi-structured interviews with key stakeholders in participating organizations including employees and top management representatives to know how they feel about data integrity and risk management best practices and its current practices in their workplaces. Figure (6) illustrates the overall research design to be followed in order to complete this study, this design may be modified periodically according to research requirements and variables.

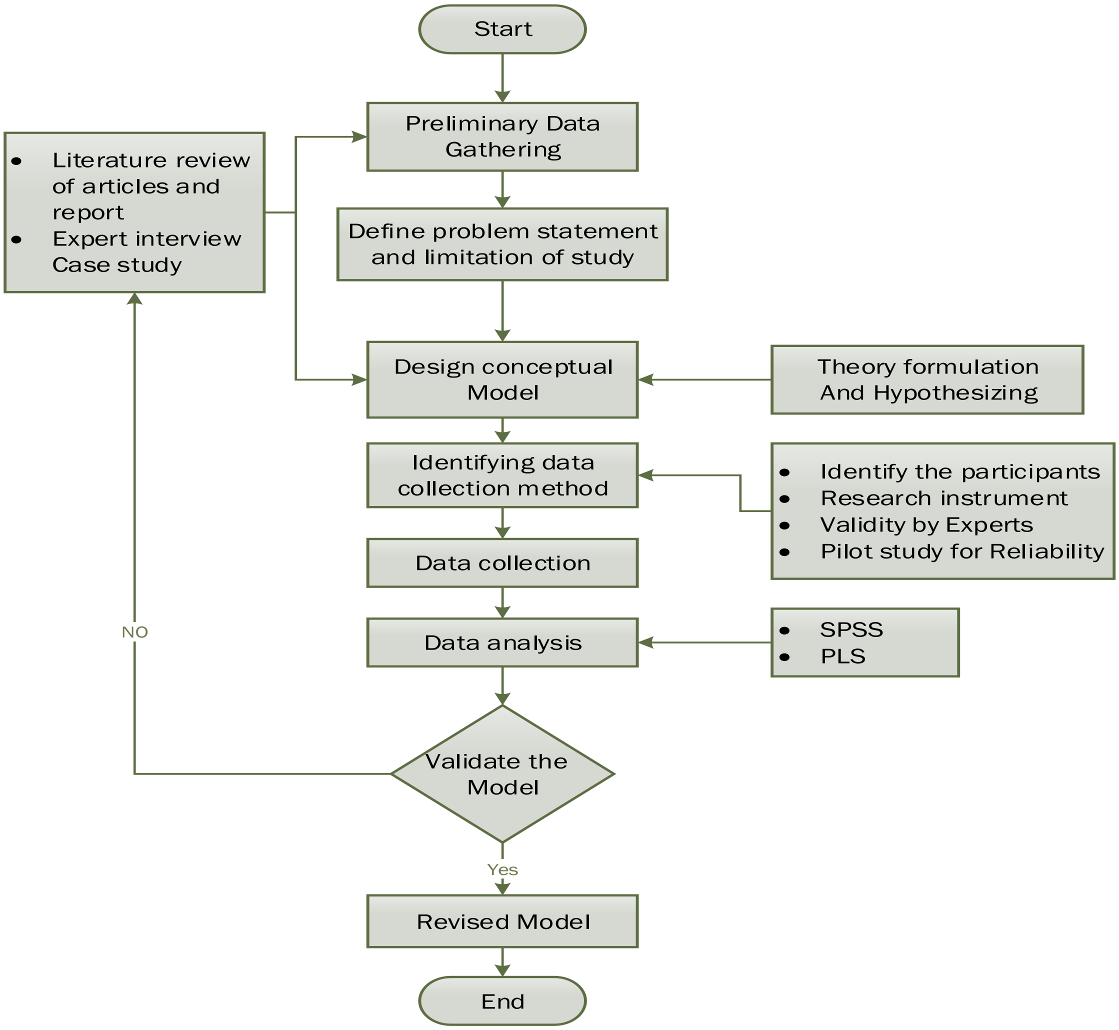
Start
Preliminary Data Gathering
Literature review of articles and report
Expert interview
Case study
Define problem statement and limitation of study
Design conceptual Model
Theory formulation And Hypothesizing
Identifying data collection method
Identify the participants
Research instrument
Validity by Experts
Pilot study for Reliability
Data collection
Data analysis
SPSS
PLS
NO
Validate the Model
Yes
Revised Model
End

Figure 6: research design.

10 Data collection and response rates

In this study, 400 set questionnaires were distributed to respondents However, only 363 questionnaires were fully answered and completed by respondents. The survey was conducted within 13 weeks. The total number of distributed survey questionnaires was 400, Of the survey, 374 questionnaires were returned and 26 questionnaires unreturned. There were missing data for eleven surveys collected from the respondents which neglected thus, a total of usable questionnaires was utilized with 363 (90.75%) response rate. The sample size of n=363 was considered as sufficient for this study. Table 4.1 shows the summary of data collection and response rate.

Table 3: Summary of data collection and response rate

Responses	Total
Distributed questionnaires	400
Returned questionnaires	374
Unreturned questionnaires	26
Missing data	11
Usable questionnaires	363
Overall response rate	93.5%
response rate after neglecting missing data	90.75 %

11 Data analysis

The reliability test was conducted for the first section (factor influencing data integrity). The results showed that the reliability coefficient (alpha value) amounted to 0.945, which got a value greater than 0.7. Therefore, it can be concluded that the section (factor influencing data integrity) has high reliability, and this is confirmed by the results of the reliability test for each of the dimensions of this section was as shown in Table 4. The reliability test was also conducted for the second section (factor influencing data integrity), and the results showed that the reliability coefficient (alpha value) amounted to 0.978, which got a value greater than 0.7. Therefore, it can be concluded that the section on (factor influencing data integrity) has high reliability, and this is confirmed by the results of the reliability test for each dimension in this section, and was as shown in Table 4. The reliability test was conducted for the third section (Data integrity), and as shown in Table 4, the reliability coefficient (alpha value) amounted to 0.856, which is a value greater than 0.7. Therefore, it can be concluded that the section on the Data integrity has high reliability and there is no need to delete any item from the items included, which is confirmed by the statistical results that were mentioned in the Item-Total

Statistics for Data integrity where each item of the Data integrity section has a stability value of more than 0.7.

Table 4: Item total statistics and analysis.

Item-Total Statistics				
	Scale Mean if Item Deleted	**Scale Variance if Item Deleted**	**Corrected Item-Total Correlation**	**Cronbach's Alpha if Item Deleted**
A1	14.15	7.962	0.776	0.883
A2	13.58	8.375	0.675	0.836
A3	13.86	8.111	0.654	0.876
A4	13.89	7.784	0.719	0.813
A5	13.75	7.895	0.690	0.865
A6	14.73	7.635	.882	.866
A7	14.13	7.579	.773	.818
A8	14.14	8.054	.715	.876
A9	14.42	8.814	.695	.869
A10	14.32	7.397	.719	.886
A11	14.41	7.107	.505	.832
A12	14.23	6.312	.670	.759
A13	14.71	6.226	.609	.727
A14	14.92	5.986	.627	.757
A15	14.72	6.267	.693	.758
A16	13.81	7.292	.685	.875
A17	13.28	6.776	.757	.856
A18	13.76	6.962	.754	.854
A19	13.91	7.397	.673	.876
A20	13.87	7.048	.778	.853

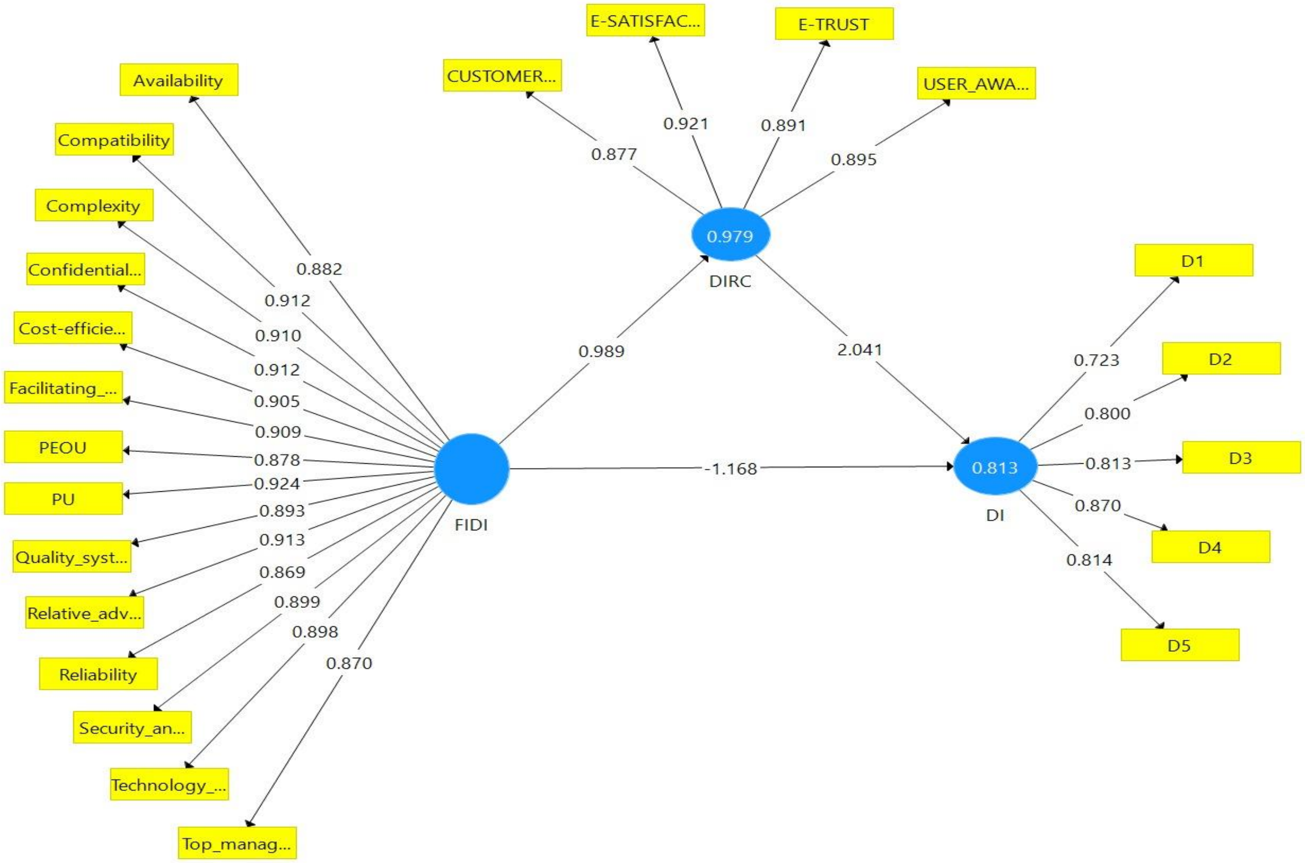

Figure 7: Research model and analysis results.

12 CONCLUSION

The data integrity is an extremely vital and significant term that indicates the performance of any financial institution that offers online banking and online payment services in an environment that utilizes a reliable ICT infrastructure. This study investigated the current status of data integrity in the central bank of Iraq and found that a number of factors that are significant and essential are missing and not considered when controlling and maintaining data integrity and risk controls in the CBI. The study recommends that the top management of CBI must consider the studied factors and implement them when setting new standards and policies to manage and control daily transactions to guarantee the integrity of their data and avoid the risks that may arise during payment and transactions processing.

Acknowledgements

The authors would like to thank Centre for Research and Innovation Management, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM) for providing facilities in this study.

REFERENCES

1. Chartis, 2018. Data Integrity and Control in Financial Services. *Chartis Research Ltd*, (March).
2. Services, F., and Summit, L., 2018. Data governance : securing the future of financial services. , (January).
3. N, I.N.H.U., Nance, G., and Series, A.R., 2018. system and method for verifying data integrity using a blockchain network. *Science*, 2.
4. Artamonov, I., Deniskina, A., Filatov, V., and Vasilyeva, O., 2019. Quality management assurance using data integrity model. *MATEC Web of Conferences*, 265, p.07031.
5. Olanrewaju, R.F., Ul Islam Khan, B., Ul Islam Mattoo, M.M., Anwar, F., Anis, A.N., and Mir, R.N., 2017. Securing electronic transactions via payment gateways – a systematic review. *International Journal of Internet Technology and Secured Transactions*, 7(3), pp.245–269.
6. Ul, B., F., R., Mehraj, A., Ahmad, A., and Assad, S., 2017. A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations. *International Journal of Advanced Computer Science and Applications*, 8(5), pp.256–271.
7. Carbó-Valverde, S., and Kahn, C.M., 2016. Payment systems in the US and Europe: efficiency, soundness and challenges.
8. Solat, S., 2017. Security of Electronic Payment Systems: A Comprehensive Survey. , (January 2017).
9. Salimon, M.G., Yusoff, R.Z. Bin, and Mohd Mokhtar, S.S., 2017. The mediating role of hedonic motivation on the relationship between adoption of e-banking and its determinants. *International Journal of Bank Marketing*, 35(4), pp.558–582.

10 Weerasinghe, S., Erfani, S.M., Alpcan, T., and Leckie, C., 2019. Support vector machines resilient against training data integrity attacks. *Pattern Recognition*, 96.

11. Kumar, D., 2019. Electronic Payment System , Risk and security issues. , 6(March), pp.1–7.
12. habad, M.A.R., and Kavitha, M., 2018. Credit card fraud detection using neural networks at merchant side. *Journal of Computational and Theoretical Nanoscience*, 15(1112), pp.3373–3375.
13. Zhang, Z., Wang, P., and Xu, H., 2019. Executives' preference for integrity and product quality: Evidence from the Chinese food industry. *Economic Modelling*.
14. Kotliarenko, A., Chirkov, A., and Kharchenko, V., 2019. Features of the estimation of the influence of various factors on the integrity of the RPV reactor under the action of a melt of metals during a severe accident. *Procedia Structural Integrity*, 16, pp.223–229.
15. Almunawar, M.N., 2015. Benefits and Issues of Cloud Computing for E-Government. *Review of Public Administration and Management*, 3(1), pp.1–2.
16. Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A., and Ullah Khan, S., 2015. The rise of

17.Shujaat, S., 2019. Consumer Acceptance of Online Banking : Application of Technology Acceptance Model Consumer Acceptance of Online Banking : Application of Technology Acceptance Model. , 14(January 2018), pp.41–52.

18. Latifi, S., 2019. *16th International Conference on Information Technology-New Generations (ITNG 2019)*,
19. Nisar, T.M., and Prabhakar, G., 2017. What factors determine e-satisfaction and consumer spending in e-commerce retailing? *Journal of Retailing and Consumer Services*, 39(July), pp.135–144.

“big data” on cloud computing: Review and open research issues. *Information Systems*, 47, pp.98–115.

20. 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.
21. Mahalakshmi, B., 2017. Assessment on Security Issues and Classification in Cloud Computing. *International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)*, 1(1), pp.30–43.