MEU جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY

Investigation on Order-Preserving Encryption for Database in Cloud Computing

دراسة تحليلية في المحافظة على الترتيب لقواعد البيانات السحابية

Prepared by:

Amro Akram Bazoon

Supervisor:

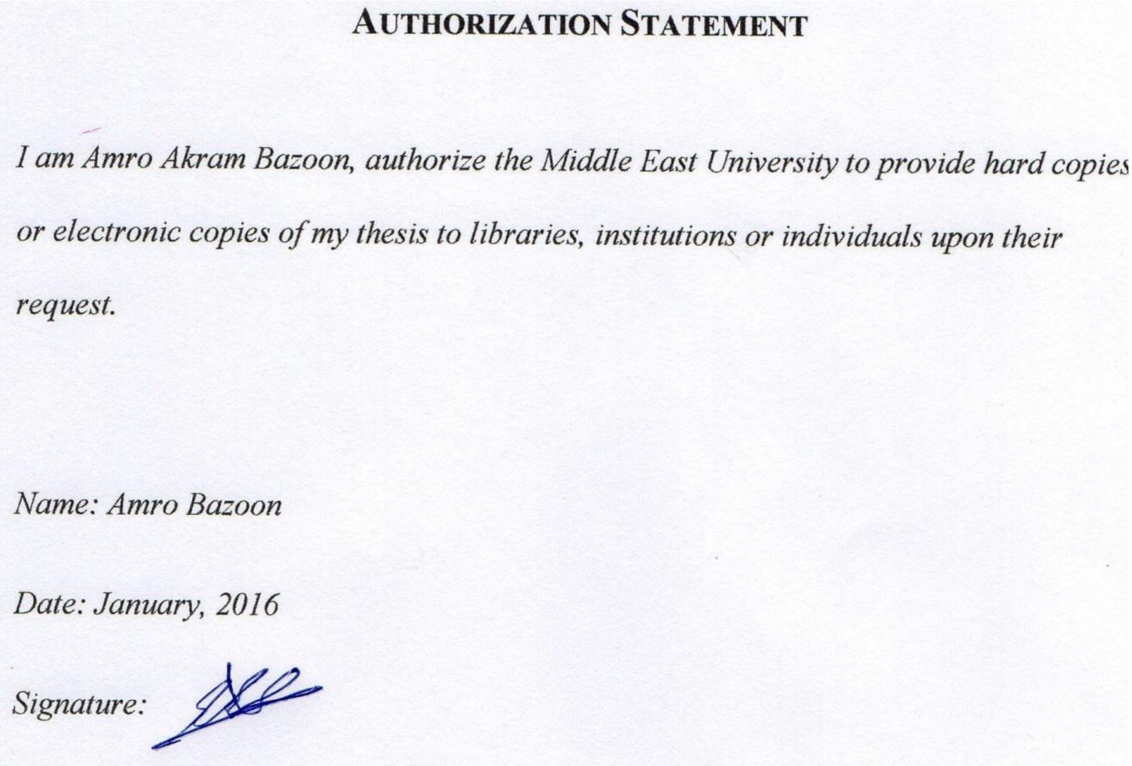
Prof. Ahmad K. A. Kayed

A Thesis Submitted in Partial Fulfillment of the Requirements of the Master Degree in Computer Science

Faculty of Information Technology

Middle East University

January, 2016



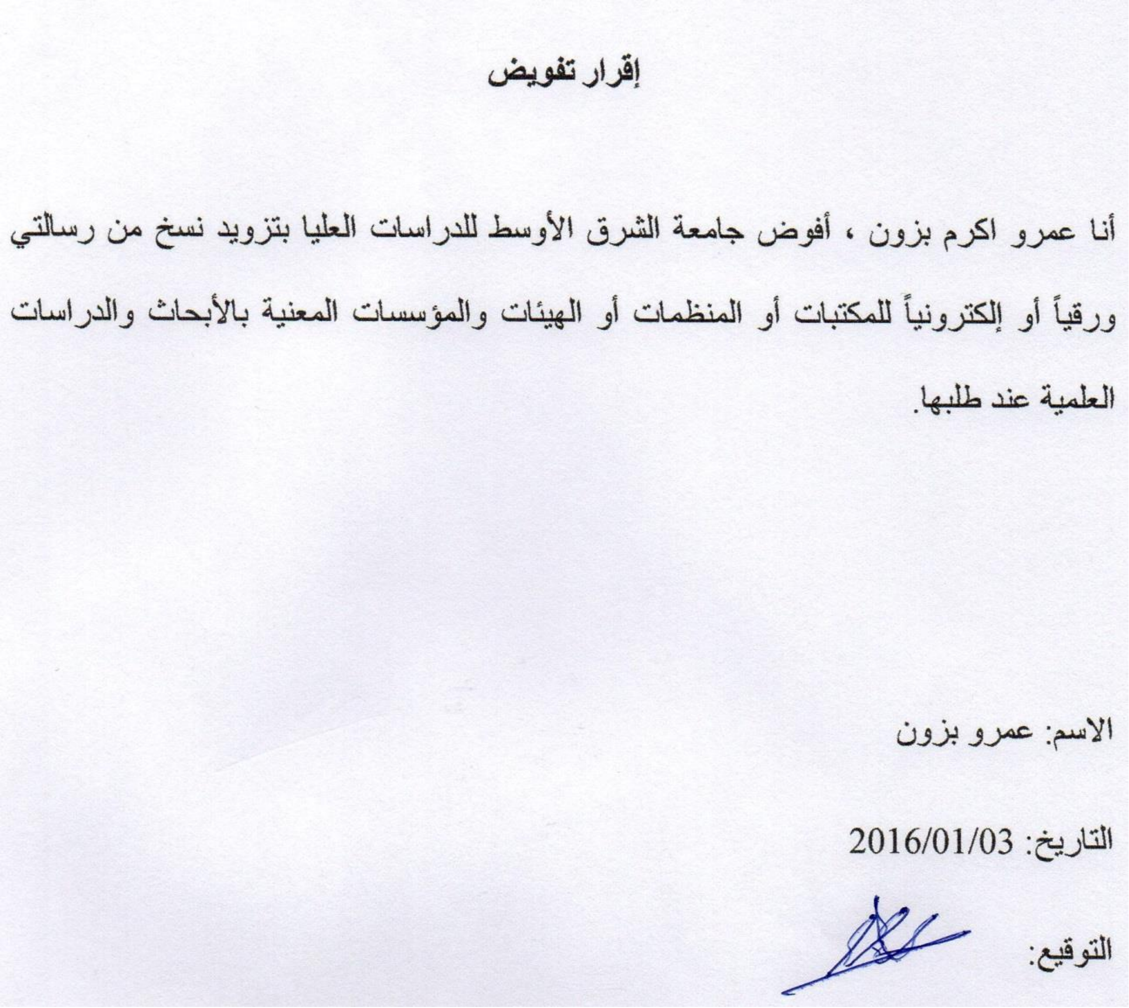
AUTHORIZATION STATEMENT

I am Amro Akram Bazoon, authorize the Middle East University to provide hard copies or electronic copies of my thesis to libraries, institutions or individuals upon their request.

Name: Amro Bazoon

Date: January, 2016

Signature:



إقرار تفويض

أنا عمرو اكرم بزون ، أفوض جامعة الشرق الأوسط للدراسات العليا بتزويد نسخ من رسالتي ورقياً أو إلكترونياً للمكتبات أو المنظمات أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: عمرو بزون

التاريخ: 2016/01/03

التوقيع:

Examination Committee Decision

This is to certify that the thesis entitled "Investigation on Order-Preserving Encryption for Database in Cloud Computing" was successfully defended and approved on Jan, 2016

Examination Committee Members	***Signature***
(Head of the Committee and Supervisor) **Dr. Ahmad Kayed** *Professor* *Dean Faculty of IT* *Middle East University*	
(Internal Committee Member) **Dr. Ahmad AL-Hmouz** *Assistant Professor* *Vice Dean Faculty of IT* *Middle East University*	
(External Committee Member) **Dr. Mohammed Ababneh** *Professor* *AL-Balqa' Applied University*	

ACKNOWLEDGMEN

I utilize this opportunity to thank everyone helped me reach this stage and everyone who encourage me during performing this thesis. I want to thank Prof. Ahmad K. A. Kayed for his guidance and supervision during writing this thesis. Extended thanks are also for my family and friends who encourage me during writing this thesis. I also want to thank everyone who believes that the knowledge is right for everyone.

Table of Contents

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IT	Information Technology
HP	Hewlett Packard
AWS	Amazon Web Services
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
DaaS	Database as a Service
SFA	Sales Force Automation
CRM	Customer Relationship Management
DBA	Database Administrator
DBMS	Database Management System
PHE	Fully Homomorphic Encryption
FHE	Partially Homomorphic Encryption
IP	Internet Protocol
OPE	Order Preserving Encryption Scheme
VB	Visual Basic
NIST	Institution of Standards and Technology

ABSTRACT

Investigation on Order-Preserving Encryption for Database in Cloud Computing

Prepared By:

Amro Akram Bazoon

Supervised By:

Prof. Ahmad K. A. Kayed

The detection of the cloud computing has led to the creation of a new revolution in the world of technology. Cloud Computing has a serious influence in decreasing the cost of firms and businesses due to the easiness of using and the probability of changing the quality of the work in a short period of time. This thesis proposed an improvement of the data encryption technique that using by Liu and Wang. The improvement aimed to increase the amount of ambiguity (noise) to enhance the level of security. This thesis investigated the effect of adding more parameters with several ranges to Liu and Wang formula, the goal was to find the effect of these parameters on the security as well as the performance also. Adding more parameters will increase the security but with add a bad effect on the performance. The results showed adding one parameter will increase the security and decrease the performance by of 2%. However, multiplying by one parameter will give a better security with 3% decreasing in performance, changing the noise needs to update and re-indexing of the database. The results showed that the re-indexing time will be almost the same in both cases, when adding or multiplying by new parameter. It showed that the execution time will be increased by 0.003 per record. This study proposed four different linear equations with several data values to raise the ambiguity (noise) in the procedure of adding data to the cloud database. We had had numerous experiences and scenarios on cloud database as will be shown in the following chapters to find the best method for the ratio of adding noise to data that stored in cloud database.

Keywords: Cloud computing, encryption, Liu and Wang, parameters, security, performance.

الملخص

دراسة تحليلية في المحافظة على الترتيب لقواعد البيانات السحابية

إعداد : عمرو أكرم بزون

إشراف : ا.م.د احمد الكايد

أدى اكتشاف الحوسبة السحابية في خلق ثورة جديدة في عالم التكنولوجيا. الحوسبة السحابية لديها تأثير كبير في خفض التكلفة للشركات والمؤسسات التجارية ايضا سهولة الاستخدام و تغيير نوعية العمل في فترة قصيرة من الزمن. واقترحت هذه الأطروحة تعديلا على تقنية تشفير البيانات ليو و وانغ. التعديل يهدف إلى زيادة كمية الغموض (الضوضاء) لتعزيز مستوى الأمن. هذه الأطروحة قامت بدراسة تأثير إضافة المزيد من المعلمات مع عدة نطاقات للصيغة ليو وانغ. وكان الهدف هو العثور على أثر هذه المعايير على مستوى آمن فضلا عن الأداء (وقت التنفيذ). إضافة المزيد من المعلمات زاد الحماية ولكنها ادت الى انخفاض في الأداء. أظهرت النتائج ان اضافة متغير واحد سوف يزيد من مستوى الأمان وفقدان 2٪ من الأداء. ومع ذلك، ضرب من قبل معلمة واحدة سيعطي الأمن بشكل أفضل مع 3٪ تفقد في الأداء. تغيير هذه الضوضاء يحتاج إلى تحديث وإعادة فهرسة-قاعدة البيانات. أظهرت النتائج أن وقت إعادة الفهرسة ستكون تقريبا نفس في كلتا الحالتين أي عند إضافة أو ضرب من قبل معلمة جديدة. وبينت ان وقت التنفيذ سيتم بنسبة 0.003 لكل سجل. واقترحت هذه الدراسة اربعة معادلات خطية مختلفة مع عدة قيم البيانات لرفع الغموض في الإجراء من إضافة البيانات إلى قاعدة البيانات السحابية. كان لدينا العديد من الخبرات وسيناريوهات على قاعدة البيانات السحابية لإيجاد طريقة مثلى لنسبة الضوضاء إضافة إلى البيانات المخزنة في قاعدة البيانات السحابية.

كلمات مفتاحية: الحوسبة السحابية , الحماية والغموض, الفعالية, ليو و وانغ, التشفير.

Chapter One:
Introduction

1. Chapter One: Introduction

1.1. Preface

When you store your photos online in state of on your computer, or when you use the webmail or the social networking sites, here you are utilizing the “cloud computing” service. If you are a community and you need to use, as an example the online billing service rather than informing the in-house one you have been utilizing for a lot of years, that online billing facility is the “cloud computing” service.

Cloud computing is the modern networking and the virtualization infrastructures have been made impression of the database outsourcing, to the third party not only the possibility, nonetheless sometimes a necessity. Following to several researches have been achieved on the database outsourcing, there were a number of systems have been suggested that utilizing the cloud services for this mission. On the other hand, even though the massive benefits of the cloud computing methodology has been recognized that, there are a number of significant matters that required to be addressed for it to be possible, the greatest critical issue of which is the security. There have been three major matters related to the security in this context: confidentiality, integrity (verifiability), and availability. (Sathyavani, S., et al., 2013)

Cloud computing denotes to the distribution of the computing resources over the internet. As opposed to keep data on the hard drive, or to update the applications using a service over the internet, at several locations to stock the information or use its applications. Doing so may give to raise up to determined privacy implications. (Chou, K., 2011)

Several private companies and government institutions that require to work as a computing resources to carry out its missions, and organization of a huge projects depending on them, on an environment and on the electronic resources emails, and establishment of these electronic environments want email, where the cost of these resources for the acquisition of the hardware, and the spaces be at work on it, as well as of the employing staff professional engineers, and professionals rationing in the IT section, in order to be work of maintenance and the daily or the annual repair issues. In case if it happened and followed up the backups to enterprise the data and all the missions of the subject was mentioned previously, it is an additional cost on the original cost for building these electronic units of the organization. (Goh, E.J., 2003)

Therefore, started thinking about a novel technology construction depending on the provision of the electronic services costs, effort, price, and less time, the importance was placed on two features: the provision of resources and work efficiently. Cloud computing technology discover where transported an excessive revolution in the world of technology, over the advantages that have been labeled in abundant study predecessor, confusion at the abundance of time, effort and cost, and also decreased the number of workers in the IT department, because they have accepted to deliver all the services and the electronic exchange for an agreed amount, whether yearly or monthly, based on the nature of the company's work. (Voorsluys, W., et al. 2011)

The features achieved by the cloud computing technology is commerce from everywhere and anytime, the only necessity is right to use and access to the internet and then began to deal with this data, where is no longer, the employer want kept data or programs on the devices themselves, as the case in conservative technology. The device comes to be just a tool for employers' access to storage data in it. More in recent times have been launched numerous labels dissimilar kinds of major cloud computing where it comes to be in music cloud, cloud applications, OS cloud, and cloud storage services. (Lee, & Kim, 2013)

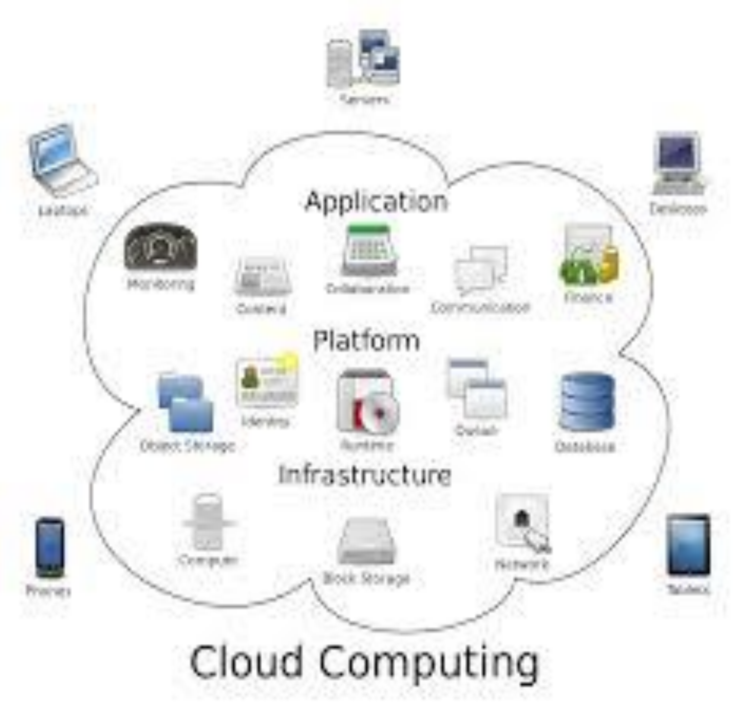


Figure 1:1 Cloud computing (Lee, & Kim, 2013)

There are a lot of cloud computing definitions one of these detentions are referred to U.S. National Institute of Standards and Technology (NIST):

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models".

Clouds computing which is a great number of congregations of the systems are associated in a private or, a public networks to make available scalable infrastructure, for the applications data and for the files storage. At the coming on of this technology the calculation of cost, application hosting, contented storing, and delivery is decreased expressively. Cloud computing is an effective method to practice direct cost advantages, and it has the possibility to make over the data center from the capital intensive to an adjustable valued environment. The impression of the cloud computing is depending on an actual fundamental attitude of the reusability of IT capabilities. (Shmueli, E., 2010)

The variance that the cloud computing carries in compare of the traditional thoughts of “grid computing”, “distributed computing”, “utility computing”, or “autonomic computing” is to expand horizons across over the organizational limitations. Forrester defined the cloud computing as: “The pool of inattentive, extremely scalable, and achieved compute infrastructure accomplished of hosting end client applications and to be paid by the consumption.”

The Cloud Computing is well thought-out a very significant and fresh business model, since this technology has established a success by letting employers to admission services and data, over and done with any device with internet right of entry, dropping the cost, easiness of use, flexibility to add new services in the work. Supplementary, the cloud computing is probability exchanging the natural surroundings of work in the limited hours and low cost compared to the traditional technology. (Bernhardt, V., 2013)

The cloud computing is putting the data in a protected database. The benefits of the cloud computing environment database seem as an attractive technique for the databases. Consequently, data safely goes into a massive concern in direction of client's data security. The database encryption is utilized for overcoming this concern. (Conway, G., 2012)

All the terms that have been launched on the new forms storage services of cloud computing, where they were firing the data as a service term (DssA), a strategy has been working out. The goal is to reach the required data stored in the cloud that are safe, simple and fast when is the different demand regions for users to deal with everyone based on user requests data. DaaS works safely, fast and simple to meet the demands of users, the strategy to reduce the user cost through the service, provide technical support, provide maintenance, provision of development and modernization, expansion memory when the user needs to be distributed at any time, at an extra cost. The features of (DaaS) are the most important technical, because of the easiness to access data and deal with it, immediately without a need to understand this data. Data quality is dealing with data and processes through data services that help to improve the percentage of certain data. (Shmueli, E., 2010)

The subject of encryption is improved in database of cloud computing, where are finding many algorithms for securing data such as keeping the security by add noise to the data, and modify some of the existing algorithms. (Conway, G., 2012)

In previous studies were clarified the importance of security, and its impact on the fear in used the cloud computing through a set of encryption algorithms, which is represent solutions to the problem of security, but there are some problems faced when progressed solving the security problem, for example its impact on the performance. (Saleh, E., et al. 2015)

The last term indicates a technology of cloud computing is using in organizations and clients that have the ability to access applications from any place in the world to meet their needs. The computing world is quickly changing towards creating programming used by other persons, instead of running on their personal computer. (Sntose, N., 2009)

The benefit of utilizing the cloud computing is represented on dissimilar forms of which, the cloud is an advantageous essentially for companies that cannot have enough money the same amount of hardware and the storing space as a huge firm. Minor companies could be stored the information deprived of the need of ordering the amount of storing space over utilizing the cloud. The cloud makes probable for the employer to entree information from anywhere at any time. Even though a traditional computer setup requires being in the same location of the data storing device. Supplementary, it can the employers run essential different applications. (Darwish, D., 2012)

The three main important types of encryption are the symmetric, asymmetric encryption, and hashing. Symmetric encryption function is to carry the readable data (“plain text”) in crypto parlance, rush and mix up it to make it unreadable to protect it from intruders eyes whereas it is being to store on a disk or to transmit over a network, then the unscramble it again when it is needed. It is generally quick, and there are many of the good encryption methods to pick out from. The most significant thing is to remember about symmetric encryption is the same in both sides need access to the same key. The best use of this type is in services that store the encrypted data on behalf of a user when the leave of the decryption key is in the hands of the user. Also use to the encrypted computers or the device storage, the resulting encrypted data still stored on the device is then useless to anyone. Finally to create a secure channel between the two network endpoints, as long as there is a disconnected scheme for the securely exchanging the key. Order preserving is a method of the symmetric encryption used in this research. (Lee.M, 2013)

Asymmetric encryption also takes the readable data, scrambles it, and unscrambles it again at the other end, but there is a twist: a different key is utilized for every end. Encryption used the public key to scramble the data, and the descriptors used the matching private or what called the secret key on the other end to unscramble it again.

Hashing is what actually happened when you hearing about passwords is being encrypted. Carefully speaking, hashing is not a form of the encryption, though it is used the cryptography. Hashing takes the data and make a hash out of it, a chain of data with the most three significant properties: the same data always produces the same hash, impossible to inverse it back to the original data, and it is infeasible to make another chain of data that creates the same hash. (Lee.M, 2013)

In this thesis, attempted progressing model offers safe database in the cloud computing where it works to keep data in a safe location.

1.2. RESEARCH PROBLEMS

Recently, searching on an encrypted database is outface for the cloud computing. Utilizing the OPE (Order Preserving Encryption) will allow the cloud provider to seek over a database without knowing the original data. The OPE process solves the searching matters but decreases the security. Where OPEs tools update and manage the information, also has the probability of changing to a particular data in the database or add a new data without the required of data decrypt in the database and the features of OPE the ability of managing all of the databases. This is due to some data could be leaked because of releasing the order of the original data. Liu and Wang was solved this leak by the addition of noises to the original data utilizing of some linear function with two client-based parameters, where the noise should be measured utilizing the applied parameters. This research is looking to inquire into the algorithm. Studies number of parameters that to be utilized, also to study the time of changing these parameters then changes the function. In addition to study the influence of these changes to the security and performance. Therefore, this study investigates the best solution to provide the best security and performance. The major target of this research is to enhance Liu &Wang algorithm and change it to be more secure with saving the performance, there are different solutions to accomplish this target, and one of these solutions will be done by adding more parameters and more equations, then determine what happened to the security and performance. In this thesis, the suggested program would be answered by the next three questions:

When does it require altering the parameters?

Which linear function will accomplish an acceptance degree of security and performance?

Number of parameters can be supplementary to accomplish enhanced security derived of affecting on the performance?

1.3. RESEARCH OBJECTIVES

The main objective of the research is improving the performance and security for stored data in the database inside the cloud computing with maintaining the performance. Where was all the previous researches focus on improving the security with observes an increase in the complexity of data that affected the performance when retrieving or processing the data. Increase the complexity of the data leads to the difficulty in dealing with the data, leading to reduced performance data processing. In this research, attempted the proposed model finds usage method to protect data by linear equation for encryption data, and decrease the complexity when retrieving data by Order-Preserving Scheme for indexing encrypted data, and take advantage of the features offered by the OPE in the way of keeping the data in the cloud database. In terms of maintaining the order of the data even though the data encryption features where the use of arrangement leads to the ease of dealing with the data encrypted in spite of, this feature provided by OPE in the way they work with encrypted data.

There are many general encryption techniques to encrypt the data before store data in the cloud database, but the problem (encryption tech.) is happened when searching over encryption data are taking more time to search, because the OPEs don’t know the operations like greater than, less than. Therefore, the OPEs encryption technique is using for preserving to enhance the performance of searching over data encrypted, but the problem of (OPEs) is have leak of information, to solve this problem, in the research the suggested solution is to add noise to the data that use the linear equations to increase security and performance.

1.4. MOTIVATION

The cloud computing is defined as the technology that prove its success and achievement by reduction in cost, easiness of use, flexibility in addition and associate new services in the work, the probability of altering the environment of work in a few hours and with low cost in compare to the traditional technology. There is a problem yet with the performance and the security, that is motivated utilizing the form of procedure in data encrypting, and the addition of noise to the data will be increased the ambiguity. different studies had been done to resolve the data encryption security, but what is the problem in data encrypting security still a connection of utilized the variables in linear equations, tending to easy extraction of jamming from the equations in the occurrence of the knowledge variables, this research altered the utilization of variables in the equation with change linear equation equivalent with more than one order does not interloper the breached data and obtain out the way also by using the encrypted data to keep the order of the data OPE Technology.

1.5. RESEARCH METHODOLOGY

In this study the work is launched depending on the problem declaration in the security due to the importance of data, where the intruder could be retrieved the data if know on the planned table that’s mean leakage of data, as well as to the complexity of enhanced performance if it is a slow performance processing. The suggested model scattered into two sides: the initial side is the client side of the secure database that is utilizing the process which is presented above in the data index encryption, where the second side is the cloud of storing the encrypted data, that added an extra parameter to promote the ambiguity in the equation that implemented by a second linear equation or maybe more than one linear equation with the growth of the parameter number to enhance ambiguity and security. The problem of this study is the addition of more parameters which are investigated the security but it is affected on the performance. Bring the Liu & Wang algorithm then add more forms of parameters and after that study the performance and shown the time window need to change schema based on hours, days is good because when we took every transaction or whenever the customer add new transactions. That's mean too many transactions leads to reduction.

Design and implementation phase

This thesis was showed a study on a range of linear equations also with increasing the number of variables utilized in the equation. Our program utilizes OPE algorithm in the data storage operation in the cloud database. Depending on the results come out of this study, it will be assessments by the following points:

- Take out the equation and the results of Liu and Wang.
- Compared with linear equations.
- Compared to the domain of the variables and what are the preferable range of variables numbers.
- Test time it takes to store data by using the new equation (re-indexing).

Evaluation Phase

We prepared three central experiments, every question in cloud database. We examined the performance for each question; we had varied also inputs to every question, as an example, the total amount of the stored data, the number of variables, the variables domain that utilized in the equation, in addition to the change in the equation.

1.6. CONTRIBUTION TO KNOWLEDGE

Afterward conducting this thesis has been accomplished to the results, when it sets to the former linear equation and the increased number of variables and equations utilized to increase the number to add up to the confusion of information,

- Identifying the effect of number of parameters on Liu & Wang formula
- Study every equation and record results.
- Identifying the time to change of each equation and the time of re-indexing in the cloud database.
- Identifying the speed and security level in the event of increasing the number of variables.

1.7. THESIS OUTLINE

Chapter One From this thesis is an introduction about the cloud computing and it is concepts in addition to the aims, objectives, problem statement, research motivations and the methodology that will be followed during the implementation of the proposed system.

Chapter Two Introduces some of the recent works that are related to the cloud computing, Order-Preserving Encryption, and the algorithms that use to investigate this research.

Chapter Three Examines the research methodology in details aided with all needed equations and flowcharts, also to investigate the model and algorithms of this study.

Chapter Four results that conclude by the three equations, and compare between them, then discussed these results to detect the best solution.

Chapter Five Introduces the conclusion for the whole work in addition to some key points suggested as future works to enhance the system performance.

Chapter Two:

Background

And

Literature Review

2. CHAPTER TWO: BACKGROUND AND LITERATURE REVIEW

2.1. OVERVIEW

This chapter will review the previous studies that have been achieved. Subjects that have been studied in this research including: the OPE algorithm and their utilizes in many areas, cloud database service, data using and linear equations and nonlinear equations, cloud computing benefits and the challenges faced it. Finally, review the software tools and the hardware tools which were used in this research.

2.2. BACKGROUND

In recent years, cloud computing has elevated a lot of benefits and a lot of firms are looking into cloud solutions for their IT requests. The security issues with the outsourced data could be resolved if the sensitive data are encrypted. Nonetheless, in numerous data-centric solicitations, it is essential to accomplish search on data objects to catch a set of data that satisfying the given criteria.

2.2.1 CLOUD COMPUTING DEPLOYMENT MODEL

Cloud computing is categorized into four major types of cloud deployment models. Such as: public, hybrid, private, and community clouds, as it shown below.

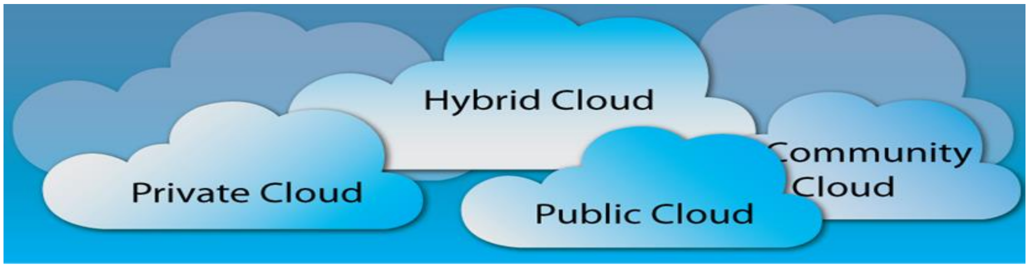


Figure 2:1 Types of cloud computing (Conway, G. 2012)

1. Public Cloud

A corporation offering the cloud facilities to the global population or to a massive industry assemblage owns the open cloud base, such as: Amazon Web Services (AWS) and Microsoft Azure. (Conway, G. 2012)

2. Community Cloud

The civilization of cloud outline is shared by several corporations and supports a specific society that has shared purposes, tasks, security necessities, policies, and compliance considerations, such as: Google Gov. (Conway, G. 2012)

3. Private Cloud

Private cloud organisation is possessed or rent out by a single society and exclusively run for that organization. Intel, Hewlett Packard (HP) and Microsoft have their own internal private clouds. (Conway, G. 2012)

4. Hybrid Cloud

Hybrid cloud technology contains of two or more clouds (public, community, or private) that keep on unique entities but are bounded together by a standardized or copyrighted technology that allows data or applications transportability. (Conway, G. 2012)

2.2.2 SOME OF THE ORDER-PRESERVING TECHNIQUE USES

Encryption is a capable method for securing classified information put away on an untrusted server, for example, in cloud computing. One of encoding secret information is that the information must be unscrambled for handling.one of real approach for figuring over scrambled information is to utilize encryption conspires that permit an untrusted server to execute particular calculation primitives over the figure writings. One of the normal operations is request correlation utilized for sorting, range checks, positioning, and so on. Request protecting encryption plans are utilized by numerous frameworks as a part of both exploration and industry to permit an untrusted server to perform request examination on cipher-texts. The (OPE) plan is a deterministic symmetric encryption conspires whose encryption calculation produces cipher-texts that save the numerical requesting of the plaintexts. Request saving encryption was presented by Agrawal et al. in 2004, and the main formal investigation of the idea and its security was performed by Boldyreva et al. in 2009. The base request safeguarding property required is to uncover no extra data about the plaintext values other than their request.

In this research facilitate the investigation of request safeguarding symmetric encryption (OPE), a primitive for permitting proficient reach inquiries on scrambled information, as of late started (from a cryptographic point of view) by Boldyreva et al. (Eurocrypt '09). To begin with, In this research address the open issue of describing what encryption by means of an arbitrary request protecting capacity (ROPF) spills about fundamental information (ROPF being the \ideal object" in the security definition, OF, fulfilled by their plan.) specifically, In this exploration demonstrate that, for a database of arbitrarily circulated plain messages and fitting decision of parameters, ROPF encryption releases neither the exact estimation of any plaintext nor the exact separation between any two of them. The research here presents valuable new procedures. Then again, in this research demonstrate that ROPF encryption releases inexact estimation of any plaintext and in addition rough separation between any two plaintexts, each to an exactness of about square foundation of the area size. In this exploration then study plots that are not arrange saving, but rather which in any case permit productive extent questions and accomplish security thoughts more grounded than POPF. In a setting where the whole database is known ahead of time of key-era (considered in a few earlier works), In this exploration demonstrate that late developments of \monotone insignificant flawless hash capacities" permit to proficiently accomplish (an adjustment of) the thought of IND-O (rdered) CPA additionally considered by Boldyreva et al., which asks that just the request relations among the plaintexts is spilled. At long last, In this research present particular request protecting encryption (MOPE), in which the plan of Boldyreva et al. is prepended with an irregular movement figure. MOPE enhances the security of OPE it might be said, as it doesn't release any data about plaintext area. In this exploration clear up that our work ought not be translated as saying the first plan of Boldyreva et al., or the variations that In this research present, are \secure" or \insecure." Rather, the objective of this line of exploration is to help specialists choose whether the alternatives give an appropriate security-usefulness tradeoff for a given application. (Boldyreva, A., et al. 2011)

A significant part of the estimation of cloud administrations lies in utilizing customer information, which frequently clashes with the customer's longing to keep that information private. Accommodating these opposing prerequisites is a critical research and designing issue, whose productive arrangement would have a sweeping business sway. Bland hypothetical methodologies, for example, completely homomorphic encryption, are wasteful. Specially appointed methodologies, for example, order preserving encryption (OPE), give answers for a restricted class of issues (e.g., assessing scrambled extent inquiries). Security accomplished in genuine frameworks, regardless of the possibility that a "perfect OPE" is utilized, is difficult to assess, and is regularly just fanciful, since the capacity to arrange ciphertexts may uncover a great deal about the basic plaintexts. They focus on a run of the mill utilization of OPE, encoded searchable webmail administration. They depict how the utilization of OPE in this setting may unveil data and talk about ways to deal with minimize its effect. The principle way to enhance security is as far as possible the kind of collaborations that ought to be permitted with a webmail server. (Kolesnikov,V. & Shikfa,A.,2012).

A many order preserving encryption (OPE) calculations have been produced in the writing to bolster seek on scrambled information. In any case, existing OPE plots just consider a solitary encryption key, which is infeasible for a down to framework with different clients (inferring that all clients ought to have the single encryption key keeping in mind the end goal to scramble or unscramble private information). In this paper, they build up the primary conventions, DOPE and OE-DOPE, to bolster the utilization of OPE in multi-client frameworks. To begin with, they present a gathering of key operators into the framework and create the DOPE convention to empower "appropriated encryption" to guarantee that the OPE encryption key is not known by any substance in the framework. Notwithstanding, in DOPE, if a key specialists is traded off, the offer of the mystery information that is sent to this key operators is bargained. To take care of the issue, they built up a novel unmindful encryption (OE) convention in view of the neglectful exchange idea to convey and scramble the shares mindlessly. At that point, they incorporate it with DOPE to get the OEDOPE convention. Security of OE-DOPE is further upgraded with extra strategies. Both DOPE and OE-DOPE can be utilized with any current OPE calculations while holding all the benefits of OPE without requiring the clients to share the single encryption key, making the OPE approach attainable in reasonable frameworks. (Xiao, L., et al. 2012)

Semantic-security of individual bits under a ciphertext is principal thought in advanced cryptography. In this work they show the principal results about this central issue for Order-Preserving Encryption (OPE): "what plaintext data can be semantically covered up by OPE scramble particles?" While OPE has increased much consideration lately because of its value in secure databases, any incomplete plaintext lack of definition (semantic security) result for it was open. Here, they propose another indistinctness based security idea for OPE, which can guarantee mystery of lower bits of a plaintext (under basically an arbitrary ciphertext examining setting). They then propose another plan fulfilling this security idea (while prior plans don't fulfill it!). They take note of that the known security thoughts let us know nothing about the above halfway plaintext lack of definition since they are restricted to being restricted based. Likewise, they demonstrate that our security idea with particular parameters suggests the known security thought called WOW, and further, our plan accomplishes WOW with preferred parameters over before plans. (Malkin, T., et al. 2013)

2.2.3 OVERVIEW DATABASE WITH CLOUD COMPUTING

Cloud computing is well-thought-out to be an ordinary development of network and usefulness computing. It supports in cooperation network and utility computing with further features for instance accessibility, scalability, flexibility, and reliability. This study will centre on one of the significant services in the cloud computing which is the database organization system in the cloud. (Gadichal, A., B., 2011)

The cloud database organization system is a dispersed database that transports computing as a service as an alternative of a product, it is a distribution resource; software and info among multiply devices over a network that is commonly the internet. It's as well an essential and crucial element in most computing environment nowadays, and their significance is improbable to reduce with the advent of the hosted cloud computing and storing. (Garzon, J., 2006)

A database is an assortment of data that is systematized so it may simply be get into, achieved and updated to information. In one vision, databases could be categorized rendering to sorts of contented: full-text, bibliographic, numeric, and images. A Database Management System (DBMS) is a group of programs that permits employers to generate and keep up a database which easiness the usage of the meaningful information. Affording to the ANSI/SPARC DBMS Report (1977), DBMS architecture must be built as a multi-layered system. (Robbins, R., 1994)

Database-as-a-Service (DaaS) is a facility that is achieved by the cloud manager (open or private) that assist applications, devoid of the application developing group “binding for traditional “ database organization function. With a DaaS, the application engineers possibly will not require to be database experts, nor the purpose to diminish a database manager or Database Administrator (DBA) to stay beside the database. This will be accomplished DaaS true tranquillity when application developers can simply call the database service and procedure the data devoid of even having to check the database. This accomplish that the database can process data so as to be maintained , promoted, backed up and allocated with the server fails, all deprived of affecting the developer in any way. From the designer's point of view, this is the sense of DaaS. (Mykletun, E& Tsudik, G., 2006)

Database security is an increasing worry verified by an upsurge number of reported instances of damage or illegal experience to the sensitive info. As the volume of data collected, booked and shared automatically enlarges, consequently does the necessity to realize the security of the database. The Defence Information Systems Agency of the US Department of Defense (2004), in its database security mechanical employment leader, statuses that the database security have to offer controlled, and secure right of entry to the contents of the database as well as to domain the honesty, constancy. (Baeten, Y., Nijs, N., 2012)

Seeking across over the encrypted data is hard, which a lot of researchers emphasis in this topic to solve this problematic and challenge, the obscurity and the damage of some of the info or not protection order-preserving in the database, the challenge currently is to discover a particular algorithms so as to permit the examination of the database while its data are being encrypted devoid of decryption. In the literature there are a lot of solutions; one of them is called cryptDB generated by a crew of researchers at MIT work on that the key idea is they put the encrypted data under trusted part whenever they need to know greater than or less than they send request to the third part and they tell this is less or greater than. The provider will not know the real data but the problematic of this solution there is several transactions among provider and trusted part. Other solution is to have encryption procedure that conserves the order. The OPEs solve the problem can do the processes but the confidence is escape of information since if the attackers listening they can see the information statistically to solve this problem Liu, & Wang adding the noise to the data. (Liu, D. & Wang, S., 2012)

2.2.4 HOMOMORPHIC CRYPTOSYSTEMS

The encryption effectiveness is very significant in the data security. There were numerous of encryption schemes, but it dissimilar from scheme to others. In this model, utilized symmetric form for provided that encryption efficiency of which the homomorphic schemes, if the encryption scheme, the homomorphic could be worry to offensive on this base, where it treated accurately homomorphism may also be applied to achieve the processing data safely. The homomorphic scheme was interested in the processing over the encrypted data, including what homomorphic, and categorized into two sorts are called Fully Homomorphic Encryption (FHE) and Partially Homomorphic Encryption (PHE). Homomorphic is a description that defines a particular property of the encryption scheme. That property, at an abstract level could be defined as the capability of achieving computations on the cipher text without decrypting it or even to know the keys. (Barkerski, Z., et al, 2011)

2.2.5 OPES (ORDER PRESERVING ENCRYPTION SCHEME)

In this section, discussed the encryption necessity to talk about the OPES (Order Preserving Encryption Scheme) the OPES can processing and preserve the data, without decrypting the operands. That’s mean applying the operations MAX, MIN, and COUNT on the data without decrypting it. Consequently, GROUP BY and ORDER BY operations can utilize the operations on the data without decrypting the data. Just when using SUM or AVG should be decrypt data. (Agrawal, R. et al., 2009)

Order-preserving symmetric encryption (OPE) is considered as a deterministic encryption system that’s the encryption function have a numerical arranging of the plain texts. OPE has an extended history in the type of the one-part codes, that are lists of the plain text and corresponding of the cipher texts, both coordinated in an alphabetical or a numerical set so only a monocular copy is in demand for an effective encryption and decryption. OPE does not only allow effective range queries, but also allow the indexing and the query processing to have been done rightly and as efficiently as for the unencrypted data, due to a query just consists of encryptions and servers that can set the wanted cipher texts in the logarithmic time via a standard tree-based data temple. Actually, following to its publication, has been indicated widely in the database society, and has been also proposed for use in in-network aggregation on the encrypted data in the sensor networks and as a tool to apply the signal processing mechanisms to the multimedia content protection. (Agrawal, R. et al., 2009)

2.2.6 CLOUD COMPUTING BENEFITS

Innovativeness would require make even their applications, consequently as to contribute the architecture replicas that Cloud Computing proposals. Some of the characteristic benefits are listed below:

1) Reduced Cost

Here are a number of whys and wherefores to attribute the cloud computing technology with minor costs. The promoting model is fee as per practice; infrastructure is not bought thus let down repairs. Initial expenditure and periodic expenses are greatly minor than the traditional computing. (Codd, E., F., 1972)

2) Increased Storage

Through the gigantic Infrastructure that is accessible by the cloud providers nowadays, storing and maintenance of great volumes of info is an authenticity. Unanticipated workload spikes are similarly accomplished effectively and efficiently, meanwhile cloud computing may be scaled animatedly. (Codd, E., F., 1972)

3) Flexibility

This is an enormously significant distinctive. With originalities having to become accustomed, even more quickly, to change the commercial conditions, rapidity to carry is serious issue. Cloud computing exertions are getting requests to the market very speedily, by utilizing the most suitable building blocks essential for deployment. (Codd, E., F., 1972)

2.2.7 CLOUD COMPUTING CHALLENGES

Notwithstanding its rising influence, worries concerning cloud computing still continue. In the estimations, the welfares are more important than the drawbacks and the model is assets exploring. Some public challenges are

- Data Protection

Data Safety is a critical component that licenses scrutiny. Originalities are unwilling to buy a guarantee of commercial data safety from sellers.. (Khachatryan, V., et al., 2010)

- Data Recovery and Availability

All commercial applications have provision level of agreements that are harshly followed. Operative teams act a key character in administration of service level contracts and runtime domination of applications.. (Khachatryan, V., et al., 2010)

- Management Capabilities

In spite of there being numerous cloud providers, the administration of platform and infrastructure is still in its early stages. Features like, Auto-scaling‟ as an example, is a critical necessity for a lot of enterprises. (Khachatryan, V., et al., 2010)

- Regulatory and Compliance Restrictions

In certain European kingdoms, government guidelines do not let customers private data and other sensitive data to be essentially located outside the state or country. (Khachatryan, V., et al., 2010)

With the cloud computing, the achievement variations to the interface that is, to the interface among the service suppliers and the numerous sets of service clients. (Khachatryan, V., et al., 2010)

2.3. LITERATURE REVIEW

Various researchers are offered a lot of ideas and key problems in the cloud computing. The literature review offers to our issue as listed below:

(Popa, R., 2011) emphasis on the protection of three layers must be protected physical security, operating system security and DBMS security, But this is not enough protection, data encryption proposed in the database, Security requirements must be high speed and detect unauthorized modifications. Each row has a different encryption key, and the encryption key is also survey opinion indicates that development and strength are features of encryption database are available among academic and business community. Furthermore, customer's reliance is different because of the work boundaries like the cost of publication and public expenditure. So as to introduce these features and depend on it widely as it was mentioned database encryption, it must be given the best research. (Popa, R., 2011)

(Hore, B., & et al) the achieving of Bucketization Technique which is reinforces privacy. The key trade between privacy and performance has been highlighted by introducing some scenarios to deduce and disclosure (the United nation may have interest in any enemy in the first level that has reliable services). Two measures were suggested for the privacy. Similar algorithms were suggested to divide data which reduces the general expenses provably, it also reduces performance‘s expenses in query treatment. They introduced algorithm for deployment of control which allows the owner of the Bucketization data to achieve the required level of data privacy (Query evaluation) by measuring a small amount. The algorithms that they introduced have been checked, and the result that shows both the artificial and real groups. (Hore, B., & et al. 2004)

(Shmueli, E., & et al, 2005) outlined the difficulties they had when designing the security index for the encrypted database. It has been determined what the challenges were they faced when designing the security index for the encrypted database. These challenges include: preventing information store, unauthorized disclosure modify, maintaining the structure of the index, and supporting the control to reach access control. The performance is not dramatically affected by time and storage, while the design considerations and storage encryption keys have been discussed, they suggested several alternatives for the issues they faced. A secure encryption for the database index has been suggested for values in one level. Performance and structure of work are simply obtained by using one of the encrypted values. Value's compilation are unrealistic to prevent spreading information and to allow unauthorized modify. Finally, to support the control of access direction in the multiuser environment, they suggested dividing the index into several sub-indexes where each sub-indexes in the encrypted column is connected to the value using the same key. (Shmueli, E., & et al. 2005)

(Kuzu, M., & et al, 2012) proposed a symmetric encryption and similarities efficient system model. They used a sensitive retail that used widely to look for similarities rapidly in space. The proposed safe LSH index and search plan to enable the rapid search for similarities in the context of the encrypted data, it is very important not to sacrifice the confidentiality of sensitive information when it supports the functionality. This study provided the definition of security proves the security of the proposed scheme in the context of the definition to ensure confidentiality. To illustrate the characteristics of the proposed plan, they have applied the application of the real world; the error in the keyword search has been realized. This application enables to search for keywords in which typographical errors in both queries and data sources. (Kuzu, M., & et al. 2012)

(Shamir, A., 1979) formulating and solving the problem to support ambiguity research and privacy to accomplish effective use of the encrypted data stored in the cloud computing was made. This study has been designed two advanced technologies (i.e. based on a wild card and techniques based on grams) for the construction of the ambiguity word groups and stored efficiently, taking into account the distance between words. On the basis of vague word groups, they suggested more brand new based coding scheme to try to pass the search, a number of ways from the tree structure was built symbols used for the transfer of the results of the ambiguity group of words. Through rigorous security analysis, they showed that the solution they have proposed is a safe and maintains privacy, while achieving the goal of keyword research correctly ambiguity. Experimental results demonstrate the efficiency of a wide rendered the solution they have proposed. They also continued work, they will continue the search for security mechanisms that support the semantics research that takes into account along primarily ambiguity words, a series of keywords, and even the semantics of complex natural language to produce relevant search very strong results. (Shamir, A., 1979)

(Liu, D., & Wang, S, 2012) suggested a technique in order to preserve indicators to facilitate inquiries on encrypted databases on a wide range. They have simple indexing to use because it is depending on a linear expressions. The plain linear indexing appearance is the information-theoretically protected meanwhile; every index is added with certain random noise. They gave judgment about controlling the amount of noise in order to allow random indicators to maintain order, they planned to put in the chart is programmable, and this means that the plain indexing terms can be collected together to advance the robustness of the indexing software and hide the distribution of the input values of the indexes. Shared how to apply the indexing system to query in encrypted databases through translation query, and carried out the first model to prove the work and their joining. (Liu, D., & Wang, S. 2012)

(Liu, D., & Wang, S. 2013) On cloud computing the database services are appearing like an attractive method of the database outsourcing. When a database is diffused on the cloud computing database service, the data privacy and security turns in to a huge worry for the users. A simple method to heading this worry is to encrypt the database. So, after encryption, the database cannot be easily impeached. In this paper, they proposed the nonlinear order preserving structure for the indexing encrypted information, which simplifies the range queries in excess of the encrypted databases. The structure is safe even there are a great number of the duplicates in the plain texts. Furthermore, their structure allowed the programmability of the basic indexing vocabularies and as a result provided the ability of beating the distribution of the plain texts from the indexes distribution. This structure was appropriate for the long-standing databases since its used did not require any supposition on the characteristics of database data, for example their scattering, range and number, which may possibly to change dramatically over the time. In this paper, the suggested structure addressed the vulnerability of the obtainable linear indexing structure and did not the leak of the information of secrets in the indexing vocabularies. This structure was programmable, sense that the basic indexing vocabularies may be collected together to advance the robustness of the indexing databases and hide the distribution of input values. This structure did not require the range of the input values and their number, and the distribution modelling before the indexing database. They presented how to apply the indexing structure to query encrypted databases by the query translation. A trial product was applied to prove their system, and the trial product performance was evaluated also. (Liu, D., & Wang, S, 2013)

(Baeten, Y., et al, 2012) order-preserving encryption permits carrying out a lot of classes of queries – as well as range queries – on encrypted databases. In recent times offered an ideal-secure order-preserving encryption or what called the encoding scheme, but the cost of supplements (encryption) is too high. This study presents an also ideal-secure, nonetheless meaningfully extra effective order preserving encryption system. The structure they did was enthused by Reed's referenced worked on the usual height of random double search trees. This structure also takes part proficiently with adaptable encryption as utilized in CryptDB. In this trials for database supplements accomplished the performance growth of up to 81% in LANs and 95% in WAN's. (Baeten, Y., et al, 2012)

(Boldyreva et al., 2015) the order-preserving encryption (OPE) schemes, whose cipher texts protect the usual ordering of the plain texts, let well-organized range query handing out over the outsourced encrypted databases devoid of the giving server admission to the decryption key. Schemes have lately received improved interest in both of the database and the cryptographic community. Especially modular order-preserving encryption (MOPE) , is a talented extension which increases the security of the basic OPE by introduce a secret modular offset to each data value former to the encrypting it. Nevertheless, execute range queries via MOPE in a na¨ıve way gives the permission to the adversary to learn this offset, opposing to any potential security gains of this approach. They systematically address the vulnerability and show that the MOPE can be used to build a practical system for executing range queries on encrypted data while providing a significant security improvement over the basic OPE. They design a system prototype that integrates our schemes on top of an existing database system and apply query optimization methods to execute SQL queries with range predicates efficiently. We provide a performance evaluation of our prototype under a number of different database and query distributions, using both synthetic and real datasets.

(Boldyreva, A., 2009) outlined the improvement of the third-party hosting, IT outsourcing, service clouds, etc. increases significant security worries. It would be harmless to encrypt serious data hosted by the third-parity, but then meanwhile, the database must be able to procedure queries on the encrypted data. A lot of research works have been advanced to provision the search query processing on the encrypted data, counting the order preserving encryption (OPE) structures. Security investigation acts a significant role on secure algorithm design. It can help understand the level of security assurance of the algorithm. (Boldyreva, A., 2009)

(Popa, R., et al, 2011) the databases cover most valued private, financial, and government data. They are the most wanted to the horrible challengers and so, it is very serious to keep in contradiction of all probable adversarial actions. With the new quick growth in the obtainability and popularity of the cloud services, a lot of individual, business, and government data are currently moving to the cloud. Consequently, databases are extra problematic to keep safe for the reason that new security and privacy matters. Numerous actions have been proposed to resolve the outsourcing database situations which reserve a particular degree of the confidentiality while still allow to perform some SQL queries professionally. CryptDB is a resent database organisation system to protect the data confidentiality while conserving the confidentiality and the performing a typical set of SQL queries in an effective way. CryptDB give the impression to be practical associated to other efforts at resolving the problematic of computing with the encrypted info and the database may be completely moved to the cloud without any security worry because all the information are previously encrypted and never exposed to the database administrator. In this paper, CryptDB is re-entered from cryptographic point of view. (Popa, R, et al, 2011)

2.4. SOFTWARE TOOLS USED IN THIS RESEARCH

- Visual Basic 2010
- SQL Server 2010
- OPE Algorithm

- Linear Equations

2.5. HARDWARE TOOLS USED IN THIS RESEARCH

In this study, the performance was evaluated utilizing a laptop computer parts shown in response such as processor and memory. Hardware will be used in the experiments is one Lenovo IdeaPad S510p laptop with the following specifications:

- (Processor): Intel® CPU 2.40 GHz (7 CPUs).

- (Memory): 8 GB RAM.

Chapter Three:

Methodology

3. CHAPTER 3: RESEARCH METHODOLOGY

3.1. INTRODUCTION

In this chapter, an experiment will be designed to serve the objectives of this research to get the suitable solution of problem, the study of the proposed solutions throughout the designed experiment to test the performance of each equation, additionally to test the existing variables in each equation based on the design experiment that is depends on the foundations of the following:

- Group multiple experiments to see the performance of each equation.
- Group multiple experiments to see the performance of each variable and its impact in the equation.
- Study time takes to change the linear equations.

3.2. PROGRAM DESIGN

The program have been designed to work on testing the performance of linear equations, calculating the time needed to change the equation, evaluating different ranges of numbers for different variables.

3.2.1 BUILDING PROGRAM

The program has been built using (Visual Basic) where it is divided into two parts; the first one is the cloud database and second one is the user application.

Cloud Database: where used the SQL Server Database and then it was added to the Northwind Database so it is applied the idea of Liu and Wang which is the theorem have to be applied in the search.

- User Application: where it is divided into two parts; the first one is the screen that appears to the user to deal with it by applying the query where (modify, delete, search data & retrieval) of the data, and the second one which isn't apparent to the user, where the implementation of the query user data is done to address in addition to the data of noise before being sent to the cloud database based on the linear equation imposed by Liu and Wang, as shown in the following example:

They using (f (x) = a ∗ v + b + noise) linear expression, a & b are variables used in the equation to get out the noise after saving data, the v= the index number, noise taking randomly from the range of numbers, the range = {equation v1 to equation v1+1), for example:

Schema	A	B
	4	9

Index 1 = 1

Index 2 = 2

Index 3 = 3

Index 1 = a ∗ v + b + noise "noise = 4*1+9 = 13,

noise = 4*2+9 = 17"

4*1+ 9 + 15 Range of noise = {,13 14, 15, 16, 17}

Index 1 = 28

Index 1 in enterprise = index 28 in cloud computing

The main problem of this technique is schema fixed and does not change with transaction or time. Where the application performs the equation as in the example above, on the data to be sent to the Cloud Database to store and add them the noise through compensation wildcard character (A) and (B) random as it is located in the schema, and compensation character (v) where it is the index number supposed to be in the database, either noise are extracted from a particular range where it is the beginning range of the equation result with compensation to the first index number, where the end range is the equation result with compensation to the second index number, when the range is completed the noise are chosen randomly from this range as shown in the example above.

3.2.2 USER PROGRAM

The user program is divided into three screens; the first screen is to add data, the second screen is to add data with the data stored in database and the replacement of noise data stored in database then adds the new data, the third screen is to delete the stored data.

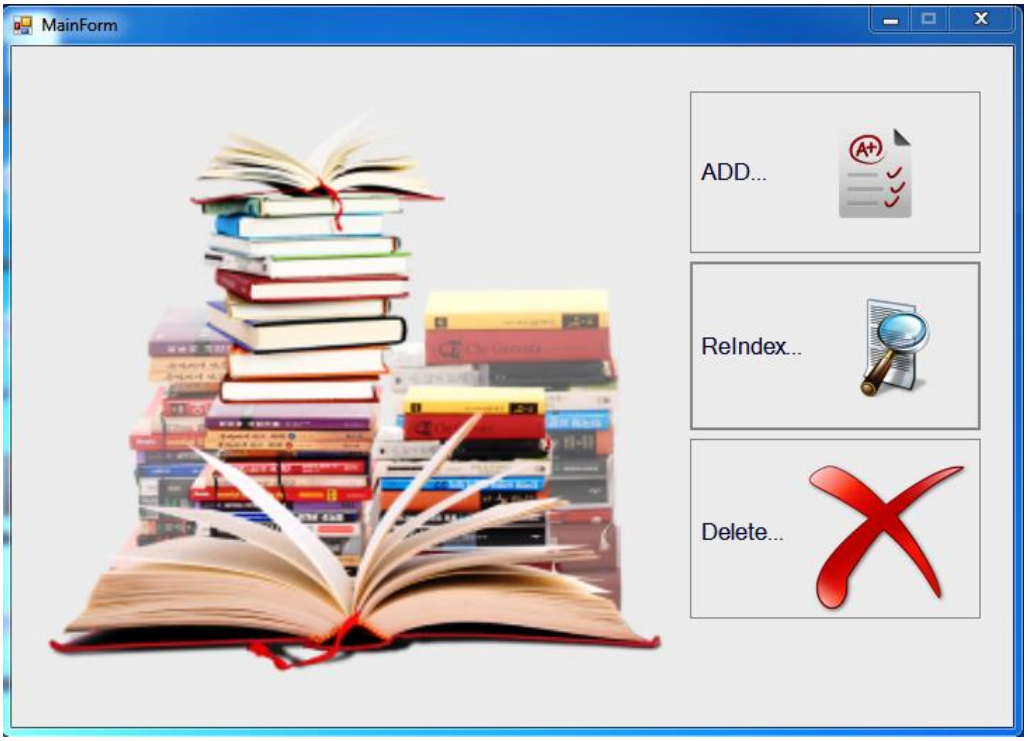
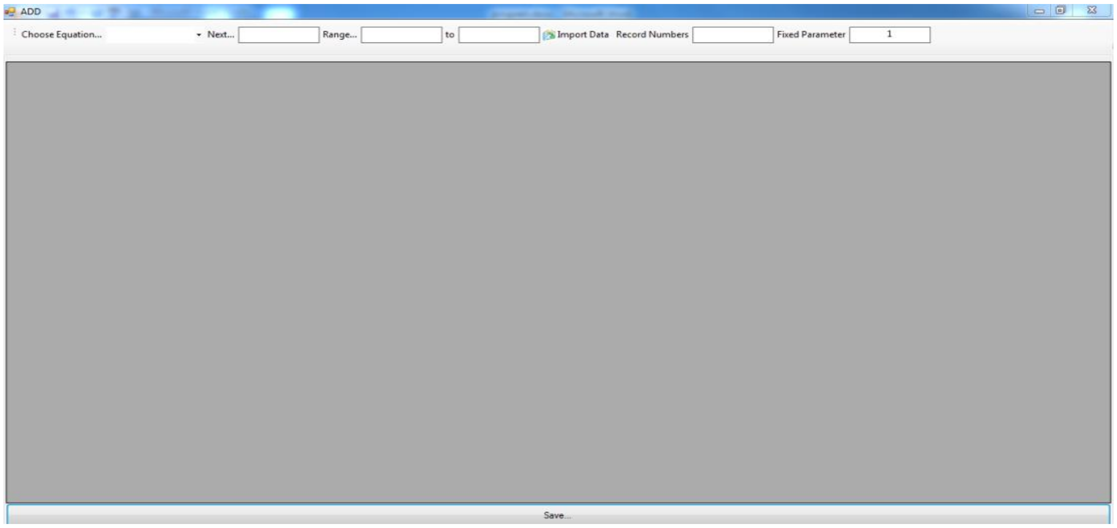


Figure 3:1 User program main form

1. First Screen: Add data

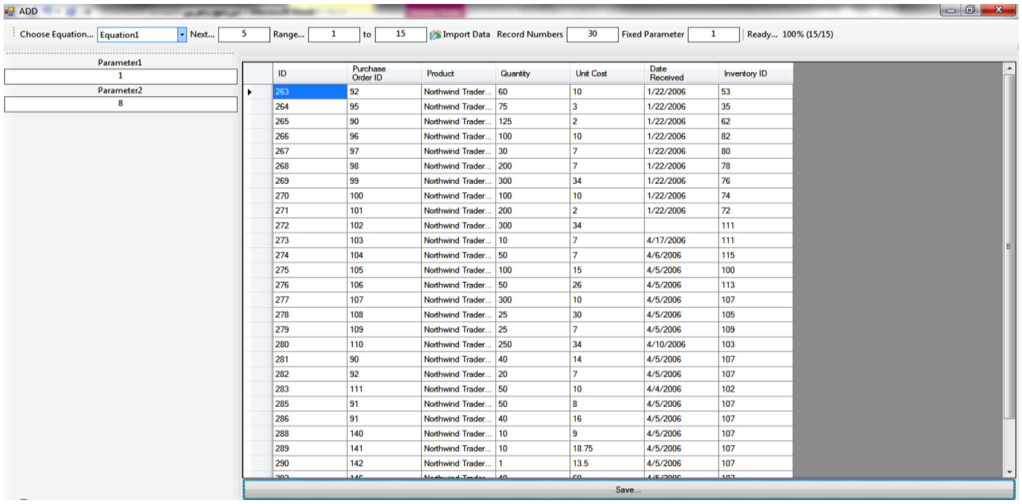
The add data screen consists of the first box to choose the equation for example equation one or equivalent of two equations or equivalent three equations, each equation needs to have a different number of variables, when choosing the equation number of boxes have to opened with equivalent to the number of variables that is needed to each equation, for example, equation number 1 need two variables, the program will be opened two boxes, where in the second box placed the number of hops for the variable 1; for example if we put number 5 the first variable will be number 5 and then changes to 10 and so on.

The third and fourth boxes are the determinants of the variables as the beginning and the end, the fifth box which is the number of registrations requesting stored in the database, there is a restore button to import data from the database and display it, after pressing the save button the data will be saved in the cloud database with change the index original number to the new index number, and then repeat the process with changing the number of the first variable as much as the number in the second box, and so the process repeated until it reaches the last number (the number specified in the fourth box).



Fixed Parameter 1

Figure 3:2 Add data screen



Choose Equation... Equation1 Next... 5 Range... 1 to 15 Record Numbers 30 Fixed Parameter 1 Ready... 100% (15/15)

Parameter1: 1

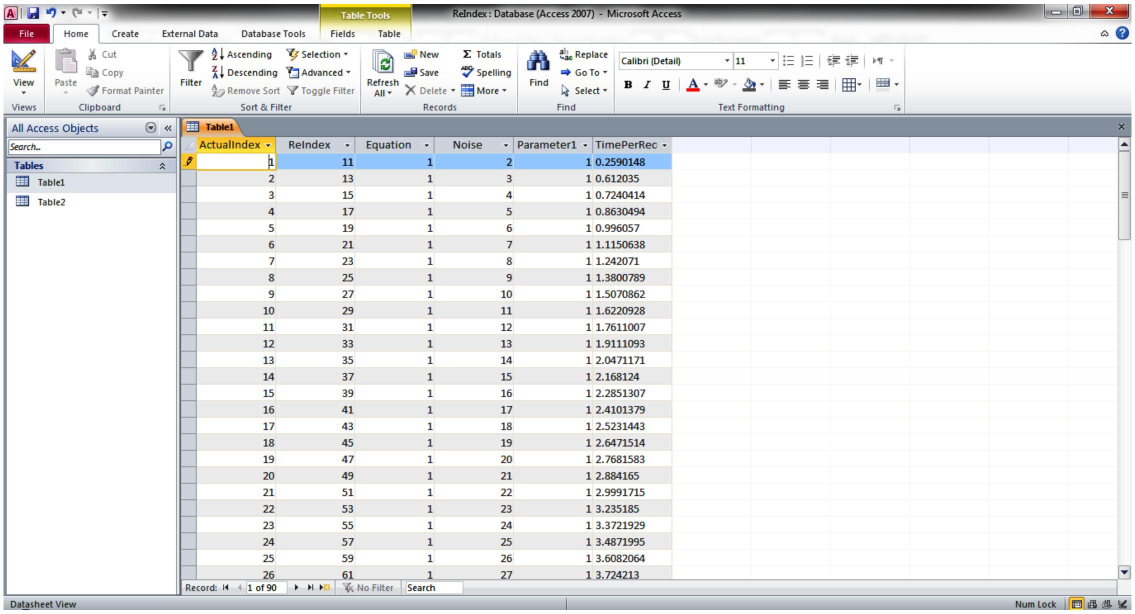
Parameter2: 8

ID	Purchase Order ID	Product	Quantity	Unit Cost	Date Received	Inventory ID
263	92	Northwind Trader...	60	10	1/22/2006	53
264	95	Northwind Trader...	75	3	1/22/2006	35
265	90	Northwind Trader...	125	2	1/22/2006	62
266	96	Northwind Trader...	100	10	1/22/2006	82
267	97	Northwind Trader...	30	7	1/22/2006	80
268	98	Northwind Trader...	200	7	1/22/2006	78
269	99	Northwind Trader...	300	34	1/22/2006	76
270	100	Northwind Trader...	100	10	1/22/2006	74
271	101	Northwind Trader...	200	2	1/22/2006	72
272	102	Northwind Trader...	300	34		111
273	103	Northwind Trader...	10	7	4/17/2006	111
274	104	Northwind Trader...	50	7	4/6/2006	115
275	105	Northwind Trader...	100	15	4/5/2006	100
276	106	Northwind Trader...	50	26	4/5/2006	113
277	107	Northwind Trader...	300	10	4/5/2006	107
278	108	Northwind Trader...	25	30	4/5/2006	105
279	109	Northwind Trader...	25	7	4/5/2006	109
280	110	Northwind Trader...	250	34	4/10/2006	103
281	90	Northwind Trader...	40	14	4/5/2006	107
282	92	Northwind Trader...	20	7	4/5/2006	107
283	111	Northwind Trader...	50	10	4/4/2006	102
285	91	Northwind Trader...	50	8	4/5/2006	107
286	91	Northwind Trader...	40	16	4/5/2006	107
288	140	Northwind Trader...	10	9	4/5/2006	107
289	141	Northwind Trader...	10	18.75	4/5/2006	107
290	142	Northwind Trader...	1	13.5	4/5/2006	107

Figure 3:3 Data set added

Upon completion of the of the data saving, the program will be stored the results in ACCESS file, where it is consist of three sheets where in the first sheet is table 1, table 2 in the second sheet, and table 3 on the third sheet .

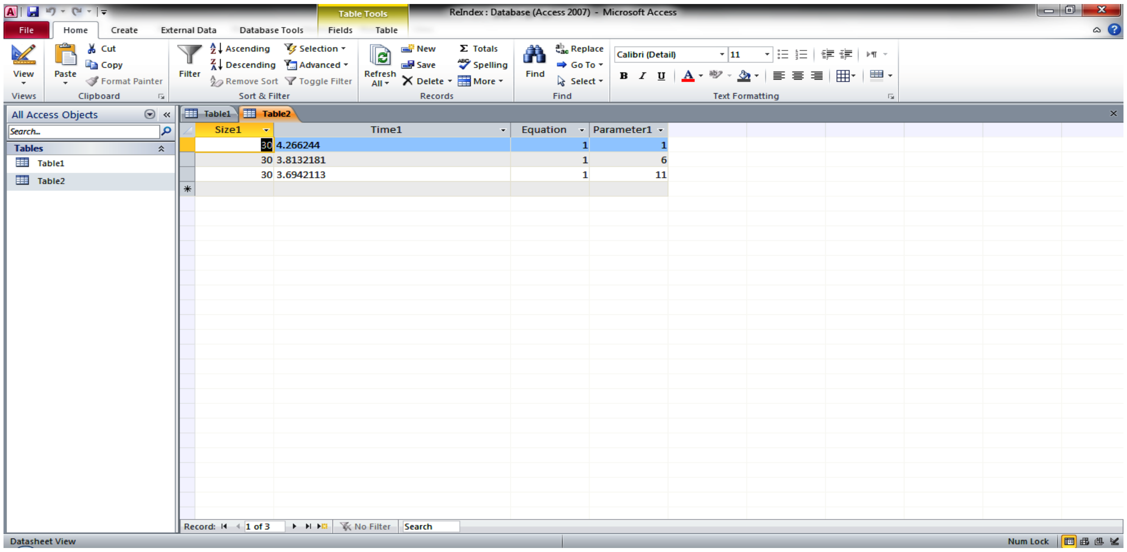
Table one consist of six columns, the first column is composed index original number before re-encrypted, the second column is the number of index after the addition of noise, the third column is the number of the equation, the fourth column is the amount of noise, the fifth column is value of the first variable, the sixth column is the time takes to save the first group of data.



ActualIndex	ReIndex	Equation	Noise	Parameter1	TimePerRec
1	11	1	2	1	0.2590148
2	13	1	3	1	0.612035
3	15	1	4	1	0.7240414
4	17	1	5	1	0.8630494
5	19	1	6	1	0.996057
6	21	1	7	1	1.1150638
7	23	1	8	1	1.242071
8	25	1	9	1	1.3800789
9	27	1	10	1	1.5070862
10	29	1	11	1	1.6220928
11	31	1	12	1	1.7611007
12	33	1	13	1	1.9111093
13	35	1	14	1	2.0471171
14	37	1	15	1	2.168124
15	39	1	16	1	2.2851307
16	41	1	17	1	2.4101379
17	43	1	18	1	2.5231443
18	45	1	19	1	2.6471514
19	47	1	20	1	2.7681583
20	49	1	21	1	2.884165
21	51	1	22	1	2.9991715
22	53	1	23	1	3.235185
23	55	1	24	1	3.3721929
24	57	1	25	1	3.4871995
25	59	1	26	1	3.6082064
26	61	1	27	1	3.724213

Figure 3:4 First result table

Table two consist of four columns, the first column is the number of registrations which are stored in the database, the second column is the time it takes to store the recordings in the database, the third column is the equation number used to save the recordings in the database, and the fourth column is the value of the used variable in the equation.



Size1	Time1	Equation	Parameter1
30	4.266244	1	1
30	3.8132181	1	6
30	3.6942113	1	11

Figure 3:5 Second result table

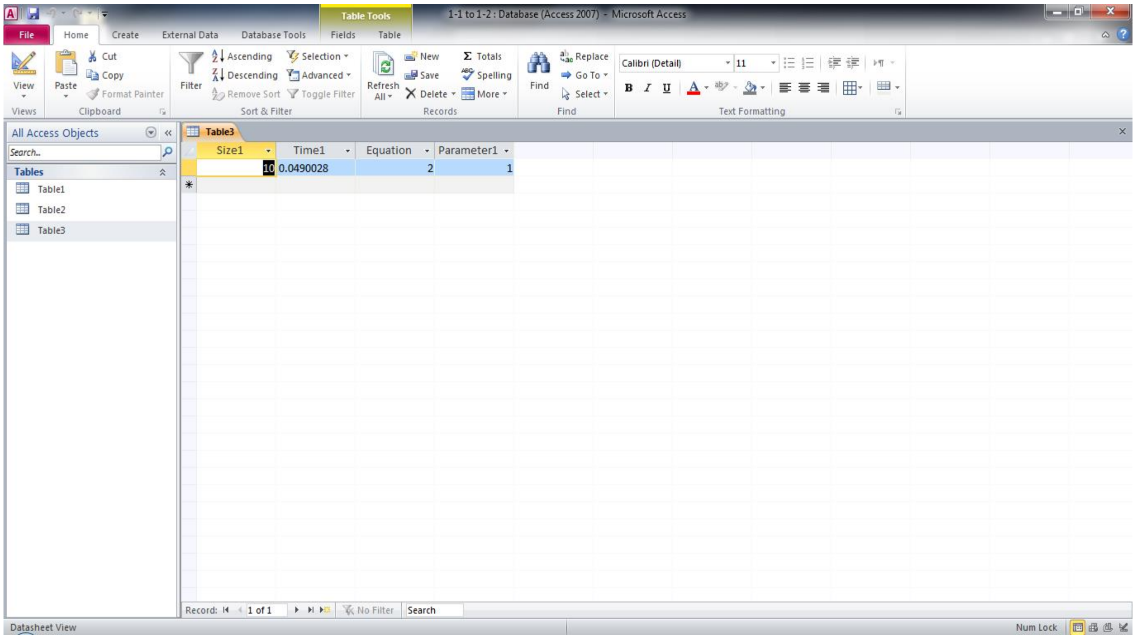


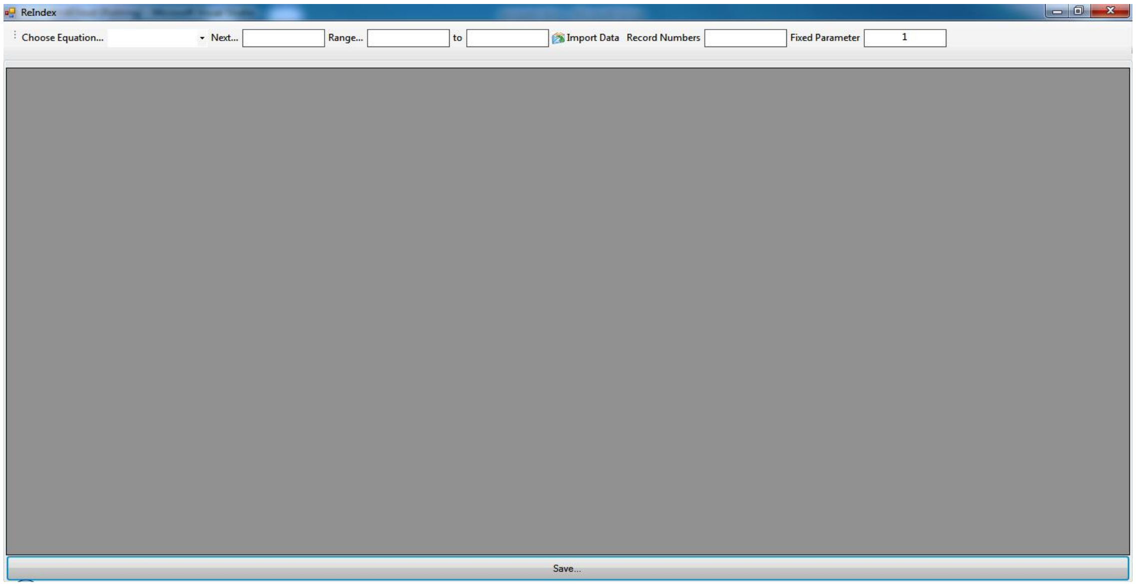
Table3

Size1	Time1	Equation	Parameter1
10	0.0490028	2	1

Figure 3:6 Third result table

Table number three contained the time needed to change from equation to another, which is depend on the number of records that received previously on the data base.

2. Second screen: Add data to the data previously stored



Fixed Parameter 1

Figure 3:7 Add data to the data previously stored screen

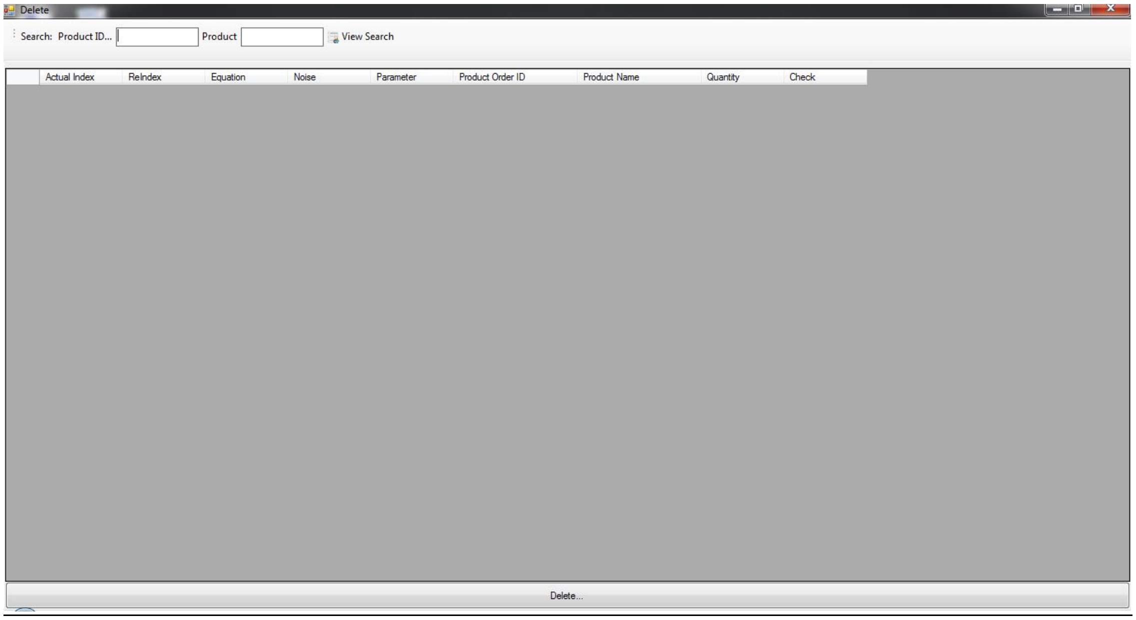
As mentioned in the first screen; the add data screen consists of the first box to choose the equation for example equation one or equivalent of two equations or equivalent three equations, each equation needs to have a different number of variables, when choosing the equation number of boxes have to opened with equivalent to the number of variables that is needed to each equation, for example, equation number 1 need two variables, the program will be opened two boxes, where in the second box placed the number of hops for the variable 1; for example if we put number 5 the first variable will be number 5 and then changes to 10 and so on.

The third and fourth boxes are the determinants of the variables as the beginning and the end, the fifth box which is the number of registrations requesting stored in the database, there is a restore button to import data from the database and display it, after pressing the save button the data will be saved in the cloud database with change the index original number to the new index number, and then repeat the process with changing the number of the first variable as much as the number in the second box, and so the process repeated until it reaches the last number (the number specified in the fourth box).

The difference between the first screen add data and second screen add data on the data already stored, the second screen is working on checking the equation if the required equation to store a new data is the same as the equation that used in the old data storage, the second screen does not make any thing only the process of adding the new data. If the required equation need to be stored data is differ from the equation which previously used in this case it is necessary to retrieve old data stored and re-using the equation selected by the user. The aim of the second screen is added data on the data previously stored to calculate the time it takes to change the equation to be able to choose the right time to change it.

3. Third screen: delete stored data

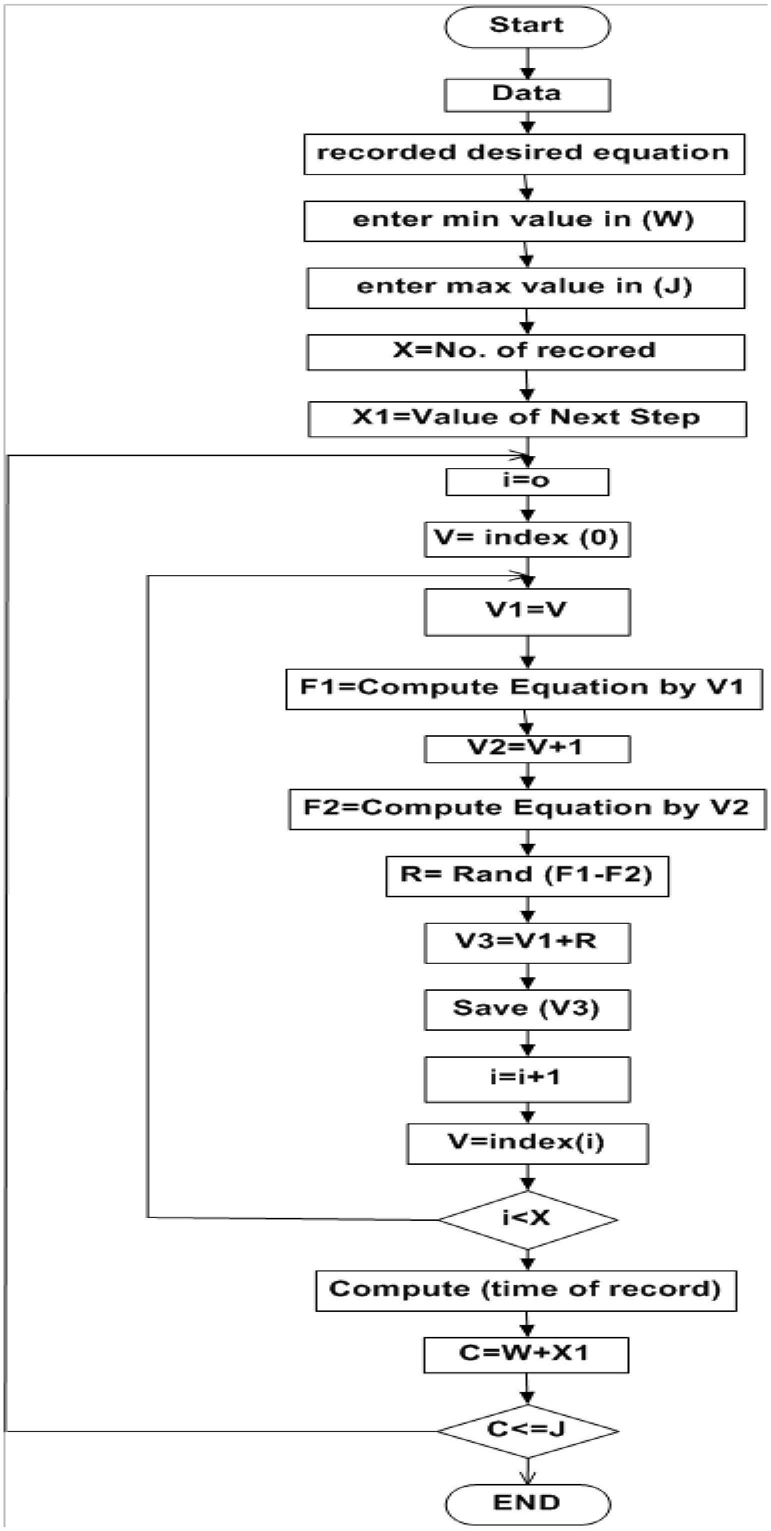
The third screen of the programme is used to delete the data was saved from the previous equation.

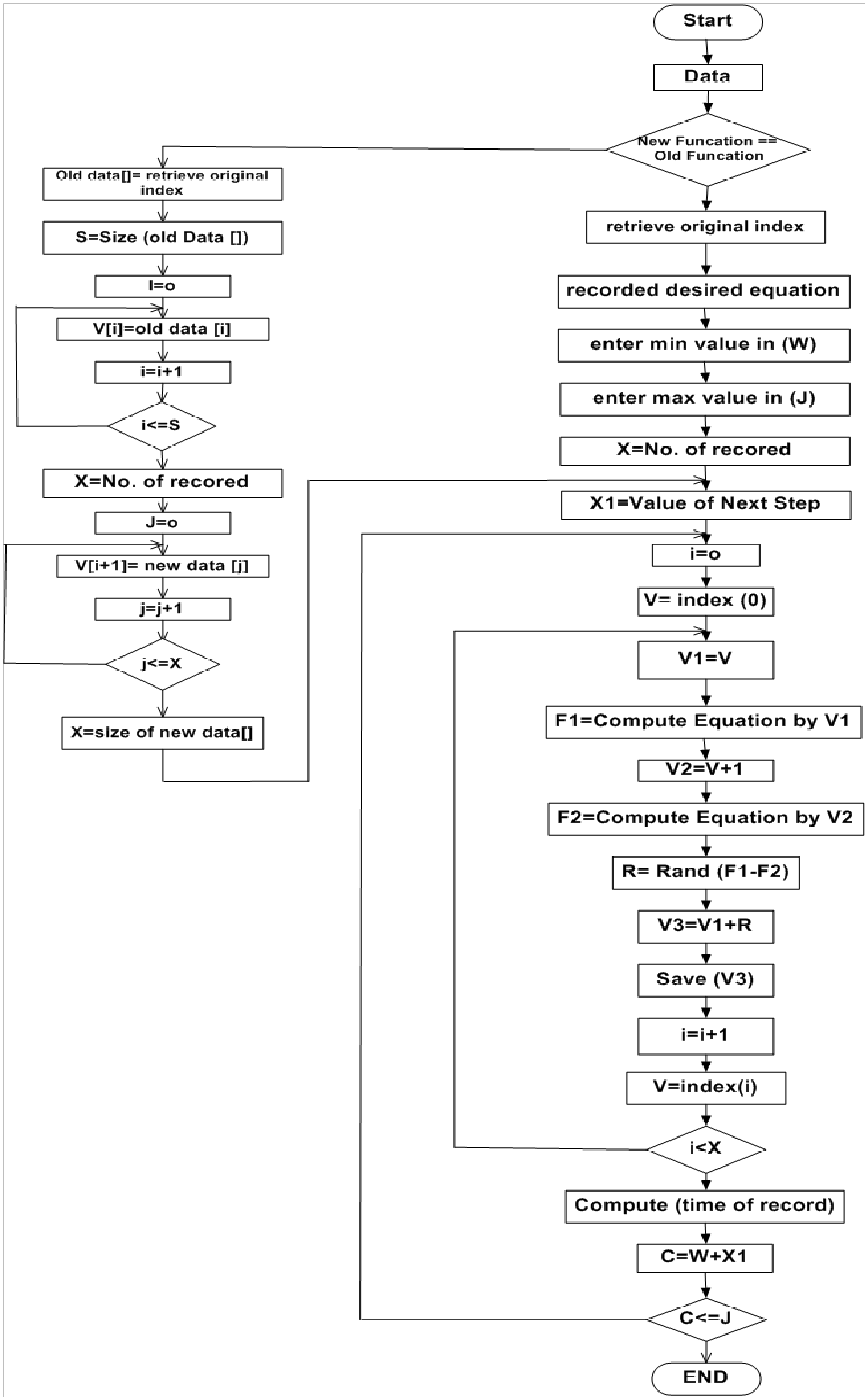


	Actual Index	ReIndex	Equation	Noise	Parameter	Product Order ID	Product Name	Quantity	Check

Figure 3.8 Delete stored screen

3.2.3 PROGRAM FLOWCHART




Start
Data
New Funcation == Old Funcation
Old data[]= retrieve original index
S=Size (old Data [])
I=o
V[i]=old data [i]
i=i+1
i<=S
X=No. of recored
J=o
V[i+1]= new data [j]
j=j+1
j<=X
X=size of new data[]
retrieve original index
recorded desired equation
enter min value in (W)
enter max value in (J)
X=No. of recored
X1=Value of Next Step
i=o
V= index (0)
V1=V
F1=Compute Equation by V1
V2=V+1
F2=Compute Equation by V2
R= Rand (F1-F2)
V3=V1+R
Save (V3)
i=i+1
V=index(i)
i<X
Compute (time of record)
C=W+X1
C<=J
END

Initial case; with no data saved in any equation

Start

Data = Display data from Excel file

Record desired equation = Choose the equation to be used to store the data and is one of the proposed equations

Enter min value in (w) = the first number of the group set for the value of the variable.

Enter max value in (j) = the last number of the group set for the value of the variable.

X=no. of record = the required number of records called from Excel file

X1= value of next step = the increased value in variable one for every save process

I=0 == counter

V= index (0) == the index initial value

V1 = v

F1=compute equation by v1 == to evaluate the initial index value in the first equation

V2=v+1 == the value of the next index

F2=compute equation by v2 == to evaluate the second index value in the first equation

R= Rand (F1-F2) == randomly chosen number from the set of numbers that have been identified.

V3=v1+R== the summation of the index value with a particular random noise range

Save (v3) == saving the initial index with the noise

I=i+1 == the next counter by one

V=index (i) == increased the index value based on the new counter

I<x == the check data save test

Compute (time of records) == calculate the time needed to save data with noise

C=w+x1 == added the value of the next step with the first particular number

C<=j == determine if the next variable is on the range or not.

Case two; saving data on other equations

Old data [] = retrieve original index == retrieve the data saved on the database

I=0 == counter

V[i] = old data [i] == resave of the saved data on other variable

I<=s == loop to finish store all the data that already stored, and check the size of the no. of data

X=no. of record = the required number of records called from Excel file

J=0 == parameter

V [i+1] = new data[j] == increased the index by one to remove the data overlap

J=j+1 == increased the variables by one

J<=x== loop for new data

X=size of new data [] == determine the new data size need to be saved on the database.

Chapter Four: Results and Discussion

4. CHAPTER FOUR: RESULTS AND DISCUSSIONS

4.1. INTRODUCTION

In this chapter, the results will be accomplished according to the equations that used to determine the performance, security, and time required to change the equation based on different ranges and parameters.

(Liu & Wang) Equation 1 = a*v+b+noise

(Proposed equation) Equation 2 = a*v+b+noise+c

(Proposed equation) Equation 3 = a*v+b+noise+c+d

(Proposed equation) Equation 4 = (a*v+b+noise)*c

4.2. LIU AND WANG EQUATION

The equation that used by Liu and Wang is: a*v + b + noise which is considered as the equation number one or the base equation in this research.

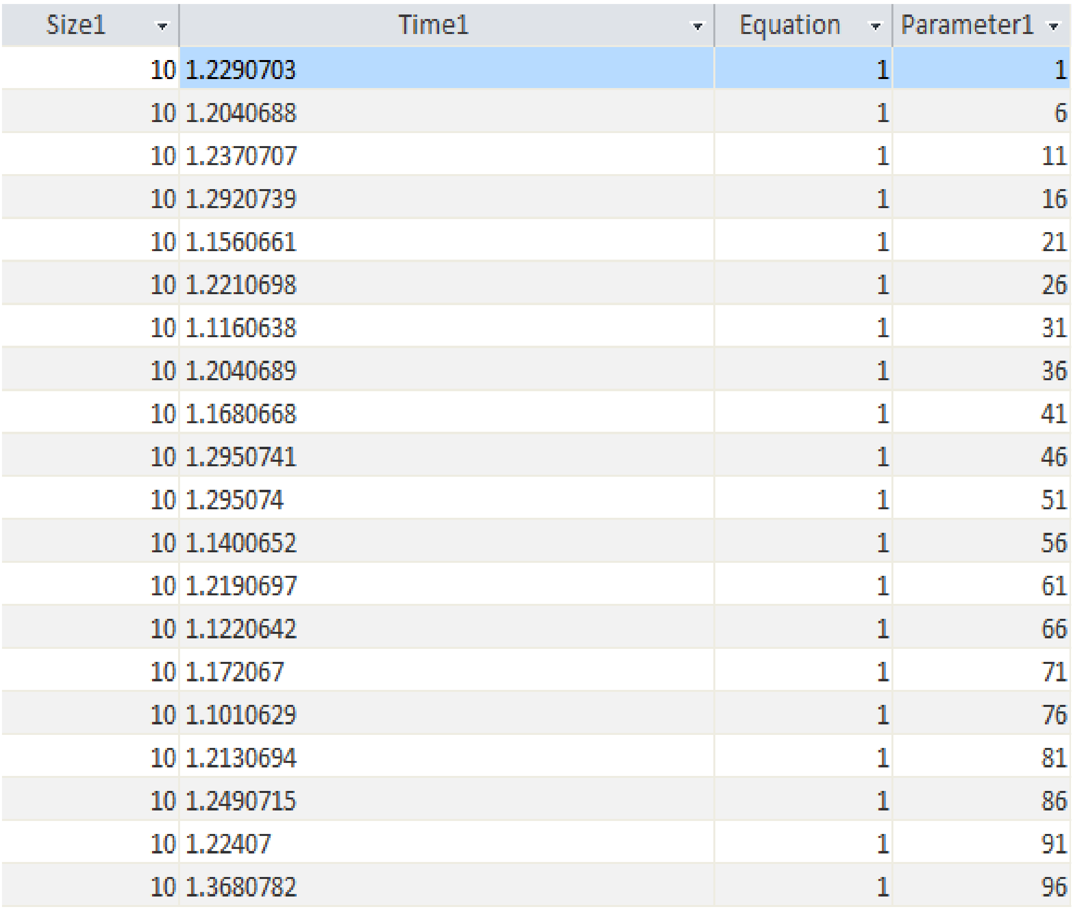
Where:

a & b: are two integer parameters

v: index number

The results of equation one is listed below in a table, where the size range is 10 – 4000 and parameter a and parameter b ranges from 1- 1650 with 5 as a step, the time will be conducted based on change one parameter while the second parameter is constant in different size ranges.

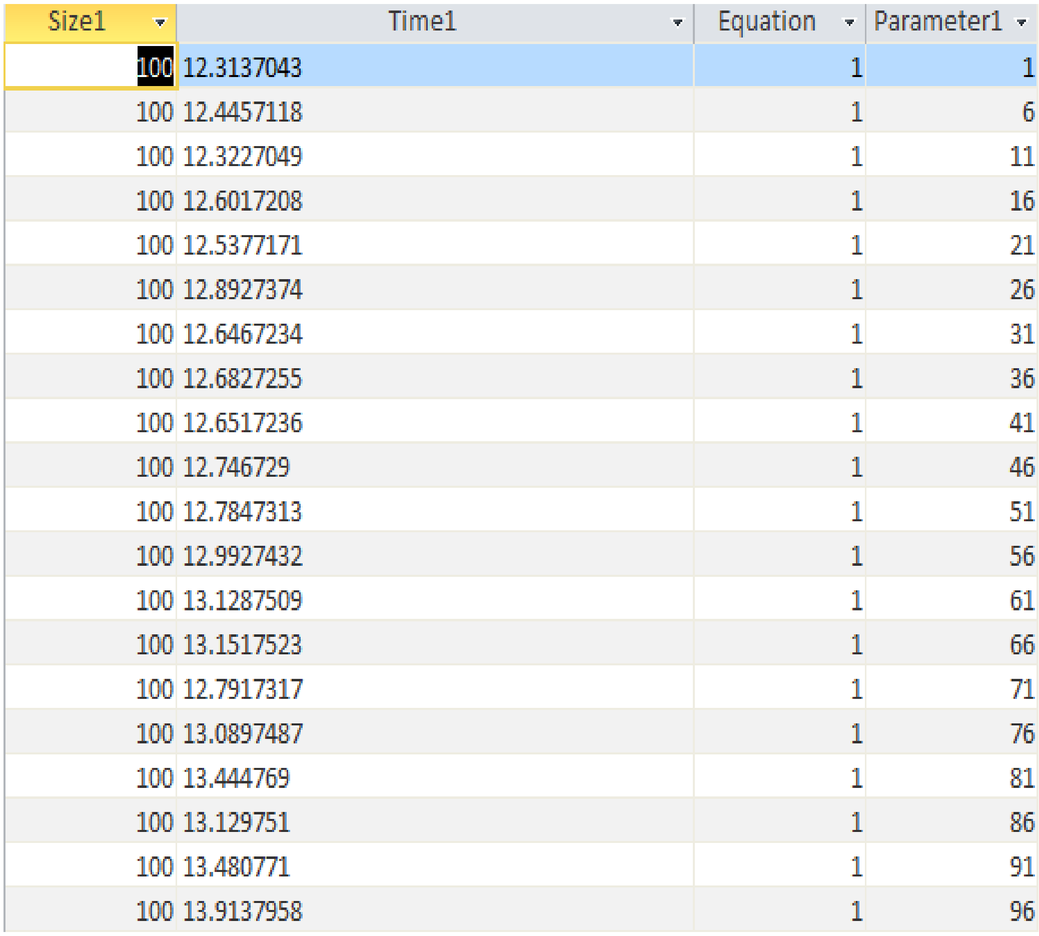
Table 4-1 Time based on parameter a



Size1	Time1	Equation	Parameter1
10	1.2290703	1	1
10	1.2040688	1	6
10	1.2370707	1	11
10	1.2920739	1	16
10	1.1560661	1	21
10	1.2210698	1	26
10	1.1160638	1	31
10	1.2040689	1	36
10	1.1680668	1	41
10	1.2950741	1	46
10	1.295074	1	51
10	1.1400652	1	56
10	1.2190697	1	61
10	1.1220642	1	66
10	1.172067	1	71
10	1.1010629	1	76
10	1.2130694	1	81
10	1.2490715	1	86
10	1.22407	1	91
10	1.3680782	1	96

As a result here the time needed is increased while the parameter (a) increased with b constant range size, and also increased with the increasing in the size range and parameter a.

Table 4-2 Time based on parameter b.



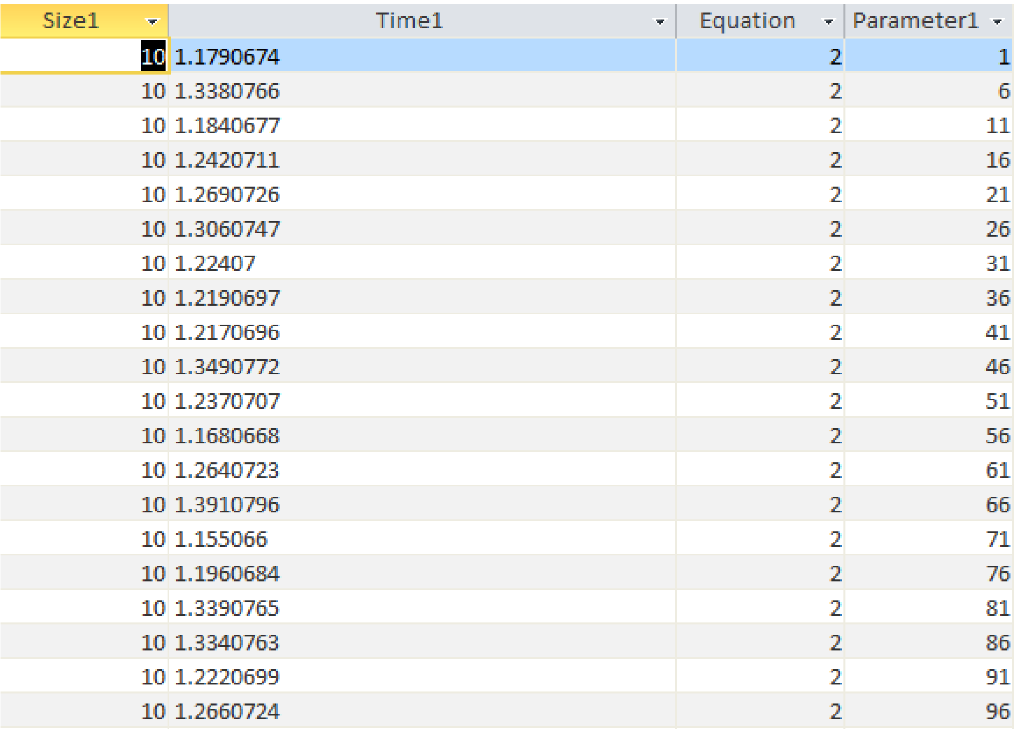
Size1	Time1	Equation	Parameter1
100	12.3137043	1	1
100	12.4457118	1	6
100	12.3227049	1	11
100	12.6017208	1	16
100	12.5377171	1	21
100	12.8927374	1	26
100	12.6467234	1	31
100	12.6827255	1	36
100	12.6517236	1	41
100	12.746729	1	46
100	12.7847313	1	51
100	12.9927432	1	56
100	13.1287509	1	61
100	13.1517523	1	66
100	12.7917317	1	71
100	13.0897487	1	76
100	13.444769	1	81
100	13.129751	1	86
100	13.480771	1	91
100	13.9137958	1	96

As a result here the time needed is increased while the parameter (b) increased with a constant range size, and also increased with the increasing in the size range and parameter b.

4.3. STUDY EQUATIONS

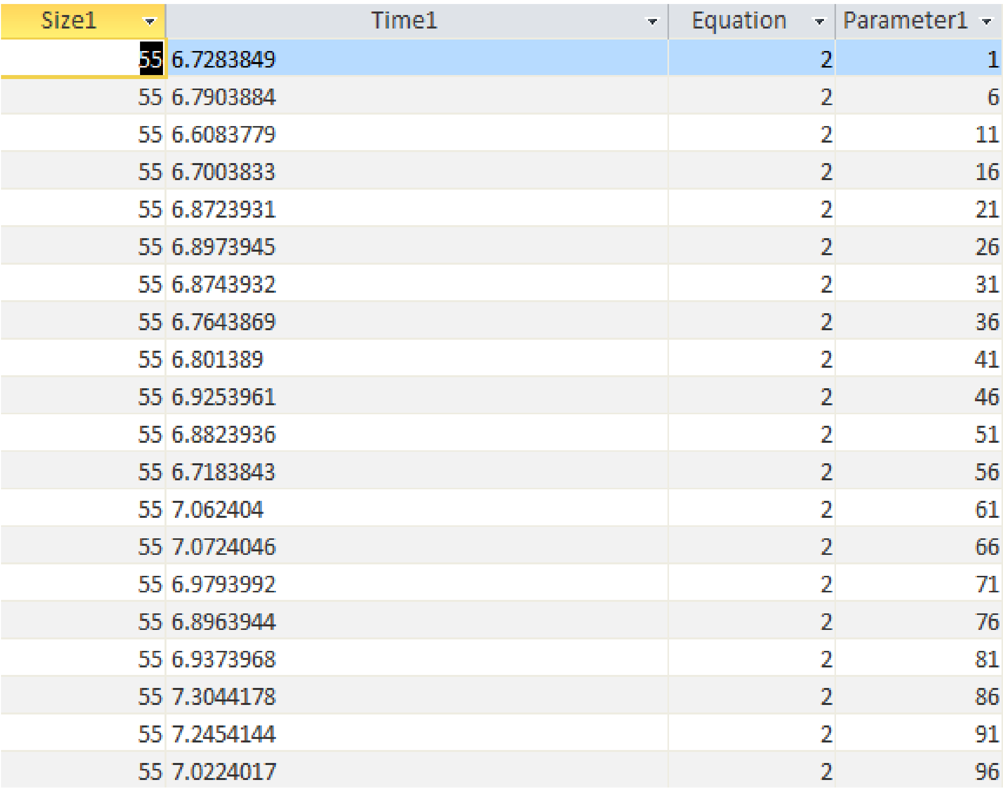
The equations here are conducted by adding extra parameters to study the time needed to change these parameters then changing the base equation to investigate the best solution that provide the best security and performance. The base equation modified by adding c and d as parameters to; a*v + b + noise which is give more security but effect on the performance.

Table 4-3 Time based on parameter a in eq2



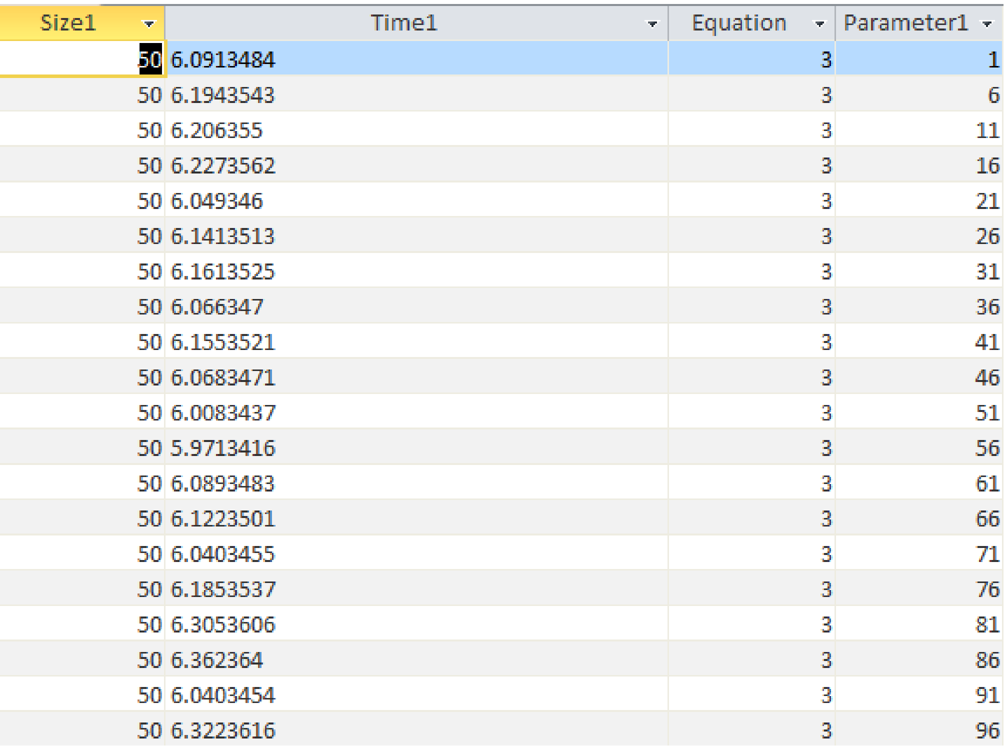
Size1	Time1	Equation	Parameter1
10	1.1790674	2	1
10	1.3380766	2	6
10	1.1840677	2	11
10	1.2420711	2	16
10	1.2690726	2	21
10	1.3060747	2	26
10	1.22407	2	31
10	1.2190697	2	36
10	1.2170696	2	41
10	1.3490772	2	46
10	1.2370707	2	51
10	1.1680668	2	56
10	1.2640723	2	61
10	1.3910796	2	66
10	1.155066	2	71
10	1.1960684	2	76
10	1.3390765	2	81
10	1.3340763	2	86
10	1.2220699	2	91
10	1.2660724	2	96

Table 4-4 Time based on parameter b in eq2



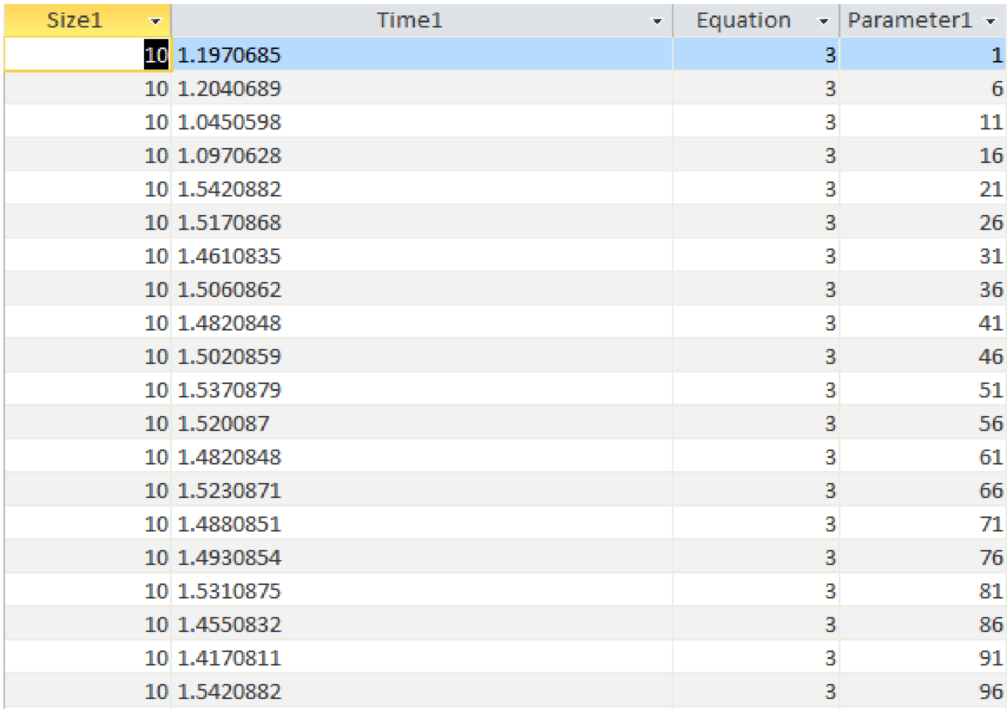
Size1	Time1	Equation	Parameter1
55	6.7283849	2	1
55	6.7903884	2	6
55	6.6083779	2	11
55	6.7003833	2	16
55	6.8723931	2	21
55	6.8973945	2	26
55	6.8743932	2	31
55	6.7643869	2	36
55	6.801389	2	41
55	6.9253961	2	46
55	6.8823936	2	51
55	6.7183843	2	56
55	7.062404	2	61
55	7.0724046	2	66
55	6.9793992	2	71
55	6.8963944	2	76
55	6.9373968	2	81
55	7.3044178	2	86
55	7.2454144	2	91
55	7.0224017	2	96

Table 4-5 Time based on parameter a in eq3



Size1	Time1	Equation	Parameter1
50	6.0913484	3	1
50	6.1943543	3	6
50	6.206355	3	11
50	6.2273562	3	16
50	6.049346	3	21
50	6.1413513	3	26
50	6.1613525	3	31
50	6.066347	3	36
50	6.1553521	3	41
50	6.0683471	3	46
50	6.0083437	3	51
50	5.9713416	3	56
50	6.0893483	3	61
50	6.1223501	3	66
50	6.0403455	3	71
50	6.1853537	3	76
50	6.3053606	3	81
50	6.362364	3	86
50	6.0403454	3	91
50	6.3223616	3	96

Table 4-6 Time based on parameter b in eq3



Size1	Time1	Equation	Parameter1
10	1.1970685	3	1
10	1.2040689	3	6
10	1.0450598	3	11
10	1.0970628	3	16
10	1.5420882	3	21
10	1.5170868	3	26
10	1.4610835	3	31
10	1.5060862	3	36
10	1.4820848	3	41
10	1.5020859	3	46
10	1.5370879	3	51
10	1.520087	3	56
10	1.4820848	3	61
10	1.5230871	3	66
10	1.4880851	3	71
10	1.4930854	3	76
10	1.5310875	3	81
10	1.4550832	3	86
10	1.4170811	3	91
10	1.5420882	3	96

As a result here the time increased by increasing the range of every parameter a or b in both equation with the increase the range size of the equation.

When we compare the three equations, we can notice that; while changing parameter a once and parameter b in the second time: let we took the size range equal to 10 in the three equations and the parameter change from 1 to 96 with 5 as a step between the parameter values, in the three equations the time needed is increased with the increase in the value of parameters, the time needed in the base equation is the smallest time in compare with the other two equations which is mean it's the best performance, but with less security, while the other two equations need more time that is less performance, but with high level of security. Using more than one equation increased the security level because the need of re-index the data in the database, so the user can't detect the equation which used to save data on it.

If we want to compare the performance or the time needed in every equation (equation 2 or 3) based on equation one, as an example:

Equation one, parameter a, size equal to 100, and the time is equal to 12.3227048 then we considered the performance equal to 100%. For equation two at the same conditions the time is equal to 12.71372772, by basic calculations;

12.3227048 ____________ 100%

12.71372772 ____________ X

Then X= 103.173

The reduction in performance is 103.1732 – 100 = 3.1732%. Tables below defined some examples:

Table 4-7 Time difference and performance, No. rec=10

No. rec	Eq. no.	Parameters	time	Eq2 – eq1	Eq3 – eq1	Reduction in performance %
10	1	A=21,b=7	1.1560661			
10	2	A=21,b=7,c=9	1.2690726	0.09		8.905%
10	3	A=21,b=7,c=9,d=100	1.521087		0.26	23.997%

Table 4-8 Time difference and performance, No. rec=50

No. rec	Eq. no.	Parameters	time	Eq2 – eq1	Eq3 – eq1	Reduction in performance %
50	1	A=260,b=7	6.5573751			
50	2	A=260,b=7,c=9	6.5663755	0.01		0.137%
50	3	A=260,b=7,c=9,d=100	6.6163784		0.05	0.892%

Table 4-9 Time difference and performance, No. rec=1000

No. rec	Eq. no.	Parameters	time	Eq2 – eq1	Eq3 – eq1	Reduction in performance %
1000	1	A=2700,b=1	348.5099336			
1000	2	A=2700,b=1,c=9	349.3699828	0.86		0.246%
1000	3	A=2700,b=1,c=9,d=100	351.5151055		2.15	0.855%

The average percentage for the reduction in performance for the above values =

$$\frac{8.905+23.997+0.137+0.892+0.246+0.855}{6}$$

= 5.83%

4.4. BEST PERFORMANCE WITH ACCEPTED SECURITY LEVEL

According to the problem statement, this study aims to investigate the best solution that provides the best level of security and performance. This is accomplished by determining the best equation and parameters can be applied to have an acceptance security degree and performance. A comparison between equation two and equation three based on equation one has been done to achieve this goal. Random cases would be taken, and then an average performance and security compared with each other. As it was shown equation two has three parameters while equation three has four parameters according to this equation three is the best security degree but with less performance or a high reduction in the performance, while equation two has an acceptable level of security with high performance or less reduction in performance compared to equation three as it is seen below, so we conclude that equation number two is the best solution for this problem.

Table 4-10 Compared eq2 with eq1

records	**Parameter a**	**Time (eq1)**	**Time (eq2)**	**Reduction in performance %**	**Parameter b**	**Time (eq1)**	**Time (eq2)**	**Reduction in performance %**
10	6	1.2040668	1.3380766	11.129765	91	1.190068	1.206069	1.344545
10	66	1.1220642	1.3910796	23.975045	96	1.22407245	1.2490715	2.042285
50	1000	5.0412884	6.193543	22.856352	16	6.0253447	7.5204302	24.81328
50	1080	6.3683642	6.3993603	0.48672	21	6.1073493	7.587434	24.23449
400	16	52.5586061	51.59595911	-1.831569	1000	49.0558058	49.2958195	0.489267
400	21	54.6061233	55.0033176	0.7273805	1050	50.3078775	49.0988083	-2.40334
1000	1	164.369401	167.2145691	1.7309595	1000	125.294166	126.012388	0.573228
1000	6	170.138303	171.75822	0.9521176	1050	132.375571	134.376631	1.511654
4000	100	565.756359	652.1342999	15.267692	300	542.818047	543.016049	0.036477
4000	110	683.939119	750.3829194	9.7148706	350	644.697875	645.578691	0.136625
Average				8.5009333				5.27785

$$\text{Avg (tot)} = \frac{avg\ reduction\ in\ a + avg\ reduction\ in\ b}{2}$$

$$= \frac{8.5009333 + 5.27785}{2}$$

$= 6.889392$ the less reduction in performance

Table 4-11 Compared eq3 with eq1

records	Parameter a	Time (eq1)	Time (eq2)	Reduction in performance %	Parameter b	Time (eq1)	Time (eq2)	Reduction in performance %
10	6	1.2040668	1.4490829	20.349045	91	1.190068	1.2350707	3.781523
10	66	1.1220642	1.4500829	29.233506	96	1.22407245	1.1970684	-2.20608
50	1000	5.0412884	6.05934666	20.194406	16	6.0253447	9.526339	58.10446
50	1050	6.3683642	6.2043549	-2.575376	21	6.1073493	9.0683471	48.48254
400	16	52.5586061	52.3539945	-0.389302	1000	49.0558058	50.7897906	3.534719
400	21	54.6061233	59.7150723	9.3560002	1050	50.3078775	50.3328216	0.049583
1000	1	164.3694014	168.2636241	2.3691896	1000	125.294166	129.074874	3.017465
1000	6	170.1383033	176.2940835	3.6181037	1050	132.375571	136.493979	3.111153
4000	100	565.7563594	652.642329	15.357489	300	542.8180474	544.672153	0.34157
4000	110	683.939119	757.9363515	10.819272	350	644.697875	647.965062	0.506778
Average				10.833233				11.87237

$$\text{Avg (tot)} = \frac{avg\ reduction\ in\ a + avg\ reduction\ in\ b}{2}$$

$$= \frac{10.83233 + 11.87237}{2}$$

$= 11.3528$ more reduction in performance

4.5. BEST RANGE OF PARAMETERS

This test was evaluated according to the ranges of the number of recodes each range is a different case to study, after the evaluating of the two tables below, I found that if increasing the value of the record ranges the time needed to save data increasing, in other hand increasing the ranges of the record number will not effect on the complexity to solve the equation I have to save data on it so the best range of parameters to have is among between 1 to 9. The determination of parameters number helps the equation to work with high speed with saving the complexity.

Table 4-12 Parameters range with 10 records

No. of record	Equation	Parameters	Digits of parameter	Time	Time deference	Reduction in performance %
10	1	A=6,b=7	1	1.47		
10	1	A=15,b=7	2	1.48	0.01	0.68
10	1	A=105,b=7	3	1.49	0.01	1.36
10	1	A=1001,b=7	4	1.51	0.01	2.72

Table 4-13 Parameters range with 1000 records

No. of record	Equation	Parameters	Digits of parameter	Time	Time deference	Reduction in performance %
1000	1	A=6,b=1	1	130.00		
1000	1	A=11,b=1	2	139.31	9.31	7.161
1000	1	A=130,b=1	3	157.96	18.65	21.507
1000	1	A=1300,b=1	4	169.68	11.72	30.52

Reduction of performance can be found like this:

1.47 ______________ 100%

1.48 ______________ X

Then X= 100.68%

The reduction in performance is100.68 – 100 = 0.68%.

4.6. THE STUDY OF THE VARIABLES NUMBER

I have studied the results based on a comparison of the number of variables of the proposed equations, where I took the number of variables 2, 3 and 4 and the study time for each equation, and I found when increasing the number of variables increases the time it takes. Therefore, the time spent in the equation No. 4 is the best time because there beating, increase uncertainty and add variable to the equation while preserving the time it takes to save the data. Table below discuss this:

Table 4-14 Study of the number of variables

No. of record	Equation	No. of parameters	Time	Time difference	Reduction in performance %
100	1	2	12.65	0.0002765	
1000	1	2	140.01	13.9070993	
100	2	3	14.67	2.0202765	0.99
1000	2	3	182.65	56.5470993	0.75
100	3	4	17.95	5.3002765	0.99
1000	3	4	217.30	91.1970993	0.84
100	4	2	13.89	1.2402765	0.99
1000	4	2	154.55	28.4470993	0.51

4.7. RE-INDEXING

To increase the security I supposed to change the saved equation, but this caused to increase the time needed so decrease the performance, below there is the variance of time between equation one and the three other equations, with the reduction in performance which is calculated as it is mention previously.

Table 4-15 Time needs to change from equation 1 to 2

Size	Time deference	Equation	Time reduction %
10	0.0490028	2	4.06788
50	0.157009	2	1.06996
100	0.3550197	2	1.24911
400	1.4980868	2	0.984676
1000	3.782216	2	0.72143
4000	14.4978268	2	2.19813
Average 5560			0.001

Table 4-16 Time needs to change from equation 1 to 3

Size	Time deference	Equation	Time reduction %
10	0.028017	3	22.94549
50	0.1510085	3	0.263374
100	0.3350192	3	0.007906
400	1.4930863	3	1.458551
1000	3.8342188	3	0.7817
4000	14.7498425	3	14.37203
Average 5560			0.007

Table 4-17 Time needs to change from equation 1 to 4

Size	Time deference	Equation	Time reduction %
10	0.02	4	19.85354
50	0.15	4	0.987654
100	0.29	4	4.371888
400	1.15	4	1.807291
1000	3.28	4	1.936648
4000	19.21	4	2.48382
Average 5560			0.005

After studying the time needed to change from equation one to the proposed equations, I found that it is a short time comparing with the original time needed to save data on the first time, so I can determine a suitable time to change the equation and save data which is refers to the short time needed to equation changing based on equation one that describe for the three equation on the tables above.

4.8. COMPARE THE RESULTS OF THE PROPOSED EQUATIONS WITH RESULTS OF THE PREVIOUS STUDY EQUATION

Table 4-18 Compare equation 1 with equation 2

No. of records	Time of Equation 1	Time of Equation 2	Reduction time %
10	1.88	1.93	0.02
50	9.01	9.71	0.07
100	17.39	17.93	0.03
400	70.49	70.69	0.002
1000	177.42	182.06	0.02
4000	795.88	796.78	0.001
Average			0.02

In this table, we compare the time it takes to store the data to the equation 1 original Liu and Wang equation with the first of the suggested after the addition of a variable; we observed rate of increase in time is 0:02.

Table 4-19 Compare equation 1 with equation 3

No. of records	Time of Equation 1	Time of Equation 3	Reduction time %
10	1.88	2.13	0.11
50	9.01	9.94	0.09
100	17.39	18.22	0.04
400	70.49	71.97	0.02
1000	177.42	183.02	0.03
4000	795.88	800.01	0.005
Average			0.04

In this table, we compare the time it takes to store the data through one original Liu and Wang with the second equation after the addition of the suggested two variables have, we noticed the rate of increase in time is 0:04.

Table 4-20 Compare equation 1 with equation 4

No. of records	Time of Equation 1	Time of Equation 4	Reduction time
10	1.88	2.01	0.06
50	9.01	9.82	0.08
100	17.39	18.01	0.03
400	70.49	71.21	0.01
1000	177.42	182.70	0.02
4000	795.88	799.12	0.0040
Average			0.03

In this table, we compare the time it takes to store the data through the original equation 1 Liu Wang The proposed equation with the second after multiplying the equation variable added; we have noticed an increase in the average time is 0:03.

Based on previous tests and study results found when adding one variable increases with the increase in security time, to store the data 0.02, while when adding two variables increase becomes twice the first time, when Multiplying variable with equation takes less time to add tow variables to the equation.

This indicates to add only one variable, but in the case of addition and multiplication best to add the second variable, according to results shown that the addition of one variable increases security while increasing the proportion of time it takes to store the data less than adding a second variable.

Table 4-21 Table of evaluate the equations

Equation No.	Reduction time	No. of parameter added	Operation type
2	0.02	1	Addition (+)
3	0.04	2	Addition (+)
4	0.03	1	Multiplication (*)

Chapter Five:
Conclusion

5. CHAPTER FIVE: CONCLUSION

Searching on an encrypted database is outface for the cloud computing. Utilizing the OPE (Order Preserving Encryption) will allow the cloud provider to seek over a database without knowing the original data. Liu and Wang was solving this leak by the addition of noises to the original data utilizing of some linear function with two client-based parameters, this research is looking to inquire into the algorithm. Studies number of parameters that to be utilized, also to study the time of changing these parameters then changes the function. Adding extra parameters will accomplish more security but it will effect on the performance.

The suggested model scattered into two sides: the initial side is the client side of the secure database that is utilizing the process which is presented above in the data index encryption, where the second side is the cloud of storing the encrypted data, that added an extra parameter to promote the ambiguity in the equation that implemented by a second linear equation or maybe more than one linear equation with the growth of the parameter number to enhance ambiguity and security.

As a result the time needed is increased while the parameter (a or b) increased with a constant range size, and also increased with the increasing in the size range and increasing in parameter a or b.

When we compare the three equations, we can notice that; while changing parameter a once and parameter b in the second time, the time needed is increased with the increase in the value of parameters, the time needed in the base equation is the smallest time in compare with the other two equations which is mean it’s the best performance, but with less security, while the other two equations need more time that is less performance, but with high level of security, as an average to the reduction in performance is equal to 5.83%. Using more than one equation increased the security level because the need of re-index the data in the database, so the user can't detect the equation which used to save data on it. Also changing the equation form the base to any other equation need more time so less performance but more security.

According to previous tests and to the study of the results, I obtained that:

1. According to this study, the best value of the variables are between one to nine because this range allows running the equation with a high speed and save the complexity of the equation.

2. According to this study, the best equation to save the speed with high level of security is equation number two and equation number four, where the addition of every variable increased the time needed to save data by 0.2%.

3. After studying the time it takes to move between equations I found that the time it takes to move from equation 1 to 2 and from equation 1 to 4 is the best time, Where the rate of increasing in time to move out of the original equation Liu and Wang equation to the proposed equation number 2 is 0.02, and that the rate of increasing in time to move out of the original equation to the proposed equation number 4 is a 0.03 time by which the study I out.

6. REFERENCES

- Agrawal, D., El Abbadi, A., Emekci, F., & Metwally, A. (2009). Database management as a service: Challenges and opportunities. In Data Engineering, 2009. ICDE'09. IEEE 25th International Conference, 1709-1716

- Baeten, Y., Nijs, N. (2012). Operating Systems & Security. IEEE International Conference, 5-10.

- Bernhardt, V. (2013). Data analysis for continuous school improvement. Routledge. IEEE International Conference, 50-53.

- Boldyreva, A., Chenette, N., Lee, Y., and O'neill, A. (2009). Order-preserving symmetric encryption. In Advances in Cryptology-EUROCRYPT 2009, Springer Berlin Heidelberg, 224-241.

- Boldyreva et al. (2015). Modular Order-Preserving Encryption, Revisited. Springer Berlin Heidelberg, 1-3.

- Boldyreva, A., Chenette, N., & O'Neill, A. (2011). Order-preserving encryption revisited: Improved security analysis and alternative solutions. InAdvances in Cryptology–CRYPTO 2011 (pp. 578-595). Springer Berlin Heidelberg.

- Brakerski, Z., and Vaikuntanathan, V. (2011). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Advances in Cryptology–CRYPTO 2011, Springer Berlin Heidelberg, 505-524.

- Codd, E., F., (1972). Relational completeness of data base sublanguages. IBM Corporation, 65-98.

- Conway, G., and Curry, E. (2012). Managing Cloud Computing-A Life Cycle Approach. In CLOSER, 198-207.
- Gadichal, A. B. (2011). Audio Wave Steganography. International Journal of Soft Computing and Engineering (IJSCE), ISSN, 2231-2307.
- Garzon, J. C., Ng, C. S., Sihoe, A. D., Manlulu, A. V., Wong, R. H., Lee, T. W., and Yim, A. P. (2006). Video-assisted thoracic surgery pulmonary resection for lung cancer in patients with poor lung function. The Annals of thoracic surgery, 81(6), 1996-2003.
- Goh, E. J. (2003). Secure Indexes. IACR Cryptology ePrint Archive, 216.
- Hore, B., Mehrotra, S., and Tsudik, G. (2004). A privacy-preserving index for range queries. In Proceedings of the Thirtieth international conference on Very large data bases-Volume 30, 720-731.
- Khachatryan, V., Sirunyan, A. M., Tumasyan, A., Adam, W., Bergauer, T., Dragicevic, M., and Adler, V. (2010). Observation of long-range, near-side angular correlations in proton-proton collisions at the LHC. Journal of High Energy Physics, 1-38.
- Kuzu, M., Islam, M. S., and Kantarcioglu, M. (2012). Efficient similarity search over encrypted data. In Data Engineering (ICDE), 2012 IEEE 28th International Conference, 1156-1167.
- Kolesnikov, V., & Shikfa, A. (2012). On The Limits of Privacy Provided by Order- Preserving Encryption. Bell Labs Technical Journal, 17(3), 135-146.

- Lee, H. O., and Kim, M. (2013).Implementing cloud computing in the current IT environments of Korean government agencies.International Journal of Software Engineering and Its Applications, Vol. 7.No.1, 5-8.
- Lee.M, (2013). Encryption Works How to Protect Your Privacy in the Age of NSA Surveillance. pressfreedomfoundation.org, 3-29.
- Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., and Lou, W. (2010). Fuzzy keyword search over encrypted data in cloud computing. In INFOCOM, 2010 Proceedings IEEE, 1-5.
- Liu, D., and Wang, S. (2012). Programmable order-preserving secure index for encrypted database query. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference, 502-509.
- Liu, D., and Wang, S. (2013). Nonlinear order preserving index for encrypted database query in service cloud environments. Wiley Online Library (wileyonlinelibrary.com).Concurrency Computat: Pract. Exper. 2013; 25:1967–1984
- Mykletun, E., and Tsudik, G. (2006). Aggregation queries in the database-as-a-service model. In Data and Applications Security XX, Springer Berlin Heidelberg, 89-103.
- Malkin, T., Teranishi, I., & Yung, M. (2013). Order-Preserving Encryption Secure Beyond One-Wayness. IACR Cryptology ePrint Archive, 2013, 409.
- NIST, U.S. National Institute of standareds.
- Popa, R. A., Redfield, C., Zeldovich, N., and Balakrishnan, H. (2011). Cryptdb: protecting confidentiality with encrypted query processing.

InProceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, ACM, 85-100.

- Robbins, R. J. (1994). Database Fundamentals. Johns Hopkins University, rrobbins@ gdb. Org, 5-8.

- Saleh, E., Alsa'deh, A., Kayed, A., and Meinel, C. (2015). Processing Over Encrypted Data: Between Theory and Practice. Submitted to be published 5-8.
- Santos, N., Gummadi, K. P., and Rodrigues, R. (2009). Towards trusted cloud computing. In Proceedings of the 2009 conference on hot topics in cloud computing, 3-3.
- Sathyavani S., Senthilkumar T. P. and Phil M. (2013) "Survey on Cloud Computing", International Journal of Computer Trends and Technology, 4 - 9.
- Seleym, A., and Darwish, D. (2012). Real-time Covert Communications Channel time Covert Communications Channel time Covert Communications Channel for Audio Signals.
- Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.
- Shmueli, E., Vaisenberg, R., Elovici, Y., and Glezer, C. (2010). Database encryption: an overview of contemporary challenges and design considerations.ACM SIGMOD Record, 38(3), 29-34.

- Shmueli, E., Waisenberg, R., Elovici, Y., and Gudes, E. (2005). Designing secure indexes for encrypted databases. In Data and Applications Security XIX. Springer Berlin Heidelberg, 54-68.
- Tsai, T. H., Chen, Y. C., Huang, H. C., Huang, P. M., and Chou, K. S. (2011). A practical Chinese wall security model in cloud computing. InNetwork Operations and Management Symposium (APNOMS), 13th Asia-Pacific. IEEE, 1-4.
- Voorsluys, W., Broberg, J., and Buyya, R. (2011). Introduction to cloud computing. Cloud Computing, 1-41.
- Xiao, L., Yen, I. L., & Huynh, D. T. (2012). Extending Order Preserving Encryption for Multi-User Systems. IACR Cryptology ePrint Archive, 2012, 192.