MEU جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY
Amman - Jordan

Comparative study for Order Preserving Encryption Characteristic

دراسة مقارنة لخصائص التشفير المتماثل

By

Anas Abdulrazzaq Ali Aljuboori
Supervisor
Prof. Ahmad Kayed

Submitted in Partial Fulfilment of the Requirements of the Master Degree in Computer Science

Computer Science Department

Faculty of Information Technology

Middle East University

January, 2018

Authorization

I, Anas Abdulrazzaq Aljuboori, authorize Middle East University (MEU) to provide copies of my thesis to the concerned libraries, establishments, and institutions upon request.

Name: Anas Abdulrazzaq Aljuboori

Date: 17-4-2018

Signature:

Examination Committee Decision

This is to certify that the thesis entitled "comparative study for order preserving encryption characteristics " was successfully defended and approved on 10-1-2018.

Examination Committee Members **Signature**

(Chairman of Examination Committee and Supervisor)

Prof. Ahmad K. A. Kayed

Professor

Middle East University 18.4.2018

(Internal Committee Member)

Dr. Ahmad Hmouz 17/4/2018

Assistant Professor

Middle East University

(External Committee Member) 18/4/2018

Prof. Wesam Almobaideen

Professor

University of Jordan

الاهداء

بسم الله الرحمن الرحيم
(قل اعملوا فسيرى الله عملكم ورسوله والمؤمنون)
إلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلى بطاعتك , ولا تطيب اللحظات إلا بذكرك , ولا تطيب الآخرة إلا بعفوك ولا تطيب الجنة إلا برؤيتك
(الله جل جلاله)

إلى من بلغ الرسالة وأدى الأمانة، ونصح الأمة، إلى نبي الرحمة ونور العالمين
سيدنا محمد صل الله عليه وسلم

كلمات الثناء لا توفيك حقك، شكراً لك على عطائك.
أ.د. حمزة عباس السوادي

يا من أحمل اسمك بكل فخر، يا من أفتقدك منذ الصغر
يا من يرتعش قلبي لذكرك، يا من أودعتني لله أهديك هذا البحث
أبي ***(عبد الرزاق الجبوري)***

إليك أماه. قطرة في بحرك العظيم.حباً وطاعة وبرا
جزاك اللهخيراً. وأمد في عمرك بالصالحات، فأنت زهرة الحياة ونورها

(امي الحبيبة)

إلى من كلل العرق جبينه. وشققت الأيام يديه، إلى من علمني أن الأعمال الكبيرة لا تتم إلا بالصبر والعزيمة والإصرار، إلى اخي أطال الله بقاءه، وألبسه ثوب الصحة والعافية، ومتعني بحبه ورد جميله، أهدي ثمرة من ثمار غرسه

(الدكتور انيس الجبوري)

الى من لم تجف دموع فراقه ولم يبرا جرحه في القلب الى من لا أنسي ذكره يوما أيها الساكن تحت الثرى لقائنا في جنة الفردوس الاعلى الغالي الحبيب

(المهندس اوس الجبوري رحمه الله)

إلى من أرى التفاؤل بعينه، والسعادة في ضحكته ,إلى شعلة الذكاء والنور, إلى الوجه المفعم بالبراءة ولمحبتك أزهرت أيامي وتفتحت براعم للغد
(الدكتور *احمد الجبوري)*

إلى من هم اقرب أليّ من روحي , الى من شاركني حضن ألام وبهم استمد عزتي وإصراري الى من تهدأ نفسي بلقياهن , ويبسم الثغر لمحياهن ,
(اخواتي ***الحبيبات لكم مني كل الود وكل التقدير)***

الى كل من دعا لي بظهر الغيب وكل من ساندني وكل من وقف جنبي وكل من تمنى لي الخير احبتي في الله
(اقاربي ***واصدقائي)***

List of Tables

List of Figures

List of Abbreviations

Abbreviations	**Meaning**
OPE	Order Preserving Encryption
OPES	Order-Preserving Encryption Scheme
ITU-800	International Telecommunication Unit
CCITT	International Telegraph and Telephone Consultative Committee
OSI	Open Systems Interconnection
IND	Indestinguishability
IND-CPA	Indestinguishability-against Chosen Plaintext Attack
IND-OCPA	Indestinguishability-against Order Chosen Plaintext Attack
MOPE	Most Order-Preserving Encoding
ROPE	Randomized Order Preserving Encryption
PRF	Pseudorandom Function
stOPE	Order Preserving Encryption state

Table of Contents

Comparative study for Order Preserving Encryption characteristic

Prepared By

Anas Abdulrazzaq Ali Aljuboori

Supervisor

Prof. Ahmad Al-Kayed

Abstract

The security of cloud’s database is the most challenge in the cloud models. Encryption is the solution for the data security problem but some encryption techniques do not preserve data order. Order Preserving Encryption (OPE) is a scheme for providing query privacy in search process under encrypted cloud’s database services.

Several institutes built general Measuring scheme that highlighted the security aspect and identified specifications and properties of security algorithms. As far as we know, an accurate Measuring scheme that clearly identifies characteristics and properties for Order-Preserving Encryption Schemes (OPES) remains unavailable. There have been some attempts to identify some OPES characteristics by Popa and Chenette, However, They did not present a fully comparative Measuring schemes that standardized the OPES. This thesis provides in-depth comparative studies by utilizing available research in this area in an attempt to propose a standardized Measuring scheme.

This thesis is based on three surveys covering the period (1991 – 2017) as well as over Two hundred research papers. This thesis studies the main characteristics of (ITU-X800), Popa, Chenette, and OPES characteristics and proposed a new OPES Measuring scheme.

According to the outcomes, the researcher proposes three (OPES) measuring schemes. This thesis called the first measuring scheme as the "Must Measuring Scheme” which consists of the mandatory properties that must be available in all (OPE) schemes. The

“Must Measuring Scheme” characteristics have been identified as the most used ones in real OPES system as well as the most cited characteristics in the OPES and security literature. This thesis called the second measuring scheme as the “Applied Measuring Scheme”. This measuring scheme consists of all characteristics in the must measuring scheme in addition to the most characteristics that have been used in real OPES systems. This thesis called the third measuring scheme as the “Theoretical Measuring Scheme”. This measuring scheme consists of all characteristics in the must measuring scheme in addition to the most characteristics that have been cited the OPES and security literature. The “must” has been identified in this thesis by using certain cutting point for the number of OPES or literature that have been use or cited this characteristics. Fifty nine ITU-X800 characteristics, 11 Popa’s characteristics, 11 OPES, 3 surveys, 200 papers, and 30 OPES papers have been carefully examined thus leading to the proposal of the three measuring scheme.

Key Words: ORDER PRESERVING ENCRYPION (OPE), ITU-X800, IND, CHARACTIRSTIC, MEASURING SCHEME

دراسة مقارنة لخصائص التشفير المتماثل

اعداد

انس عبد الرزاق علي الجبوري

إشراف الاستاذ الدكتور

احمد كايد

الملخص

التحدي الكبير في قاعدة البيانات السحابية هو كيفية حماية هذه القاعدة. التشفير هي العملية الاكثر أمنا لحل هذه المشكلة ولكن بعض تقنيات التشفير لا تحافظ على ترتيب البيانات بعد عملية التشفير. حفظ ترتيب التشفير (OPE) هو مخطط لتوفير خصوصية الاستعلام في عملية البحث تحت خدمات قاعدة البيانات السحابية المشفرة.

هناك العديد من الاطر العامة التي اهتمت بالأمن بشكل عام حددت المواصفات والخصائص الواجب توفرها في الخوارزميات المتخصصة في مجال الامن. ولكن وحسب علم الباحث لا يوجد إطار واضح ودقيق يحدد المواصفات والخصائص الواجب توفرها في مجال خوارزميات التشفير المتماثل (OPE).

علما كانت هناك بعض المحاولات التي قام بها (Popa, Chenette) لكن لم تكن اطارا عام للتشفير المتماثل. هذا البحث يقوم بأجراء دراسات مقارنة عميقة واستخدام الدراسات المتوافرة في هذا المجال لاقتراح مخطط القياس .

اعتمد هذا البحث ثلاثة مسوحات تغطي الفترة الزمنية (1991-2017) وكذلك على أكثر من مئتي ورقة بحثية لاقتراح مخطط القياس هذا.

ونتيجة الدراسة يقترح الباحث ثلاثة مخططات قياسية للتشفير المتماثل وهي قائمة على اساس الخصائص التي لابد ان تتوافر في جميع خوارزميات التشفير المتماثل وتمت تسميتها بالمخطط

الواجب. وكذلك الخصائص الاكثر استخداما والمخطط الثالث المخطط النظري. تمت دراسة (59) خاصية من خلال ال(ITU-X800) وكذلك (11) خاصية من خلال عمل (Popa) وكذلك(11) تطبيق للخوارزميات بالتفاصيل لاقتراح المخططات القياسية الثلاثة السابقة.

الكلمات المفتاحية: التشفير المتماثل، خصائص التشفير المتماثل، مخططات القياس.

Chapter One
Introduction

1.1. Introduction

The Cloud storage enables the clients to store documents online in a result the clients can get to them from any area through the web. The good example for this service is Dropbox service.

The security issues with the cloud’s database can be solved if the sensitive data are encrypted. Naturally, it leads to the problem that how the database management system (DBMS) can process queries on encrypted data. Search queries can be classified into exact-match search.

Queries and Range search queries are more general and more difficult to handle under security constraints. One important class of methods to enable range query processing on encrypted data is Order Preserving Encryption (OPE) (Boldyreva, et. al. 2009. Agrawal, et. al. 2004; Bebek., 2002).

An Order Preserving Encryption (OPE) is a scheme for providing query privacy in search process under encrypted cloud’s database services. This scheme allows performing cloud database queries to search over encrypted environment. The encryption scheme of OPE depends on symmetric encryption which produces cipher texts that preserve the numerical ordering of plaintexts. OPE’s characteristics have keys generations, ordering techniques, encryption algorithms, for several database management systems such as (MySQL, Oracle, etc.). (Boldyreva, et. al. 2009)

Several institutes built general measuring schemes that highlighted the security aspect and identified specifications and properties of security algorithms. As far as we know, an accurate measuring scheme that clearly identifies characteristics and properties for Order-Preserving Encryption Schemes (OPES) remains unavailable. There have been some attempts to identify some OPES characteristics by Popa and Chenette (Agrawal R, 2004).

However, they did not present a measuring schemes that standardized the OPES. There is a need to build a measuring scheme for the OPEs algorithms to show the characteristics of how to design this measuring scheme.

This thesis provides comparative studies by utilizing available research in this area in an attempt to propose a standardized measuring scheme. This thesis survives many measuring schemes to find characteristics for designing measuring scheme for OPEs. This measuring scheme should include the main OPE's characteristics such as key generation such as (i.e. pseudorandom function), encryption algorithm, and ordering technique. This thesis also builds a measuring scheme based on security measuring scheme. This thesis adapts the (Security architecture for Open Systems Interconnection for (CCITT). (TU-X.800) is part of (OSI) it defines a systematic way of defining and providing security requirements to be useful (OSI, 1991). It adapts these characteristics for (OPEs algorithm because ITU-X.800 is well-known OPEs algorithms). Many researchers studied the characteristic and also compared the applicability to adopt them for OPE algorithms including Popa and Chenette works in this domain.

1.2. Problems Statement

The main problem of cloud computing is security. Using encryption techniques solve some have problems of data security for cloud computing but they have created new problems such as performing operations over encrypted data. Many OPE schemes have made processing over encrypted data possible, however there are several OPE algorithms that are still exist. There is a need to find a set of characteristics that can compare all of OPE algorithms. Several surveys are available about the privacy of OPEs but there are no standard measuring scheme in order to compare these algorithms. This thesis will study the previous reported measures and develop a new measuring scheme, then investigated and compare these available algorithms using this proposed measuring scheme.

This thesis will answer the following questions:

1. What are the main characteristics that can be applied on OPE algorithms?
2. How can we build a measuring scheme for OPEs?
3. How can we compare the available OPE algorithms?

1.3. Objectives

The main objectives of this thesis are to compare the OPE schemes and their characteristics as encryption and decryptions algorithms by using the ordering techniques and how can the authors evaluate encryption and decryption algorithms and how they use them to design their schemes. Such scheme should include the required algorithms to achieve good performance and high level of security.

According to the previous studies, the researcher will build a methodology to design a new measuring scheme for OPE’s characteristics as follows. The detail of this scheme will be explained later in chapter three:

1. Prepare a database for almost all OPEs characteristics of schemes and references.
2. Compare the schemes and references and classify the characteristics to propose a new measuring scheme with OPE characteristics.
3. Only the higher characteristics that satisfied OPEs schemes will be considered.

1.4. Motivation

There is a necessity to find a solution for the security of data problem. Encryption is one of the proposed and strong solutions and exactly computing directly over encrypted data without decrypting them. OPES is one of the encryption techniques that provide this ability of computing with the preserve of order of plaintext to corresponding encrypted measuring schemes.

The challenge is how to bring those studies that are talking about OPEs algorithms and make a classification to apply them on the standards of ITU-X800.

1.5. The Study Boundaries

The study applies cloud and implements two OPE techniques (Popa and Chenette) after comparing them and combining the OPE characteristics to build a measuring scheme which adapt the ITU-800 standard. The research is a comparative study for existing literature.

1.6. The Study Limitations

The definition of ITU X800, which is define the general security-related architectural elements that can be applied to communications systems and gives a general depiction of security and related components that can be utilized to give the services. ITU-X800 is concerned only with those visible aspects of communication path that permit networked elements to achieve secure transfer of information between them to assess conformance of any implementation to this or any other security standard (Committee, 1991). The Indistinguishability (INDs Standard) is powerful standard to present the almost any known of cryptographic objects (Nir Bitansky, 2015). The researcher limits himself with the ITU-X800 and IND to build a reliable measuring scheme component.

1.7. Thesis Outline

Chapter One: The thesis is an introduction about the OPEs algorithms, and it is concepts in addition to the aims, objectives, problem statement, 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 comparative of OPE Order-Preserving Encryption schemes that will use to investigate this thesis.

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

Chapter Four compare the recent OPE schemes and ITU-X800 standards. The results are classified to include the characteristics for OPEs measuring scheme.

Chapter Five: Presents 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

2.1. Literature review

This chapter will review the previous studies that have been achieved. Subjects that have been studied in this thesis include the OPE algorithms and their utilization in many areas, shared database service, and implementation at internet and networking environment to verify benefits and challenges.

2.2. Background

In the last decade, OPE algorithms have developed to be more powerful at security level reducing the execution time to retrieve the data from distributed system in heavy traffic networking requests.

Starting with the literature review from Popa, et. al., 2009, where he proved that mutable ciphertexts are needed for ideal security. He used a mutable ciphertext technique used for a small number of plaintext change in values. A mutable OPE was offered, the first order-preserving encoding scheme that achieves ideal IND-OCPA security, where the order of elements was based on the ciphertexts. In addition, a scheme was employed and assessed on micro benchmarks and on the context of an encrypted MySQL database application. mOPE uses the idea of mutable ciphertexts, it was shown that mutable ciphertexts are required to achieve IND-OCPA. A stronger notion of same-time OPE security that allows an adversary to learn only the order of elements was achieved to present in an encrypted database at the same time, and present an extension of mOPE, called stOPE, that achieves this stronger definition. Versions of mOPE and proof that mOPE achieves good performance both in micro benchmarks and in the context of an encrypted database running TPC-C queries, and that it outperforms the state of the art OPE scheme by 1-2 orders of magnitude were presented.

A year later, Carlo Curino, E. P. (2010) concluded that the ideal OPE object achieves one-wayness security. The outcomes exhibited in the paper give a general technique to investigating their security in addition to enhancing the comprehension of the security of OPE schemes and guide its parameter choices. The outcomes demonstrate that in spite of the fact that the discount may recover some data about the plaintext x, the likelihood for the discount to completely recover the plaintext x is an immaterial capacity of (log m) if the number h of known plaintexts/ciphertext. This was achieved through contemplating the security of OPE schemes by breaking down the plaintext that remaining parts mystery from the adversary against a known plaintext assault with h known plaintexts and proposing a scientific model to improve the OPE scheme Based on the security analysis.

Raluca Ada Popa et. al (2011) evaluation showed that chaining encryption keys to user passwords requires 11–13 unique schema annotations to secure more than 20 sensitive fields and 2–7 lines of source code changes for three multi-user web applications. It also showed that CryptDB has low overhead, reducing throughput by 14.5% for phpBB, a web forum application, and by 26% for queries from TPCC, compared to unmodified MySQL. CryptDB; a system that provides a practical and strong level of confidentiality in the face of two significant threats confronting database-backed applications was presented. CryptDB meets its goals using three ideas: running queries efficiently over encrypted data using a novel SQL-aware encryption strategy, dynamically adjusting the encryption level using onions of encryption to minimize the information revealed to the untrusted DBMS server, and chaining encryption keys to user passwords in a way that allows only authorized users to gain access to encrypted data. The author’s evaluation on a large trace of 126 million SQL queries from a production MySQL server shows that CryptDB can support operations over encrypted data for 99.5% of the 128,840 columns seen in the trace. The throughput penalty of CryptDB is modest, resulting in a reduction of 14.5–26% on two applications as compared to unmodified MySQL. The author’s analysis shows that CryptDB protects most sensitive fields with highly secure encryption schemes for six applications. The developer effort consists of 11–13 unique schema annotations and 2–7 lines of source code changes to express relevant privacy policies for 22–103 sensitive fields in three multi-user web applications.

In 2012, Alexandra Boldyreva, N. C. (2012) proposed Randomized Order Preserving Encryption (ROPE). ROPE follows the mOPE scheme by contributing haphazardness to it, in order to fulfill IND-OCPA security. The ROPE scheme actualizes embed, erase and question works on an encrypted MySQL database. OPE is a scheme that leaks nothing beyond the order. ROPE scheme grants different SQL questions to be utilized immediately on encoded information. The execution of ROPE scheme is contrasted, and the current DOPE conspire and watched that there is a question recovery time overhead. In any case, ROPE conspire renders greater secrecy and achieves the IND-OCPA security for OPE when contrasted with the current OPE scheme. The execution of ROPE scheme is contrasted and the current DOPE scheme and watched that there is a question recovery time overhead. Still, ROPE scheme renders greater privacy and achieves the IND-OCPA security for OPE when contrasted with the current OPE schemes.

In the same year, Vladimir Kolesnikov and Abdullatif Shikfa (2012) illustrated how the use of OPE may reveal information and deliberated tactics to minimize its effect. A high-level architecture of a webmail system that depend on OPE to protect client data from the web server was provided. Several of the most serious sources of insecurity were established, and how to largely mitigate their effects was projected. He proposed that the main avenue to improve privacy is to limit the type of interactions that should be allowed with a webmail server.

In 2014, several approaches and papers were proposed. Chenette et. Al designed an efficient OPE scheme and proved its security under our notion based on pseudo-randomness of an underlying block-cipher. It showed that a direct unwinding of standard security ideas for encryption, for example, lack of definition against picked plaintext assault (IND-CPA) is unachievable by a pragmatic OPE scheme. Instead, a security thought in the spirit of pseudorandom capacities (PRFs) and related Priorities asking that an OPE scheme look \as-random-as-possible" subject to the order-preserving constraint was proposed. The structure depends on a characteristic connection we reveal between an arbitrary request saving capacity and the hypergeometric likelihood conveyance. Specifically, it influences black-box to utilization of an effective examining calculation for the last mentioned.

Mavroforakis, et. Al introduced order-preserving encryption (OPE) schemes, where ciphertexts save the natural ordering of the plaintexts, permit proficient range query processing over outsourced scrambled databases without giving the server access to the decryption key. Such plans have as of late gotten expanded enthusiasm for both the database and the cryptographic groups. In particular, modular order-preserving encryption (MOPE), due to (Boldyreva et al.,2009), is a promising extension that increases the security of the basic OPE by introducing a secret modular offset to each data value prior to encrypting it. However, executing range queries via MOPE in a nave way allows the adversary to learn this offset, negating any potential security gains of this approach. In this paper, the authors efficiently address this powerlessness and demonstrate that MOPE can be utilized to assemble a functional framework for executing range inquiries on encrypted data while providing a noteworthy security improvement over the essential OPE. The authors introduce two new query execution algorithms for MOPE: our first algorithm is efficient if the user's query distribution is well-spread, while the second scheme is efficient even for skewed query distributions. Interestingly, our second algorithm achieves this efficiency by leaking the least important bits of the data, whereas OPE is known to leak the most-important bits of the data. The authors also show that our algorithms can be extended to the case where the query distribution is adaptively learned online and present new, appropriate security models for MOPE and use them to rigorously analyze the security of our proposed schemes. Finally, 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. The authors provide a performance evaluation of our prototype under a number of different database and query distributions, using both synthetic and real datasets.

Also, and during the same year, Patrick Grofig, I. H. investigated how an encrypted database can (technically) ensure privacy. He studied the use case of a mobile personalized healthcare app. The authors showed that an encrypted database can ensure data protection against a cloud service provider. Furthermore, he showed that if privacy is considered in application design, higher protection levels can be achieved, although encrypted database are a transparent privacy and security mechanism.

The Order Preserving Encryption was settled by many algorithms to support search query processing on encrypted data. Security analysis helps in understanding the level of security that is assured by an algorithm. Currently, security analysis of OPE schemes are limited. Xiao, Osbert Bastani, et al, (2014) presented the ideal OPE object and constructed an OPE scheme that is computationally indistinguishable from the ideal object. Thus, the security of proposed OPE scheme is indistinguishable to that of the perfect OPE object. In any case, the security of the perfect protest had not been investigated. In this paper. The authors considered the security of OPE scheme by dissecting the plaintext that stayed mystery from the adversary against a known plaintext assault with (h) known plaintexts.

In 2015, N.Jayashri, T.Chakravarthy, proposed the simplest way to protect data privacy is data encrypted before Prior to outsourcing / before outsourcing, but encryption also can be rephrased to makes the deployment of traditional data utilization services difficult. deploying traditional data utilization services difficult. This problem on the best way to look encrypted information has as of late picked up consideration and lead up to the improvement of accessible encryption techniques. The authors tried to execute Modular Order Preserving Encryption (MOPE), a crude which permits a proficient particular range queries on encrypted documents. This is a sort of Searchable Encryption Scheme. This is a kind of Searchable Encryption Scheme. MOPE enhances the security of OPE in the sense, as it doesn't leakage any data about the area of plaintext, Boldyvera et.al. Principle objective of this work is to enhance the security furnished by the current MOPE approaches with the assistance of Multivariate Hypergeometric Distribution (MHGD).

Benjamin Fuller, M. V. (2017) proposed a security idea in the soul of pseudorandom capacities (PRFs) and related natives asking that an OPE scheme look "as-random-as-possible" subject to the request protecting limitation after that an efficient OPE scheme and demonstrate its security under our thought in light of pseudo randomness of a basic underlying block cipher.

Kayed, et. al. 2016 was concerned with data owner, access control and data transferring process. The author made surveys to look for applications, tools, building blocks, and approaches that can be used directly to process encrypted data (i.e., without decrypting it). The investigation review gave an outline of current frameworks and methodologies that can be utilized to process encoded information, talk about business use of such frameworks, and to dissect the present improvements around there. The paper also studied both PHE and FHE schemes. The paper also studied both PHE and FHE schemes. PHE encryption schemes preserve homomorphic property which can be discussed from two different perspectives. It is seen as a shortcoming in the encryption scheme since it can't fulfill indistinguishability under versatile picked ciphertext assault (IND-CCA2) necessities, and subsequently, can be broken. For example, a picked ciphertext assault by Ahituv et al. was accounted for against a homomorphic scheme where the expansion operation is upheld. Not at all like PHE, and to beat the security issues of the present plans, a leap forward in 2009 presented by Gentry for his proposition of the FHE scheme. FHE bolsters subjective calculation over encoded information and stays secure. Regardless of Gentry's accomplishment, his approach stays exceptionally costly and impractical. Also, the authors discussed and classified several aspects of processing over encrypted data, such as functional encryption, searchable encryption, multiparty computation, and the recent industry offerings. (Salah et. al., 2016).

Sahin and El Abbadi (2017) provided a comprehensive analysis of the state-of-the-art in the context of data security and privacy for outsourced data. The paper’s aim to cover common security and privacy threats for outsourced data, and relevant novel schemes and techniques with their design choices regarding security, privacy, functionality, and performance. The authors’ explicated focus is on recent schemes from both the database and the cryptography and security communities that enable query processing over encrypted data and access oblivious cloud storage systems.

Shafagh et. al. (2015) the Authors introduced Talos, a system that stores IoT data securely in a Cloud database while still allowing query processing over the encrypted data and achieved this by encrypting IoT data with a set of cryptographic schemes such as order-preserving and partially homomorphic encryption. In order to achieve this in constrained IoT devices, Talos relies on optimized algorithms that accelerate order-preserving and partially homomorphic encryption by 1 to 2 orders of magnitude. The authors assessed the feasibility of Talos on low-power devices with and without cryptographic accelerators and quantify its overhead in terms of energy, computation, and latency. With a thorough evaluation of our prototype implementation, the authors showed that Talos is a practical system that can provide a high level of security with a reasonable overhead and envision Talos as an enabler of secure IoT applications. Then the authors presented Talos, a practical secure system that provides strong communication and data security features for privacy-preserving IoT applications. Talos leverages and tailor's cryptographic primitives that allow computation on encrypted data without disclosing decryption keys to the Cloud. To achieve this, we utilize optimized encryption schemes, specifically for the expensive additive homomorphic and order-preserving encryptions, accelerating them by 1 to 2 orders of magnitude.

Chenette, N. et. al. presented new, appropriate security models for MOPE and used them to rigorously analyse the security of our proposed schemes. They designed 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. They provide a performance evaluation of our prototype under a number of different database and query distributions, using both synthetic and real datasets. A year later, they built efficiently implementable order-revealing encryption from pseudorandom functions. They presented the first efficient Order-revealing encryption scheme which achieves a simulation-based security notion with respect to a leakage function that precisely quantifies what is leaked by the scheme. In fact, ciphertexts in our scheme are only about 1:6 times longer than their plaintexts. Moreover, they showed how composing our construction with existing Order-Preserving Encryption schemes results in order-revealing encryption that is strictly more secure than all preceding order-preserving encryption schemes.

Kadam Sandip, Kanchan Doke (2016) used processing of NN queries in an untrusted outsourced environment; i.e. (cloud), whereas at an equivalent time protective the POI and querying users' location positions. They used techniques based on mutable order preserving encoding (mOPE). It is a secure order-preserving encryption and updating database. User identity privacy in existing access control schemes Anony Control decentralizes the central authority to limit the identity leakage. The authors proposed two methods to support secure kNN query processing: VD-kNN which is based on Voronoi diagrams TkNN which relies on Delaunay triangulations. Both use mutable order preserving encoding (mOPE) for building block. VD-kNN fetch exact results, but this method's performance overhead may be high. TkNN only offers approximate NN results, but with better performance. Anonymity with Attribute-based encryption effectively for users identity (Location) and secure content (POI) in the cloud.

Tobias Boelter et. al. (2017) presented the first one-roundtrip protocol for performing range, range-aggregate, and order-by-limit queries over encrypted data that both provides semantic security and is efficient. The authors accomplished this task by chaining garbled circuits over a search tree, using branch-chained garbled circuits, as well as carefully designing garbled circuits. The authors showed how to build a database index that can answer order comparison queries. The authors implemented and evaluated our index. The authors demonstrated that queries as well as inserts and updates are efficient, and that our index outperforms previous interactive constructions. This index is part of the Arx database system, whose source code will be released in the near future. The authors constructed and evaluated the first practical, functionally rich index that allows efficient computation of standard database queries on encrypted data and they proved our scheme secure in a novel, precisely defined, and well-motivated security model.

Timo Schindler, Christoph Skornia(2016) proposed a feasible solution with Order-Preserving Encryption (OPE) and further, state of the art, encryption methods to sort and process Big Data on external resources without exposing the unencrypted data to the IaaS provider. They introduced a proof-of-concept client for Google BigQuery as example IaaS Provider. The authors had proposed different encryption algorithms which can be used with the concept besides Order-Preserving Encryption. Different data in a dataset does need different encryption algorithms depending on the projected queries and operations. This does have an impact on the design of the database scheme and can increase data security. The authors revisited the Modular Order-Preserving Encryption (MOPE) Algorithm. MOPE is slightly different to mOPE, but is also possible for an external database service to gain more information besides the order by observing the user's queries. In the author discusses three contributions to hide the user's query distribution by mixing it with another distribution.

Nasrin Dalil1 and Ahmed Kayed (2015) presented a survey's various encryption functions provided to support querying over encrypted data, especially Order Preserving Encryption. To meet the security goals for the outsourcing data; it should be outsourced as encrypted. Moreover, queries should be performed over encrypted data. There are different encryption functions which satisfy processing queries over encrypted data. Importantly, ordered encrypted data facilitate the comparisons and relation operation between data items.

Hossein Shafagh, A. H. (2017). The authors advocated the necessity of privacy and security guarantees for the paradigm of co-located storage of personal health data. The authors suggested two core security functionalities: true end-to-end encryption, such that only encrypted data is stored in the cloud and secure sharing of encrypted data, without disclosing data owner’s secret keys. They discussed the challenges in adopting such an end-to-end encryption paradigm while preserving the cloud’s basic processing functionalities over encrypted data and how to cryptographically enforce access control. The authors figured out the design space for composing such a system and the accompanying risks. They then lay down the design of our scheme to fulfill the encrypted sharing goal. They were in the process of finalizing their design and developing a reference implementation.

Harshali Anant Agutale (2015) had discussed the probabilistic OPE technique known as one-to-many OPE. The expected result is to be that cloud server cannot penetrate in actual user data and provide the search on encrypted data will be performed and results will appear in order of relevance score. Even though with good security of one-to-many OPE, the cloud can get the information of the plain text if differential attack occurred on the cipher text by calculating the differences between the cipher text. One-to-Many OPE is designed for ranked search of encrypted data over the cloud and to preserve the order of relevance scores and conceal their distributions. But as discussed in it is seen that cloud server can estimate the distribution of relevance scores by change point analysis on the differences of cipher texts of One-to-Many OPE. In future work, the author had described to improve One-to-Many OPE in two ways. One way is to divide the plaintext into several sets and divide the corresponding bucket into several sub-buckets by which some new change points will appear in the differential attack, which will cover up the original distribution of plaintexts. Another way is to add noise in the inverted index by adding some dummy documents IDs and keywords.

TimWaage (2016): The work identified the practical requirements for utilizing OPE in existing NoSQL cloud database technologies. It also provides runtime analysis of two popular OPE schemes combined with two popular NoSQL wide column store databases. The author discussed how OPE can be used in NoSQL WCSs and quantified the performance of two OPE schemes on the two currently most popular platforms. As we already did the same for a couple of schemes for searchable encryption.

Wenting Zheng, et. al. (2017): The author proposed Mimicry, the first key-value store that reconciles encryption and compression without compromising performance. At the core of MiniCrypt is an observation on data compressibility trends in key-value stores, which enables grouping key-value pairs into small *key packs*, together with a set of distributed systems techniques for retrieving, updating, merging and splitting encrypted packs. The evaluation showed that MiniCrypt compresses data by as much as 4 times with respect to the vanilla key-value store, and can increase the server's throughput by up to *two orders of magnitude* by fitting more data in main memory. The presented MiniCrypt, the first big data key-value store that reconciles encryption and compression. MiniCrypt makes an empirical observation about data compression trends and provides a set of distributed systems techniques for retrieving, updating, merging and splitting encrypted packs while preserving consistency and performance. The evaluation shows that MiniCrypt can increase the server's throughput by up to two orders of magnitude.

Chapter Three

The Methodology and Proposed Work

Overview

Chapter Three studies the guiding map for the whole parts of This thesis in order to concentrate and explain the processes of Data collections and surveying.

The methodology is based on surveying and data collecting to define a measuring scheme for schemes of OPEs and to build a clear vision about these schemes. After that, data will be comparing and classified to show all the characteristics of each scheme.

3.1. Introduction:

Many experts studied the development of the security systems in the local areas of network and internet environments. The OPES schemes are vital for "DB "outsourcing in the cloud computer paradigm.

This thesis studies almost all the OPES schemes in detailed and put a strategy in order to compare and classify each part of it. But there is no classification for this type of schemes so the goal of my research is to build a measuring scheme by selecting all the studied articles to create one

This thesis is based on the comparative studies where the surveys in this domain cover from the period from 1991 to 2017.

This thesis borrows the main characteristics of general Encryption techniques summarized in the ITU-X800 framework and adding IN Distinguishability Standard characteristics. This frameworks has been enhanced by analysing the applicability of these characteristics over the existing OPES schemes.

Section 3.1. Clarifies this thesis methodology and introduces their steps and structure in order to describe the proposed methodology. The proposed methodology consists of five steps started with the surveying stage which will present all the articles in OPEs domain which have been studied in Section 3.2. Section 3.3 will analyse and explain the technique of analysis which will be based on classifying authors who studied the OPEs schemes and also based on classifying the characteristics of OPE schemes themselves. Finally, 3.4 and 3.5 will explain the proposed measuring scheme according to these classifications.

3.1. The Methodology

The term of methodology defines as a method section describes actions to be taken to investigate a research problem and the rationale for the application of specific procedures or techniques used to identify, select, process, and analyse information applied to understanding the problem, thereby, allowing the researcher to critically evaluate a study’s overall validity and reliability (Kallet, 2004).

There are several major research approaches for methodologies. They are quantitative research, qualitative research, and mixed research (Creswell, 2003). Here are the

This thesis adapted the quantitative research’s methodology and in specific an experimental research methodology since this thesis studied and surveyed the ITU-X800 characteristics, OPEs schemes and INDs Standards properties.

The methodology of this thesis will answer two questions: How was the data collected or generated? And, how was it analysed. This will be answered in section (3.3).

Collect three surveys, OPEs schemes from articles, ITU-X800 characteristic from International Telecommunication Union book, and INDs standards from the articles as well.

3.2. The Proposed Work

The Proposed work of this thesis includes five steps:

1. Collecting characteristics from surveyed OPES articles to find out the characteristics by using ITU-800 and IND standards.
2. Comparing which will find out repetitions of these characteristics for each article.
3. Classification of the second step results.
4. Extracting and deciding which characteristics are applicable for OPEs Measuring Scheme.
5. Evaluating the Measuring Scheme and applying the existing OPEs schemes to find the best one.

All these steps are summarized in figure Fig 3.1. These steps will be described in details in the following sub-sections.

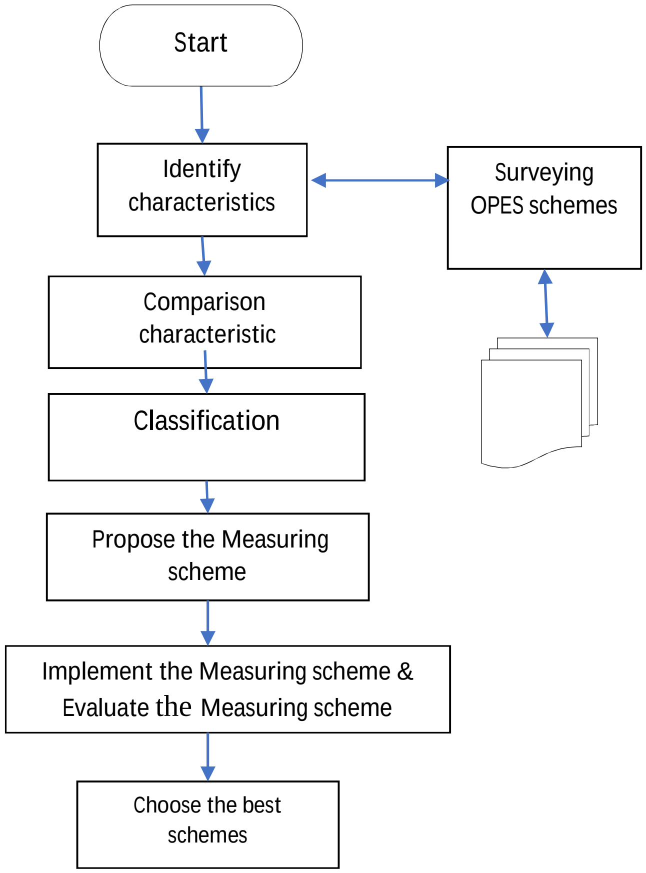

Start
Identify characteristics
Surveying OPES schemes
Comparison characteristic
Classification
Propose the Measuring scheme
Implement the Measuring scheme & Evaluate the Measuring scheme
Choose the best schemes

Figure. 3-1 The Road Map for the Proposed Research Methodology

3.3. Surveying OPEs Scheme

This thesis collects almost all papers in the domain of OPEs by studying three main surveys which covered the period (1991-2017). From these surveys there were 30 articles that have been selected since they covered almost all characteristics of OPES. This goal is achieved by finding ITU-X800 characteristics from the articles. Then finding ITU-X800 characteristics from the articles' scheme (3) and by finding IND standards from the articles schemes (Agrawal R, 2004).

Two frameworks have been studied, which are ITU-X800 characteristics and INDs standards. ITU-800 is general security frameworks while and IND-CPA (in distinguishability under chosen plaintext attack) framework focuses on OPEs characteristics proposed by Popa, and Chettene (Bebek. G, 2002).

Main properties of IND-CPA is

> The main properties of IND-CPA that the schemes are manipulate part of the cryptography's process. OPES leak some information, but they support the effect of encryption over database. The security protocol that are done by OPE schemes is named in distinguishability- against Chosen Plaintext Attack (IND-CPA). This security protocol presents that the cipher text cannot disclose anything about the plaintext value w without their order. Most OPES cannot satisfy all standards notions of this security protocol IND-CPA since most OPES used deterministic encryption techniques and leak the order-relations among the plaintexts. Therefore, it is important for each application to choose the best security protocol that it requires (Boldyreva, Chenette, Lee & O'Neill, 2009).

The main OPEs characteristics and their techniques have been extracted and compared with the ITU-800 and IND standards. The ITU-800 is International Telecommunication

Unit in 1991 and other references. This thesis also studied these articles the characteristics and converted them into three main tables. Table 3.1 summarized all authors who wrote in OPES and see if the ITU characteristics have been discussed in their papers. The Table 3.2 summarized the schemes and see if the ITU characteristics are applied on these schemes. The Table 3.3 summarized the schemes and see if the IND characteristics are applied on these schemes. All previous studies built their methodologies to solve certain problems and add a new technique to the OPES algorithm to improve the security part (key generation in one side and performance of OPES itself in other side) and to achieve under certain environments (Cloud, LAN, and Distributed database).

38 characteristics have been chosen from 59 characteristics listed in ITU-800. The rest of 59 are either a branch of the main 38 characteristics or refers to one of the main 38 characteristics. Applying these 38 characteristics on OPEs using the articles that explained them is not an easy process. Each author explains and comprehends these characteristics sometimes in different ways. This thesis reads carefully these articles to decide if the 38 characteristics are applied on OPEs or not. The results of these steps have been concluded in three tables. These tables will be described briefly in section 3.4 and details in chapter 4.

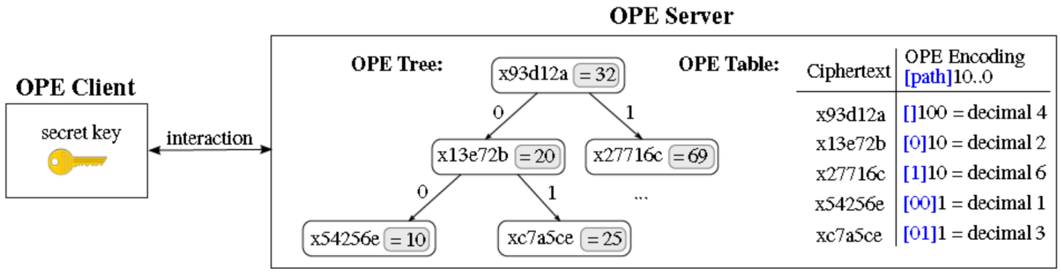
In This thesis we explain how 4 schemes work as an example of scheme work

1. **Raluca Ada Popa, Frank H. Li, Nickolai Zeldovich "An Ideal-Security Protocol for Order-Preserving Encoding"**

   Popa and her team presented a new scheme which is based on mutable OPE. This scheme is dealing with encrypted words and standard encryption scheme. The scheme contributed to implement the ideal security of OPE which is named IND-OCPA for no exceptional of order values, and to present the requirement of mutability to achieve the ideal security and also contributed to increase the strength of security in database system by implementing same-time OPE security (stOPE) that learns the order of items present in the database at the same time. Also, the authors created a searching tree in mOPE which is contained the plaintext values encrypted by the application. The tree length is equal the path encoding. The authors implemented mOPE and stOPE to understand how they work and how to improve their performance.

The authors built their scheme to be consisted of two parts OPE client and OPE server. The client has encrypted data to send it to the server. The server is not trusted part and has passive and active threat, then they classified thirteen OPE schemes into two classes (guarantee and not). They focused on not guarantee schemes to increate the passive threat.

Accordingly, the figure below illustrates the authors' scheme that shows the private key in the OPE client side and the cipher-tree which is defined to be in the OPE server. The client helps the server to find the location inside the tree and the server will encrypt client's plaintext based on the tree. The authors created an algorithm to implement mOPE tree traversal process.



Ciphertext	OPE Encoding [path]10..0
x93d12a	[]100 = decimal 4
x13e72b	[0]10 = decimal 2
x27716c	[1]10 = decimal 6
x54256e	[00]1 = decimal 1
xc7a5ce	[01]1 = decimal 3

Figure: shows data structure of mOPE scheme

Popa's team submitted about two theorems, four definitions, and implemented about 12 algorithms to support their mOPE scheme. All of these are distributed as the following as:

Definition (1): described about the processing of mOPE encryption as the sequence (Key generation, Initializing server state (busy, ready, ..etc.), Encryption, Decryption, Ordering at the server. This definition is implemented by 5 algorithms

Definition (2): described the correctness of definition (1)'s parameters.

Definition (3): described the related mOPE with the standard indistinguishability under an ordered chosen-plaintext attack (IND-OCPA) to be equivalent to the mOPE.

Theorem (1): is the authors' scheme that mOPE is IND-OCPA secure. The authors proofed that in their paper.

Theorem (2): is to trace almost all stateful schemes within the protocol IND-OCPA to apply ciphertext size in the plaintext size. The authors proofed that in their paper. They designed six algorithms to implement their idea.

Definition (4): is specified to store and order the encrypted queries which are stored in the server side. The six algorithms in theorem (2) will be as input values in stateful schemes. This definition is supporting the correctness requirements.

The authors built a strong database in the server to be the best of other schemes like BCLO and CryptDB because mOPE does not leak any information besides order. They used MySQL database to implement their scheme.

The author evaluated their scheme by the results which were given from the following aspects:

- Experimental setup
- Throughput
- Storage and ciphertext sizes
- Ciphertext update cost

2. Alexandra Boldyreva, Nathan Chenette, Younho, Lee, Adam O'Neillx, “Order-Preserving Symmetric Encryption”

The authors based on the **LazySample, LazySampleInv cryptography algorithms** to enhance the following aspects:

- **The encryption and decryption procedures:** The two cryptography algorithms cannot change from encryption to decryption procedure directly because the two algorithms share and store join state of the random keys which are came from hypergeometric (HG) algorithm. The authors replaced the join state by implementing subroutine GetCoins which is named to TapeGen for generating pseudorandom keys (PRF). The author suggested to solve this problem by composing the variables of input and output lengths and made them as one block. Then, they proofed their theorem by associating the two variables.
- **The random of key generation:** The authors suggested a new theorem to deal with the block-text and block-cipher by using a pseudorandom function and they proofed it in their paper.

The security of OPE: the authors suggested a theorem to make the scheme as a POPF-CCA secure. They proofed by applying the previous theorem which is reduced to pseudo-randomness of an underlying block-cipher. The efficiency of the scheme follows from the suggested implementation of TapeGen by encryption and decryption required time for at

most logN + 1 invocations of HG on inputs of size at most logN plus at most
(5 logM + 12).(5 logN + λ + 1)=128 invocations of AES on average for λ in the theorem.

3. **Charalampos Mavroforakis, Nathan Chenette, Adam O'Neill, George Kollios, Ran Canetti, "Modular Order-Preserving Encryption, Revisited"**

The authors focused to build a cryptography system in which any client can store encrypted files in untrusted server. They planned to build MOPE schemes which achieved the security and efficiency system. They proposed scheme consists of the following three parts:

1. Clients: the main jobs are sent queries to proxy server and received answers from proxy server.
2. Proxy Server: is a trusted server which sends to DB server two types of queries (real and not real) by combing them together.
3. Database Server (PostgreSQL server): is not trusted server which will receive the encrypted queries. The server will decrypt the queries by secret key then will send the requested answers back to the proxy server after encrypted them by the server.

The authors applied very important algorithms which contributed to solve the suggested problem and the algorithms are as following as:

1. Uniform Query Algorithm: This algorithm will unify the distributed queries that will solve two problems: (i) not unify queries; (ii) security offsetting.
2. Periodic Query Algorithm: The authors implemented this algorithm to avoid the inefficiency of the uniform query algorithm. Also, the algorithm will reduce the reduce the size of the histogram that is used to generate the fake queries.

Finally, the authors showed five theorems to improve the two algorithms and they proofed them in their paper. The authors evaluated the performance of scheme by using TPC-H benchmark.

4. Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing"

Popa's team presented two problems which are related to the confidentiality and reducing data leakages. The authors suggested to solve these problems by using CryptDB scheme. The CryptDB scheme executes strategy of SQL encryption which can verify the symmetric keys. They discussed the adjustable query encryption for reducing the leakage of information by implementing the CryptDB in SQL query encryption scheme. The third idea is to generate a chain of passwords to the users' queries for increasing the confidentiality properties.

All the above, Popa's team worked to present new ideas for improving CryptDB to achieve the best confidentiality in the DBMS. They focused on two threats which mentioned from CrpytDB. The following threats are described in detailed to show the strength points of CrptyDB as:

1. Arrangement of Database Server Threat:

   The authors assumed that the database inside the proxy sever is not protected enough so that CrpytDB encrypts the queries and the transferred data between the user and DB server. The encryption process is used a secret key to encrypt the queries.

2. Arbitrary threats:

   The authors described this case because logined users attack their data arbitrarily. To solve this case, the author built their scheme among application, proxy, and SQL server configurations. The encryption process in the first threat is not enough to solve so that CryptDB scheme arranges and follows the logined users and any intruder will erase it.

The authors built the CryptDB scheme inside the proxy server because it is trusted server and it will store all users' secret keys. The CryptDB scheme works in four steps; (i) the query is encrypted by secret key which is generated from random function (ii) The proxy traces the SQL server before executing the encrypted query. The authors used the AES to apply the equality in encryption and decryption length size and then used the OPE because it is strong in encryption. (iii) The proxy server pushes the encrypted query to the SQL server. The proxys' responsibilities are very important because the authors implemented about 18,000 lines of C++ to execute the functions of CryptDB scheme and secured the transferred queries between proxy server and SQL server. All related protocols in indistinguishability are implemented to achieve the standardization of protections (iv) The SQL server sends the required query as a result of the process to proxy server.

The authors evaluated the results of CryptDB scheme which is consisting of the four parts as follows as:

1. The improving challenges:
2. The security level of CryptDB scheme
3. The CryptDB performance
4. The query types and how are applied in CryptDB scheme.

According to the author’s analysis, the authors showed that CryptDB is very good scheme for encryption and it is very sensitive in the privacy policies and Multi-user web applications.

3.4. Comparison characteristics

The results of the three tables will present the variances of the 38 characteristics of articles and schemes which based on ITU-X800 characteristics INDs standards. The first (Table 3.1) is called “Author Table”. This table is a cross matrix between authors who studied OPEs schemes and the ITU-X800 38 characteristics. For each 38 characteristics, Table 3.1 decides if the authors studied or not this characteristic. A sample of Table 3.1 is presented below. Full detailed are presented in chapter 4.

Table 3.1 Sample illustrating the authors table and 38 ITU-X800 characteristics

Seq.	Paper Author	ITU-X800 characteristics				
		Access control	**Authentication**	**Authorization**	**Cryptography**	**Key Management**
1.	Chenette et., al. (1)	✓	✓		✓	
2.	Fuller et. Al	✓	✓	✓	✓	
3.	Popa et., al.	✓			✓	
4.	Sahin	✓		✓	✓	
5.	Chenette et., al. (2)	✓			✓	✓
6.	Kayed et., al.	✓	✓		✓	✓

Table 3.1 distributes the articles' scheme on same 38 characteristics which reflect all schemes characteristics. Table 3.2 is called "Schemes Table". This table is a cross matrix between schemes who discussed OPEs schemes and the ITU-800 38 characteristics. For each 38 characteristics, Table 3.2 lists all references that discussed this characteristic using reference number. These references with their numbers are detailed in chapter 4 in Table 4.6. Sample of Table 3.2 is listed below.

Table 3.2 Sample Illustrating the Schemes Tables Shows schemes Sharacteristics with Their References

Seq.	Schemes	ITU-X800 characteristic				
		Access control	**Authentication**	**Authorization**	**Cryptography**	**Key Management**
1.	Random OPE [9]				9,23	9,23
2.	OPE's Chenette scheme [1]	1,11, 19, 20	1,11, 19, 20	19,20	1,11, 19,20	1,11,20
3.	Mutable OPE [17]	6,7, 10, 15	6,7, 10, 15	6,7, 10, 15	6,7,10, 15, 17	6,7, 10 15, 17
4.	Modular OPE scheme [5]	5, 13			5 ,13	5, 13
5.	CryptDB scheme[16]	3,4,21,16	4,16, 21, 28	4,16, 21, 28	3,4,14,16,21 ,28, 30	4,14, 16,21,28, 30
6.	MiniCrypt [27]	27			9,23	27

These two tables will show the volume of work and it will be easy to find which the characteristics should be used to improve a certain scheme and which characteristics should be used to build a certain measuring scheme. The third Table 3.3 is same as the second table but the researcher used The IND standards instead of ITU characteristics to explore to the number of scheme which are used the IND standards or protocols. Sample of Table 3.3 is presented below. This table is very important which will help us to build the measuring scheme and to classify the characteristics. The characteristics will be classified from very important in the case if it has large number of references and very low if it the number of references is very small.

Table 3.3 Sample Illustrating the Authors' Schemes and Their IND Standards

Seq.	**Schemes**	**INDistinguishability standards**				
		IND-CPA	**IND-CCA**	**IND-CCA1**	**IND-CCA2**	**IND-CCA3**
1.	Random OPE [9]	23,24	9,23,24	9,23	9,23	9,23
2.	OPE's Chenette scheme [1]	1,11, 12, 20	1,11,20	1,11,20	1,11,20	1,11,20
3.	Mutable OPE [17]	6,7,15,22, 28	6,7,15, 17	6, 7,15, 17	6,7,15, 17	6,7,15, 17
4.	Modular OPE scheme [5]	14	5,13	5,13	5,13	5,13
5.	CryptDB scheme[16]	4,16,29	4,16,29	4,16,29	4,16,29	4,16,29
6.	MiniCrypt [27]	30	30	30	30	30

This thesis collected the main keywords of all the related ITU-X800 characteristics and summarized them in Table 4.7 which will be presented in chapter 4.

3.5. Classifications:

This thesis classified the characteristics after analyzing the results of the above tables. The classification will be based on fact that how many the characteristic is repeated in these articles. The classification levels are consisting of three levels from high to low levels (A, B, and C). The next chapter will show more details about that. The classification will show up some of characteristics which are very important to build any OPES’s measuring scheme. The measuring scheme could be used to enhance the ability to use, compare understand, study, evaluate, and create OPEs schemes and characteristics.

3.6. Implementation and Evaluation:

This part of methodology will present the results of measuring schemes implement and what the research has achieved to solve these problems. The measuring scheme will show how to decide if a scheme is good or not by applying the classification on that scheme. It will also be helpful for any new OPEs schemes where the good schemes should confirm as much as possible to these characteristics. The recommendations of This thesis will be discussed in chapter 5.

Chapter Four

Implementation and Discussion

Overview

This chapter applies the methodology that has been explored in chapter 3. The chapter will present in details the 30 articles that have been used to develop the measuring scheme. The articles discussed in details the OPES schemes. The chapter will illustrate the weakness and strength of these schemes which based on the ITU-X800 and IND standard.

Chapter four organized as follow: Section 4.1. will identify the ITU-X800 characteristics with Indistinguishability Standards. Section 4.2 will Surveying OPEs Scheme the tables of previous section and describe the steps which is followed to do this process. Section 4.3 will present the researcher’s work results of data collections, surveying and analysis processes.

4.1. ITU-X800 characteristics and Indistinguishability Standards

4.1.1 ITU-X800 Characteristics

The ITU-X800 is a well-known International Telecommunication Union (recommendation 800 was a study group consists of 59 characteristics. This thesis has selected the most important characteristics from these 59. The selection criteria where based on two reasons. The first reason is choosing the main characteristics and ignoring the sub-characteristics unless the sub-characteristics are essential to define the main characteristic. The second reason is removing any repeating characteristic. Some characteristics have been included in another characteristic so we choose only the main ones. From that we end with 38 characteristics. These characteristics are: (Stallings, 2005), (Committee, 1991)

ITU-X800 Characteristics
Access control, Accountability, Active threat, Audit, Authentication, Authorization, Availability, Capability, Channel, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Denial of service, Digital signature, Encryption, Key management, Manipulation detection, Masquerade, Notarization, Passive threat, Password, Physical security, Repudiation, Privacy, Routing control, Security policy, Security service, Selective field protection, Sensitivity, Traffic analysis, Traffic flow confidentiality, Trusted functionality

4.1.2. Indistinguishability Standards

The IND-CPA is an attack model for cryptanalysis which the attacker can obtain the ciphertexts for arbitrary plaintexts. (Anderson, 2001). The goal of the attack is to gain information that reduces the security of the encryption scheme.

The IND-CPA is essential in our framework since these characteristics are essential for OPEs. We choose 8 from 10 characteristics using the same criteria for choosing ITU-800. These characteristics are:

Seq.	The Standards Name	Characteristics
1.	Indistinguishability	IND-CPA, IND-CCA, IND-CCA1, IND-CCA2, IND-CCA3, IND-CCVA INT-PTXT, INT-CTXT

Indistinguishability definition is a circular secure scheme which is based on a probabilistic asymmetric key encryption scheme. If an encryption system contains the property of indistinguishability, then an adversary will be unable to distinguish pairs of ciphertexts based on the message they encrypt.

4.1.2.1 Relations Among Characteristics (Mihir Bellare,2000)

Protection objectives for symmetric encryption plans incorporate lack of definition and non-flexibility, every one of which can be considered under either picked plaintext or (versatile) picked ciphertext assault, prompting four thoughts of security we truncate IND-CPA, IND-CCA, NM-CPA, NM-CCA. (The first denitions were in the symmetric setting yet can be "lifted" to the symmetric setting utilizing the encryption prophet). The relations among these thoughts are surely knew. (These papers state comes about for the asymmetric setting, it is a simple exercise to exchange them to the symmetric setting). The author consider two thoughts of uprightness (them utilize the terms realness and respectability exchange capably) for symmetric encryption plans. INT-PTXT (respectability of plaintexts) requires that it be computationally infeasible to create a ciphertext decoding to a message which the sender had never encoded, while INT-CTXT (trustworthiness of ciphertexts) requires that it be computationally infeasible to deliver a ciphertext not already delivered by the sender, paying little mind to regardless of whether the hidden plaintext is "new." (In the two cases, the foe is permitted a picked message assault.) The first of these ideas is the more characteristic security necessity while the enthusiasm of the second, more grounded thought is maybe more in the suggestions them discuss below:

These thoughts of credibility are without anyone else's input very disjoint from the ideas of protection; for instance, sending the message free with a going with (solid) MAC accomplishes INT-CTXT however no sort of security. To make for helpful correlations, we consider every idea of legitimacy combined with IND-CPA, the weakest thought of security; in particular the ideas on which we center for examination intentions are INT-PTXT ^ IND-CPA and INT-CTXT ^ IND-CPA. (Read "^" as "and".)

Figure 1 shows the diagram of relations between these ideas and the previously mentioned more established ones in the style of implication. A "implication" A→ B implies that each symmetric encryption plot meeting idea A likewise meets thought B. A "separation" A≠ B implies that there exists a symmetric encryption plot meeting idea A however not thought B. (This under the negligible presumption that some scheme meeting idea A exists since generally the inquiry is debatable.) Only an insignificant arrangement of relations is expressly demonstrated; the connection between any two ideas can be gotten from the indicated ones. (For instance, IND-CCA does not infer INT-CTXT ^ IND-CPA on the grounds that something else, by following arrows, we would get IND-CCA→INT-PTXT ^ IND-CPA repudiating an expressed partition.) The spotted lines are indications of existing relations while the numbers commenting on the dim lines are pointers to Propositions.

A few points may be worth highlighting. Integrity of ciphertexts even when coupled only with the weak privacy requirement IND-CPA merges as the most powerful notion. Not only does it imply security against chosen-ciphertext attack, but it is strictly stronger than this notion. Non-malleability whether under chosen-plaintext or chosen-ciphertext attack does not imply any type of integrity. The intuitive reason is that non-malleability only prevents the generation of ciphertexts whose plaintexts are meaningfully related to those of some challenge ciphertexts, while integrity requires it to be hard to generate ciphertexts of new plaintexts even if these are unrelated to plaintexts underlying any existing ciphertexts. Finally, INT-PTXT ^ IND-CPA does not imply INT-CTXT ^ IND-CPA.

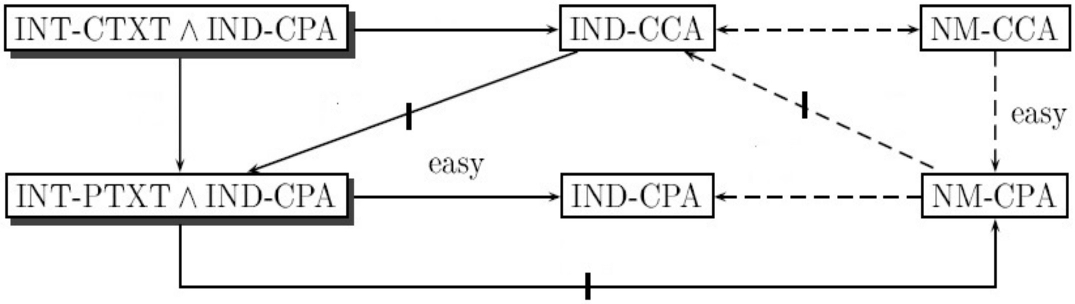


Figure 4.1: Shows the Diagram of Relations Between IND-CPA and INT-TXT

4.2. Surveying OPEs Scheme

4.2.1 Comparison characteristics

As the researcher mentioned in chapter 3, After the researcher identified the characteristics required by ITU-X800 and IND standard The author surveyed the data available in the main articles and compare the characteristics of the article in terms of one of the author and the importance of each author, then extracted the characteristics as shown in Table 4.1. The table shows these articles by author first column and ITU characteristics in the header of table. The researcher chooses the character (✓) to indicate that characteristic is available inside the text of article otherwise the box is empty. For example, the researcher compared a reference's methodology to find the characteristic "Authentication". If the researcher finds it, make (✓) otherwise left it empty. In the end, the researcher counted each characteristic in the last row to know how many papers discussed those characteristics.

Table 4.1 Part (1) - The authors' Articles and their Mentioned Characteristics-ITU-X800

Seq.	Paper Author	International Telecommunication Union – X800																		
		1. Access control	2. Accountability	3. Active threat	4. Audit	5. Authentication	6. Authorization	7. Availability	8. Capability	9. Channel	10. Ciphertext	11. Cleartext	12. Confidentiality	13. Credentials	14. Cryptanalysis	15. Cryptography	16. Data integrity	17. Data origin authentication	18. Decryption	19. Denial of service
1.	Chenette et., al. [1] 2009	✓		✓		✓				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
2.	Fuller et. al 2017	✓		✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	
3.	Popa et., al. 2009	✓		✓							✓	✓	✓	✓	✓	✓	✓	✓	✓	
4.	Sahin 2015	✓		✓			✓	✓			✓	✓			✓	✓	✓	✓	✓	
5.	Chenette et., al. (2) 2015	✓									✓	✓			✓	✓	✓	✓	✓	
6.	Kayed et., al. (1)2016	✓		✓		✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	
7.	Hossein Shafagh	✓	✓	✓			✓		✓	✓	✓				✓	✓		✓	✓	
8.	Jan Mohd Najar (2015)	✓				✓	✓	✓			✓		✓		✓	✓	✓	✓	✓	
9.	Reddy [9]			✓							✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10.	Kadam	✓				✓	✓				✓				✓	✓			✓	
11.	Xiao et., al [11]	✓		✓							✓	✓	✓	✓	✓	✓	✓	✓	✓	
12.	Harshali et al., 2017										✓	✓	✓		✓	✓			✓	✓
13.	Jayashri 2015	✓		✓				✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
14.	Chenette et., al. 2016										✓	✓			✓	✓	✓	✓	✓	
15.	Grofig et., al 2014	✓					✓	✓			✓		✓		✓	✓	✓	✓	✓	
16.	Popa et., al.[16], 2011	✓		✓		✓	✓	✓			✓	✓	✓		✓	✓	✓	✓	✓	
17.	Popa et., al.[17], 2013	✓		✓		✓	✓	✓			✓	✓	✓		✓	✓	✓	✓	✓	
18.	Rima 2016	✓				✓					✓	✓	✓		✓	✓	✓	✓	✓	
19.	Abdullatif Shikfa	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
20.	Agutale 2015										✓				✓	✓			✓	
21.	Nasrin Dalil, Kayed 2015	✓			✓	✓	✓	✓			✓		✓		✓	✓	✓	✓	✓	
22.	Hithnawi et. al. 2015	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
23.	Chenette et., al. (3) 2011										✓	✓			✓	✓	✓	✓	✓	
24.	Tobias Boelter et. al. (2017) [24]	✓		✓							✓	✓			✓	✓			✓	
25.	Timo Schindler (2016) [26]	✓						✓			✓			✓	✓	✓			✓	
26.	Gadekar	✓			✓	✓	✓				✓			✓	✓	✓	✓	✓		
27.	Wenting Zheng, et. al. (2017) [27]	✓		✓				✓					✓			✓			✓	
28.	Tim Waage 2016 [28]			✓		✓	✓					✓	✓		✓	✓	✓		✓	
29.	Ms. Omar [29]	✓									✓	✓			✓	✓			✓	
30.	Mr. Bazoon [30]		✓								✓	✓			✓	✓			✓	
The total		23	2	16	3	13	13	12	4	5	28	21	18	10	29	30	21	22	29	2

Table 4.1 Part (2) - The Authors' Articles and Their Mentioned Characteristics-ITU-X800

Seq.	Paper Author	International Telecommunication Union – X800																		
		20. Digital signature	21. Encryption	22. Key management	23. Manipulation detection	24. Masquerade	25. Notarization	26. Passive threat	27. Password	28. Physical security	29. Privacy	30. Repudiation	31. Routing control	32. Security policy	33. Security service	34. Selective field protection	35. Sensitivity	36. Traffic analysis	37. Traffic flow confidentiality	38. Trusted functionality
1.	Chenette et., al. [1] 2009		✓		✓		✓	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓
2.	Fuller et. al 2017		✓		✓		✓	✓	✓	✓	✓		✓	✓	✓	✓		✓		✓
3.	Popa et., al. 2009		✓					✓		✓	✓			✓	✓	✓				✓
4.	Sahin 2015		✓					✓		✓	✓			✓	✓	✓				✓
5.	Chenette et., al. (2) 2015		✓	✓	✓						✓			✓	✓		✓			
6.	Kayed et., al. (1)2016	✓	✓	✓	✓	✓		✓		✓	✓			✓	✓	✓		✓	✓	✓
7.	Hossein Shafagh		✓	✓						✓	✓			✓	✓	✓	✓			✓
8.	Jan Mohd Najar (2015)	✓	✓	✓			✓	✓	✓	✓	✓				✓					
9.	Reddy [9]		✓				✓	✓		✓		✓				✓		✓	✓	✓
10.	Kadam		✓	✓						✓	✓			✓	✓					✓
11.	Xiao et., al [11]		✓					✓		✓				✓	✓	✓		✓	✓	✓
12.	Harshali et al., 2017		✓	✓						✓	✓				✓	✓	✓		✓	
13.	Jayashri 2015	✓	✓		✓			✓		✓	✓			✓	✓	✓		✓	✓	✓
14.	Chenette et., al. 2016		✓	✓							✓			✓	✓					✓
15.	Grofig et., al 2014		✓	✓					✓		✓			✓	✓	✓		✓	✓	
16.	Popa et., al.[16], 2011		✓	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓		✓	✓	✓
17.	Popa et., al.[17], 2013		✓	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓		✓	✓	✓
18.	Rima 2016		✓											✓	✓	✓			✓	✓
19.	Abdullatif Shikfa	✓	✓				✓	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓
20.	Agutale 2015		✓	✓						✓	✓					✓	✓			✓
21.	Nasrin Dalil, Kayed 2015		✓	✓						✓	✓			✓	✓	✓	✓			✓
22.	Hithnawi et. al. 2015		✓	✓				✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓
23.	Chenette et., al. (3) 2011		✓	✓							✓			✓	✓		✓			✓
24.	Tobias Boelter et. al. (2017) [24]		✓	✓				✓		✓	✓			✓	✓	✓	✓			
25.	Timo Schindler (2016) [26]		✓	✓						✓	✓				✓	✓				✓
26.	Gadekar		✓	✓						✓	✓			✓	✓	✓				✓
27.	Wenting Zheng, et. al. (2017) [27]		✓	✓				✓						✓	✓	✓	✓			✓
28.	Tim Waage 2016 [28]		✓	✓				✓		✓	✓			✓	✓					✓
29.	Ms. Omar [29]		✓	✓					✓	✓	✓			✓	✓	✓				✓
30.	Mr. Bazoon [30]		✓	✓						✓	✓			✓	✓	✓				✓
	The Total	**4**	**30**	**21**	**7**	**1**	**7**	**16**	**7**	**24**	**26**	**1**	**4**	**25**	**28**	**24**	**8**	**11**	**12**	**25**

Also, the researcher repeated the same process to extract Table 4.2 to explore the relationship between the articles' scheme and their characteristics. Table 4.2 shows the same characteristics in the header of the table and the names of schemes in the first column. The indication here is the number of article inside the table to show that the characteristic is available in text of articles otherwise the box will be left it empty. In this table, the researcher also counted each how many times the schemes discussed each characteristic. Also in the same table, the researcher counted how many papers discussed each scheme. For example, the table discussed the Popa's scheme (CryptDB scheme) in four articles. Each article discussed about same characteristic (Access control) of Popa's schemes in the articles 3,4,16 and 21 in Table 4.2 The researcher found four papers that discussed Popa's scheme. The researcher processed the same with the other schemes.

This section will present the researcher's work results of data collections, surveying and comparative processes**.**

Table 4.2 (Part 1) - The Authors' Scheme and Their Mentioned Characteristics-ITU-X800

Seq.	Paper Scheme	International Telecommunication Union – X800																		
		20. Access control	21. Accountability	22. Active threat	23. Audit	24. Authentication	25. Authorization	26. Availability	27. Capability	28. Channel	29. Ciphertext	30. Cleartext	31. Confidentiality	32. Credentials	33. Cryptanalysis	34. Cryptography	35. Data integrity	36. Data origin authentication	37. Decryption	38. Denial of service
1.	Random OPE [9]										9, 23	9, 23	9		9, 23	9, 23	23	23	9, 23	
2.	OPE's Chenette scheme [1]	1,11, 19, 20		19	19	1,11, 19, 20	19, 20	19, 20	19	19, 20	1, 11, 19, 20	1,11 19,2 0	19 20	19	1,11, 19,2 0	1,11, 19,2 0	19	19	1,11, 19, 20	
3.	Mutable OPE [17]	6,7, 10, 15		7,17		6,7, 10, 15	6,7, 10, 15	7,15	7	7	6,7,1 5,10, 17	6, 7, 15, 17	6,7,1 5, 17		6, 7, 15,1 0 17	6,7,1 0, 15, 17			6, 7,10 15, 17	
4.	Modular OPE scheme [5]	5, 13		5	5, 13			5,13	13		5, 13	5, 13	5,13		5, 13	5 ,13			5, 13	
5.	CryptDB scheme[16]	3,4,21, 16	30	3,4,16, 28	21	4,16, 21, 28	4,16, 21, 28	4,16, 21			3,4,14, 16,21, 30	3,14, 28, 30	3,16, 21, 28	3	3,4,14, 1621, 28, 30	3,4,14, 16,21, 28, 30	3,14, 21, 28	3,14, 21	3,4,14, 16,21, 28, 30	
6.	MiniCrypt [27]	27		27				27					27			27			27	
7.	half-gate garbling scheme [24]	24		24							24	24			24	24			24	
8.	OPE scheme, Popa 2016[25}	29				25	25	25			25,29	29	25		25,29	25,29			25,29	
9.	Fully Homomorphic Encryption OPE	18, 22		22		18, 22	22	22	22	22	18,2 2	18, 22	18, 22	22	18, 22	18, 22	18, 22	18, 22	18, 22	
10.	ORAM Scheme	2,4		2,4			2,4	2,4			2,4	2,4			2,4	2,4	2,4	2,4	2,4	
11.	Multi-Round Encryption Algorithm	8, 26			26	8, 26	8, 26	8			8, 26		8	26	8, 26	8. 26	8, 26	8,2 6	8	
	The no. of articles	23	1	13	5	17	16	15	4	4	28	22	19	4	28	29	12	11	29	0

Table 4.2 (Part 2) - The Authors' Scheme and Their Mentioned Characteristics-ITU-X800

Seq.	Paper Scheme	International Telecommunication Union – X800																			
		Digital signature	Encryption	Key management	Manipulation detection	Masquerade	Notarization	Passive threat	Password	Physical security	Privacy	Repudiation	Routing control	Security policy	Security service	Selective field protection	Sensitivity	Traffic analysis	Traffic flow confidentiality	Trusted functionality	The Total of scheme
1.	Random OPE [9]		9, 23	9, 23							23			9, 23	23		23			9, 23	**2**
2.	OPE's Chenette scheme [1]	19, 20	1, 11, 19, 20	1, 11, 20			19	19		19	1, 11,19, 20		19	1, 11, 19,20	19	19, 20		19	19	19, 20	**4**
3.	Mutable OPE [17]	6	6, 7,10,15, 17	6,7, 10 15, 17				6,7, 17	15	10	6, 7,10,15, 17			6,7,10 15, 17	10	6,7, 15, 17				6,7,10, 15 17	**5**
4.	Modular OPE scheme [5]		5, 13	5, 13							5, 13			5, 13							**3**
5.	CryptDB scheme[16]		3,4,14,16, 21,28, 30	4,14, 16,21,28, 30				3,4,16, 28		3, 21, 28, 30	3,4,14, 16,21, 28 ,30			3,4,14,16,21, 28, 30	3, 14 21,28 30	3,4,1621, 30	21			3,4,14,16,21, 28, 30	**7**
6.	MiniCrypt [27]		27	27				27						27	27	27	27			27	1
7.	half-gate garbling scheme [24]		24	24				24		24	24			24	24	24	24				**1**
8.	OPE scheme, Popa 2016[25}		25,29	25,29					29	25,29	25,29			29	29	29				25,29	**2**
9.	Fully Homomorphic Encryption OPE		18, 22	22				22	22	22	22		22	18,22	18, 22	18, 22		22	18, 22	18,22	2
10.	ORAM Scheme		2,4					2,4		2,4	2,4			2,4	2,4	2,4				4	1
11.	Multi-Round Encryption Algorithm	8	8, 26	8, 26			8	8	8	8, 26	8, 26			26	8, 26	26				26	2
	The total of atricles	4	30	25	0	0	2	14	4	14	27	0	2	28	17	19	4	2	3	23	30

The research repeated the same process to explore **INDistinguishability** standards from the selected articles and to put them in the Table (4.3). The researcher selected the articles' schemes with their IND standards in order to show the relationship between them for different aspect. The indication as well is the number of article inside the table to show that the IND standard is available in text of articles otherwise the box will be left it empty.

Table 4.3 The Authors' Scheme and Their Mentioned INDistinguishability Standards

Seq.	OPE Scheme	INDistinguishability standards								
		IND-CPA	IND-CCA	IND-CCA1	IND-CCA2	IND-CCA3	IND-CCVA	INT-PTXT	INT-CTXT	No of schemes
1.	Random OPE [9]	23,24	9,23,24	9,23	9,23	9,23	9	9	9	3
2.	OPE's Chenette scheme [1]	1,11, 12, 20	1,11,20	1,11,20	1,11,20	1,11,20	1,11,20	1,11,20	1,11,20	4
3.	Mutable OPE [17]	6,7,15,22, 28	6,7,15, 17	6, 7,15, 17	6,7,15, 17	6,7,15, 17	6,7,15, 17	6,7,15, 17	6,7,15, 17	5
4.	Modular OPE scheme [5]	14	5,13	5,13	5,13	5,13	5,13	5,13	5,13	3
5.	CryptDB scheme[16]	4,16,29	4,16,29	4,16,29	4,16,29	4,16,29	4,16,29	4,16,29	4,16,29	3
6.	OPE scheme, Popa 2016[25]	30	30	30	30	30	30	30	30	1
7.	Fully Homomorphic Encryption OPE	18	18	18	18	18	18	18	18	1
8.	ORAM Scheme	22	22	22	22	22		22	22	1
9.	Multi-Round Encryption Algorithm	26	26	12	12	12	12	26	26	2
10.	half-gate garbling scheme [24]	24						24	24	1
11.	Mini-Crypt Scheme	27	27	27	27		27		27	1
The total of articles		21	20	19	19	18	17	18	19	

The research repeated the process third time to explore **Indistinguishability** standards from the selected articles and to put them in the Table (4.3). The researcher selected the articles' schemes with their IND standards in order to show the relationship between them for different aspect. The indication as well is the number of article inside the table to show that the IND standard is available in text of articles otherwise the box will be left it empty. Finally, The Table 5.1 shows the selected articles as references for the previous three Tables (4.2, 4.3, 4.4) following in the index.

4.2.2 Articles' Summary

The researcher created the Table 4.4 to summarize each article. The table consists of the name of authors and the characteristics that have been cited and discussed by the author. The details of these articles can be found literature in the chapter two.

Table 4.4 Illustrate the Articles' Characteristics which are used by Authors

Seq.	Authors	Characteristics
1.	Chenette et., al. 2009	Access control, Active threat, Authentication, Channel, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Manipulation detection, Notarization, Passive threat, Physical security, Privacy, Routing control, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
2.	Fuller et. al 2017	Access control, Active threat, Authentication, Authorization, Availability, Channel, Ciphertext, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Manipulation detection, Notarization, Passive threat, Password, Physical

Seq.	Authors	Characteristics
		security, Privacy, Routing control, Security policy, Security service, Selective field protection, Traffic analysis, Traffic, Trusted functionality
3.	Popa et., al. 2009	Access control, Active threat, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Passive threat, Physical security, Privacy, Security policy, Security service, Selective field protection, Trusted functionality
4.	Sahin 2015	Access control, Active threat, Authorization, Availability, Ciphertext, Cleartext, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Manipulation detection, Masquerade, Notarization, Passive threat, Password, Physical security, Privacy, Security policy, Security service, Selective field protection, Trusted functionality
5.	Chenette et., al. (2) 2015	Access control, Ciphertext, Cleartext, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Manipulation detection, Privacy, Security policy, Security service, Sensitivity
6.	Kayed et., al. (1) 2016	Access control, Active threat, Authentication, Capability, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Digital signature, Encryption, Key management, Manipulation detection, Masquerade, Passive threat, Physical security, Privacy, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
7.	Hossein Shafagh	Access control, Accountability, Active threat, Authorization, Capability, Channel, Ciphertext, Cryptanalysis, Cryptography, Data origin authentication, Decryption, Encryption, Key

Seq.	Authors	Characteristics
		management, Manipulation detection, Physical security, Privacy, Security policy, Security service, Selective field protection, Sensitivity, Trusted functionality
8.	Jan Mohd Najar (2015)	Access control, Accountability, Active threat, Audit, Authentication, Authorization, Availability, Capability, Channel, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Denial of service, Digital signature, Encryption, Key management, Notarization, Passive threat, Password, Physical security, Privacy, Security service
9.	Reddy and Ramachandram	Active threat, Ciphertext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Notarization, Passive threat, Physical security, Repudiation, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
10.	Kadam	Access control, Authentication, Authorization, Ciphertext, Cryptanalysis, Cryptography, Decryption, Encryption, Key management, Physical security, Privacy, Security policy, Security service, Trusted functionality
11.	Xiao et., al	Access control, Active threat, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Passive threat, Physical security, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
12.	Harshali et al., 2017	Ciphertext, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Decryption, Denial of service, Encryption, Key management, Physical security, Privacy, Security policy, Security service, Selective field protection, Traffic flow confidentiality
13.	Jayashri 2015	Access control, Active threat, Availability, Ciphertext,

Seq.	Authors	Characteristics
		Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Digital signature, Encryption, Manipulation detection, Passive threat, Physical security, Privacy, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
14.	Chenette et., al. 2016	Ciphertext, Cleartext, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Privacy, Security policy, Security service, Trusted functionality
15.	Grofig et., al 2014	Access control, Authorization, Availability, Ciphertext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Manipulation detection, Masquerade, Notarization, Passive threat, Password, Privacy, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality
16.	Popa et., al. 2011	Access control, Active threat, Authentication, Authorization, Availability, Ciphertext, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Manipulation detection, Notarization, Passive threat, Password, Physical security, Privacy, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
17.	Popa et., al., 2013	Access control, Active threat, Authentication, Authorization, Availability, Ciphertext, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Manipulation detection, Notarization, Passive threat, Password, Physical security, Privacy, Security policy, Security service, Selective field protection, Traffic analysis,

Seq.	Authors	Characteristics
		Traffic flow confidentiality, Trusted functionality
18.	Rima 2016	Access control, Authentication, Ciphertext, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Security policy, Security service, Selective field protection, Traffic flow confidentiality, Trusted functionality
19.	Abdullatif Shikfa	Access control, Active threat, Audit, Authentication, Authorization, Availability, Capability, Channel, Ciphertext, Cleartext, Confidentiality, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Digital signature, Encryption, Notarization, Passive threat, Physical security, Privacy, Routing control, Security policy, Security service, Selective field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
20.	Agutale 2015	Ciphertext, Cryptanalysis, Cryptography, Decryption, Encryption, Key management, Physical security, Privacy, Selective field protection, Sensitivity, Trusted functionality
21.	Nasrin Dalil, Kayed 2015	Access control, Audit, Authentication, Authorization, Ciphertext, Cleartext, Cryptanalysis, Data integrity, Data origin authentication, Decryption, Denial of service, Digital signature, Encryption, Key management, Manipulation detection, Masquerade, Notarization, Passive threat, Password, Physical security, Privacy, Security policy, Security service, Selective field protection, Sensitivity, Trusted functionality
22.	Hithnawi et. al. 2015	Access control, Active threat, Authentication, Authorization, Availability, Capability, Channel, Ciphertext, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, passive threat, Physical security, Privacy, Routing control, Security policy, Security service, Selective

Seq.	Authors	Characteristics
		field protection, Traffic analysis, Traffic flow confidentiality, Trusted functionality
23.	Chenette et., al. (3) 2011	Ciphertext, Cleartext, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Decryption, Encryption, Key management, Privacy, Security policy, Security service, Sensitivity, Trusted functionality
24.	Tobias Boelter et. al. (2017)	Access control, Active threat, Ciphertext, Cleartext, Cryptanalysis, Cryptography, Decryption, Encryption, Key management, Passive threat, Physical security, Privacy, Routing control, Security policy, Security service, Selective field protection, Sensitivity
25.	Timo Schindler (2016)	Access control, Availability, Cleartext, Cryptanalysis, Cryptography, Decryption, Encryption, Key management, Physical security, Privacy, Security service, Selective field protection, Trusted functionality
26.	Gadekar	Access control, Audit, Authentication, Authorization, Ciphertext, Credentials, Cryptanalysis, Cryptography, Data integrity, Data origin authentication, Encryption, Key management, Physical security, Privacy, Security policy, Security service, Selective field protection, Trusted functionality
27.	Wenting Zheng, et. al. (2017)	Access control, Active threat, Availability, Confidentiality, Cryptography, Decryption, Encryption, Key management, Passive threat, Security policy, Security service, Selective field protection, Sensitivity, Trusted functionality
28.	Tim Waage 2016	Active threat, Authentication, Authorization, Cleartext, Confidentiality, Cryptanalysis, Cryptography, Data integrity, Decryption, Encryption, Key management, Passive threat, Physical security, Privacy, Security policy, Security service, Trusted functionality
29.	Ms. Omar [29]	Access control, Ciphertext, Cleartext, Cryptanalysis, Cryptography, Decryption, Encryption, Key management, Password, Physical security, Privacy, Routing control,

Seq.	Authors	Characteristics
		Security policy, Security service, Selective field protection, Trusted functionality
30.	Mr. Bazoon	Accountability, Ciphertext, Cleartext, Cryptanalysis, Cryptography, Decryption, Encryption, Key management, Physical security, Privacy, Routing control, Security policy, Security service, Selective field protection, Trusted functionality

4.2.3 Analysis Process

Collection and surveying processes are made the characteristics of ITU-X800 and INDs standards for all articles which are mentioned in three main tables and described them in details. This section will compare the results of these tables in order to find which characteristics are important than the others. This chapter presents these characteristics description and their application in detailed. It shows the results by figures and compare charts in order to highlight the reasons that are based on the classification of 30 articles.

From Table (4.1) the researcher counted how many papers discussed each ITU characteristics the Figure (4.2) illustrates each characteristic (38 characteristics) with the number of papers that discussed this characteristic. For example, 23 authors have discussed the "access control" characteristic while only 2 papers have discussed the "accountability" characteristic. This indicates "Access control" characteristic is more important than "accountability" characteristic.

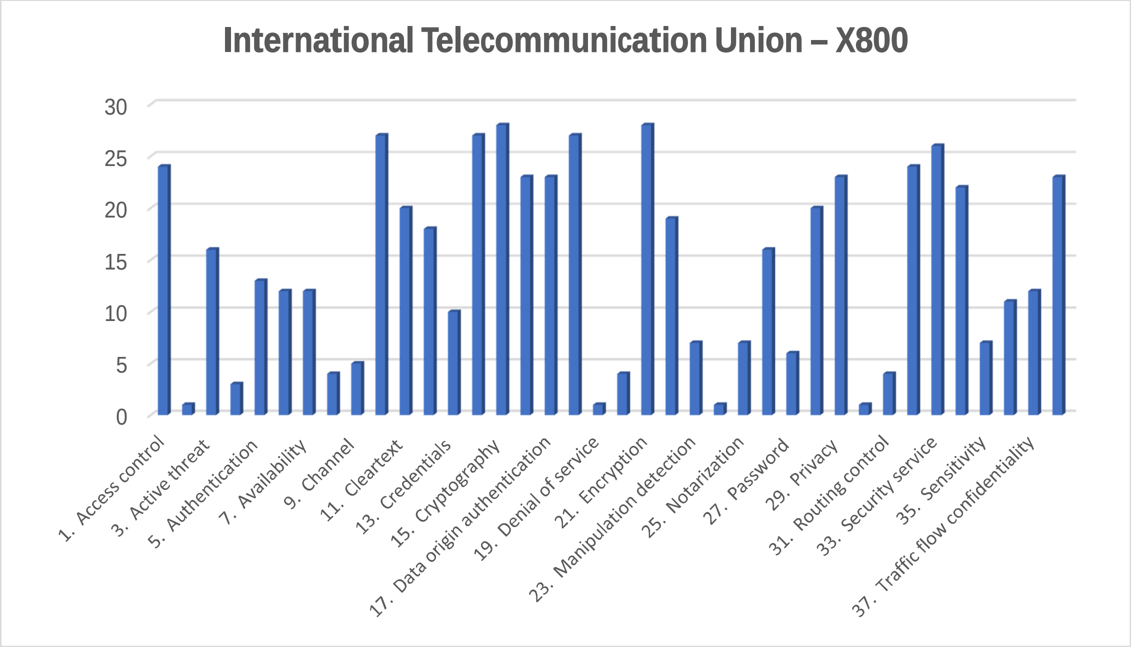


Figure 4.2: Illustrate the Related Between the Authors' Articles and Their Characteristics

Figure 4.3 illustrates the results of Figure 4.2 but in different order to from the most important characteristics to the lowest one. This makes it easier to find the best characteristics.

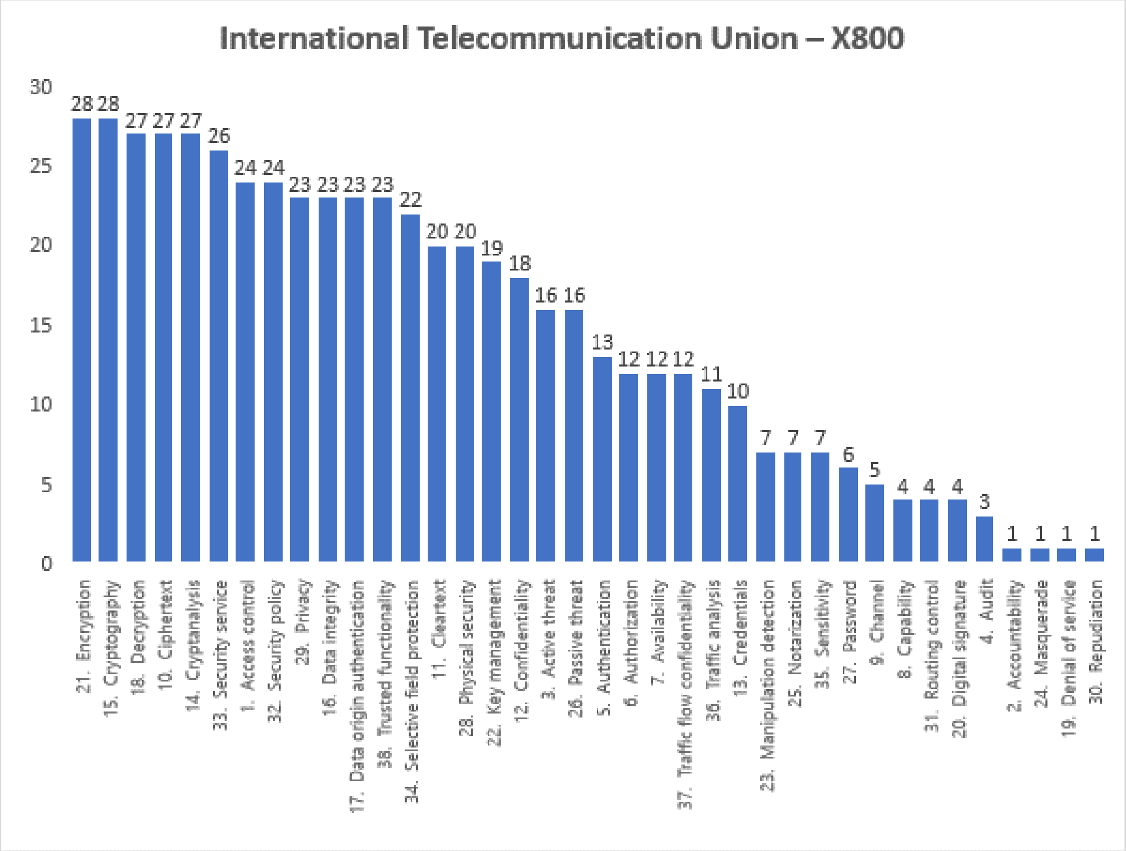


Figure 4.3: Shows the ITU-X800 Characteristics that the Authors Repeated and Focused on Them

From Table (4.2) the researcher counted how many papers discussed same scheme. The Figure (4.4) illustrates each scheme (Popa's and Chanette's schemes) with the number of schemes that discussed this scheme. For example, CryptDB scheme has seven authors who counted and discussed this scheme while "MiniCrypt" has one scheme that discussed it. This give us indicator that number of CryptDB best than MiniCrypt scheme.

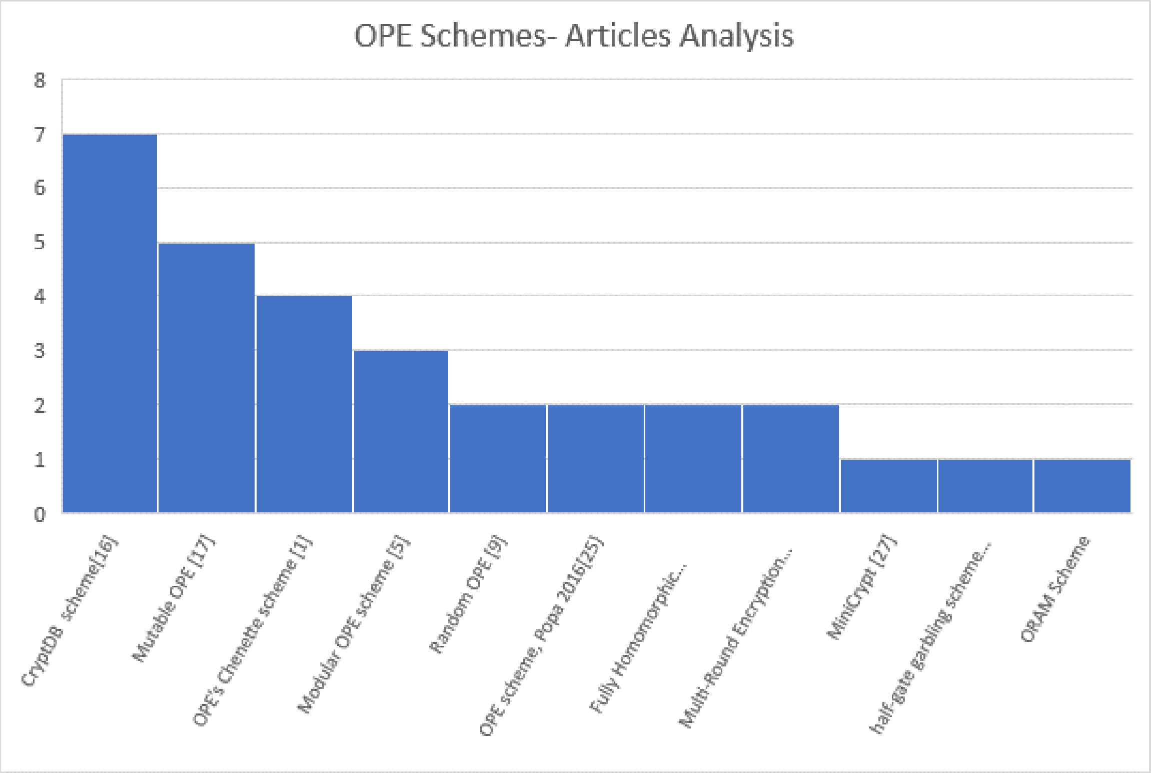


Figure 4.4: Shows the related between authors' schemes with number of papers have same scheme

From Table (4.3) the researcher counted how many schemes discussed each IND standards the Figure (4.5) illustrates each IND standards (8 standards) with the number of schemes that discussed this standard. For example, Mutable OPE has 5 schemes that are counted and discussed this standard while "ORAM" has 1 scheme that discussed it. This give us indicator that no

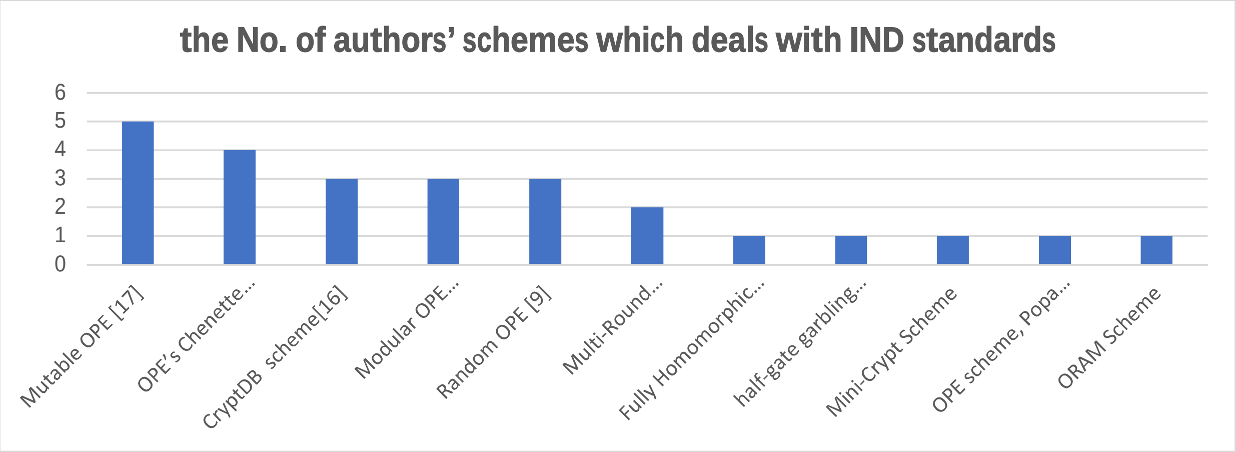


Figure 4.5: Shows the No. of Authors' Schemes Which Deals with IND Standards

From Table (4.3) the researcher counted how many schemes discussed each IND standards the Figure (4.6) illustrates each IND standards (eight standards) with the number of schemes that discussed this standard. For example, Mutable OPE has five schemes that are counted and discussed this standard while "ORAM" has one scheme that discussed it. This given indicator that number of Mutable OPE scheme is batter than the "ORAM" scheme.

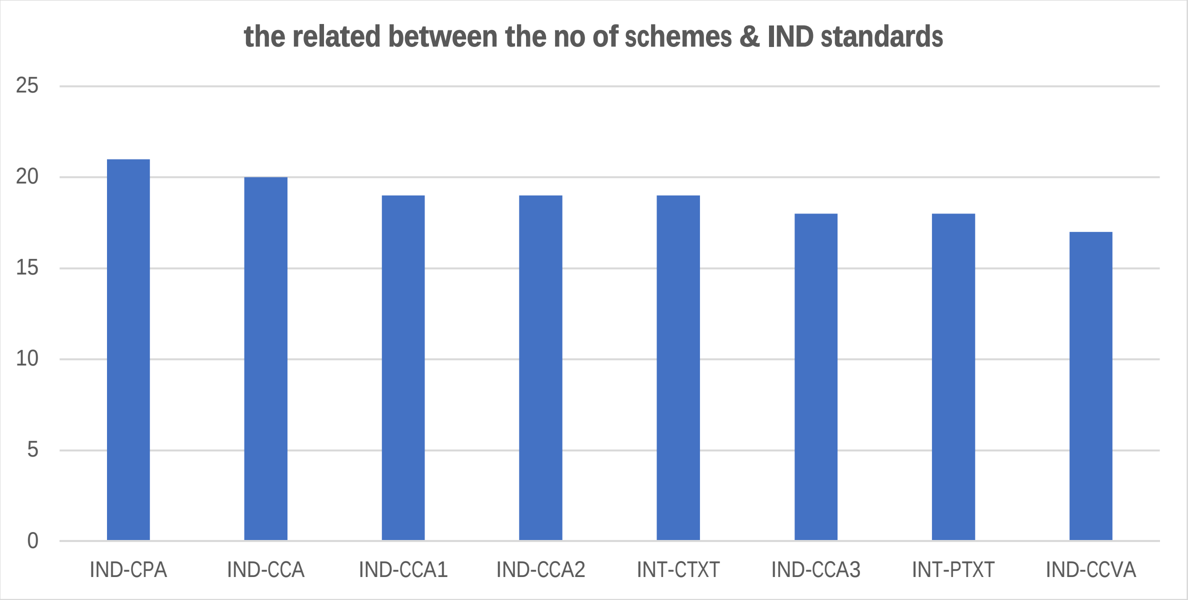


Figure 4.6: Shows the Related Between Authors' Schemes with IND Standards

From Table (4.3) the researcher counted how many schemes discussed each IND standards the Figure (4.6) illustrates each IND standards (8 standards) with the number of schemes that discussed this standard. For example, IND-CPA has 21 schemes that are counted and discussed this standard while "IND-CCVA" has 17 scheme that discussed it. This give us indicator that no IND-CPA is most important than "IND-CCVA".

4.3. The Classification

The classification part is a statistical which compares the results. This thesis classifies the characteristics and schemes into a set of groups each group has certain proprieties. In statistical questionnaire usually, the answers are classified in three or five groups [Creswell, 2003]. This thesis is classifying the schemes and characteristics into five and three groups. The classification type is frequency distribution because the characteristics are collected by the numbers of occurring and indicating in the articles.

Accordingly, the researcher suggested two attempts of classifications (3 classes) to find which the best is.

Table (4.5) illustrates the characteristics which are important (Class A) and they are 13 characteristics and the number of articles have been discussed and counted between (21-30) articles. The characteristics in middle level (Class B) is counted between (11-20) articles and the number of characteristics are 11 chars. The weak level (Class C) is counted between (0-10) articles which are discussed 14 characteristics.

Table 4.5. Three Classes of the Characteristics

Seq.	Characteristics	No of Characteristics	Level	Range
1.	Selective field protection, Data integrity, Data origin authentication, Privacy, Trusted functionality, Access control, Security policy, Security service, Ciphertext, Cryptanalysis, Decryption, Cryptography, Encryption	13	A	21-30
2.	Traffic analysis, Authorization, Availability, Traffic flow confidentiality, Authentication, Active threat, Passive threat, Confidentiality, key Management, Cleartext, Physical Security	11	B	11-20
3.	Accountability, Denial of service, Masquerade, Repudiation, Audit, Capability,	14	C	0-10

	Digital signature, Routing control, Channel, Password, Manipulation detection, Notarization, Sensitivity, Credentials			

For examples the Encryption characteristic based on all authors’ articles because all OPES schemes focused on the encryption process and tried to improve this characteristic. In the other side the audit characteristic did not base on the authors’ articles in order to the process of auditing has not important like Encryption.

In the scheme, there are different results of surveying. The researcher surveyed the characteristics in a certain scheme. For examples Encryption based on all selected schemes which are 11 schemes. The scheme has highest scale is the best than less scheme which has not the encryption characteristic.

Also, the researcher suggested to do attempt of classification (3 classes) to find the characteristics repetitions for the scheme (regarding to Table 4.4).

According to Figure (4.4), Table (4.6) illustrates the characteristics which are important (Class A) and they are 11 characteristics and the number of scheme had been discussed and counted between (21-30) articles. The characteristics in middle level (Class B) is counted between (11-20) articles and the number of characteristics are 11 chars. The weak level (Class C) is counted between (0-10) articles which are discussed 16 characteristics.

Table 4.6. Three Classes of the Characteristics in the Schemes

Seq.	Characteristics	The No. of Characteristics	Level	Range
1.	Encryption, Cryptography, Decryption, Cipher text, Cryptoanalysis, Privacy, Key Management, Security Policy, Access control, Trusted Functionality, Clear text	11	A	21-30
2.	Selective field protection, Confidential, Security service, Authentication, Authorization, Availability, Passive threat, Physical security, Active threat, Data Integrity, Data origin authentication	11	B	11-20
3.	Accountability, Denial of service, Masquerade, Repudiation, Audit, Capability, Digital signature, Routing control, Channel, Password, Manipulation detection, Notarization, Traffic analysis, Sensitivity, Credentials, Traffic flow confidentiality	16	C	0-10

According to Figure (4.4), the researcher creates the Table (4.7) which is illustrating the schemes which are the best (Class A) and they are 12 articles are discussed about (CryptDB, MutableOPE) schemes and the number of schemes had been discussed and counted between (5-7) schemes. The good classification (Class B) and they are 15 articles discussed about (OPE Chenette, Modular OPE,) schemes and the no. of schemes had been discussed and counted between (2-4). The bad classification (Class C) and they are 3 articles are discussed about (MiniCrypt, half-gate garbling, ORAM) schemes and the no. of articles had been discussed and counted between (less than 2).

Table 4.7. Three Classes of the Number of Articles Discussed About the Same Scheme

Seq.	Schemes	The No. of Articles	Level	Range
1.	CryptDB, MutableOPE	12	A	5-7
2.	OPE Chenette, Modular OPE, RandomOPE, OPE Popa 2016, Fully Homomorphic, MultiRound Encryp.	15	B	2-4
3.	MiniCrypt, half-gate garbling, ORAM	3	C	< 2

According to Figure (4.5), Table (4-8) illustrates the IND standards which are important (Class A) and they are 5 standards and the number of schemes had been discussed and counted between (4-5) articles. The standards in middle level (Class B) is counted between (2-3) articles and the number of standards are eight chars. The weak level (Class C) is counted between (0-1) articles which are discussed one standard.

Table 4.8 Three classes of the IND standards in the schemes

Seq.	Schemes	The No. of schemes	Level	Range
1.	Mutable OPE, OPE's Chenette scheme	2	A	4-5
2.	CryptDB scheme, Modular OPE scheme, Random OPE, Multi-Round Encryption Algorithm	4	B	2-3
3.	Fully Homomorphic Encryption OPE, half-gate garbling scheme, Mini-Crypt Scheme, OPE scheme, Popa 2016, ORAM Scheme	5	C	0-1

For examples the Mutable OPE scheme based on 5 IND standards because all IND schemes focused on the Mutable OPE and tried to improve this scheme. In the other side the ORAM scheme did not base on the 1 IND standard in order to the Mutable scheme is the best than ORAM scheme.

According to Figure (4.6), Table (4.9) illustrate the IND standards which are important (Class A) and they are 2 standards and the number of articles had been discussed and counted between (20-21) articles. The standards in middle level (Class B) is counted between (18-19) articles and the number of standards are five IND standards. The weak level (Class C) is counted less than 17 articles which are discussed one standard.

Table 4.9 Three Classes of the IND Standards in the Schemes

Seq.	IND standards	The No. of Standards	Level	Range
1.	IND-CPA, IND-CCA	2	A	20-21
2.	IND-CCA1, IND-CCA2, IND-CTXT, IND-CCA3, INT-PTXT	5	B	18-19
3.	IND-CCVA	1	C	Less 17

For examples the Mutable IND-CPA standard based on 21 articles because all schemes focused on the IND standards and tried to improve this scheme. In the other side the IND-CCVA standard base on the less than 17 articles in order to the IND-CPA is the important than IND-CCVA standard.

4.4. Building of Measuring Scheme

According to the classification process in chapter 4, the researcher presents the final results of the research. The results are collecting all the classifications from schemes, articles and their characteristics including the IND standards. The researchers based on the classification in Table (4.5) and Table (4.7). Table 4.10 is summarizing and classifying all the work into four groups. These groups are High - High, Low- Low, High Low, and low High. First cell in the Table 4.10 will be the High-High classes for the articles and the schemes. The right cell from the first row of the table will be High class of schemes with Low class of articles. The first cell from the second row will be Low class of schemes with High class of articles.

Table 4.10 the Combination between Articles Table (4.5) & Schemes Table (4.7)

Articles Scheme	High	Low
High	Encryption, Cryptography, Decryption, Cipher text, Cryptoanalysis, Access Control, Privacy, Trusted Functionality, Security Policy, IND-CPA, IND-CCA	Key Management, Cleartext
Low	Security Services, Selective field protection, Data Integrity, Data Origin Authentication, IND-CCA1, IND-CCA2, IND-CTXT, IND-CCA3, INT-PTXT	Authorization, Availability, Authentication, Active threat, Passive threat, Physical Security, Confidentiality

Table 4.10 illustrate the combination between the Table (4.7) and Table (4.9). The researchers based on the classification in Table (4.5) and Table (4.7). These are (high scheme high references, high scheme low references, low scheme high reference, and low scheme low reference). The first field in the Table 4.10. Is the High-High classes of articles and scheme, the “high scheme high references” means that the characteristics in this class have been identified as

the highest characteristics that have been used in real OPES system as well as the highest cited characteristics in the OPES and security literature. The second filed is the High-Low classes of articles and schemes. The “high scheme low references” means that the characteristics in this class have been identified as the highest characteristics that have been used in real OPES system as well as the lowest cited characteristics in the OPES and security literature. The third filed is the Low-High classes of articles and schemes. The “low scheme high references” means that the characteristics in this class have been identified as the lowest characteristics that have been used in real OPES system as well as the highest cited characteristics in the OPES and security literature.

The last filed is the Low-Low classes of articles and schemes. The “low scheme low references” means that the characteristics in this class have been identified as the lowest characteristics that have been used in real OPES system as well as the lowest cited characteristics in the OPES and security literature this filed ignored.

4.5. The Results and Discussion:

As noted in the previous Table (4.11), which is illustrated the results of all previous works and preparations. The researcher lists all classification characteristics in Table (4.10) and the characteristics of scheme from Table (4.10). The researcher writes down the classification of each characteristic for scheme and articles to be as the table below. For example, in Table 4.5 the characteristic “encryption” is the high classification in the table so that the researcher gave it Letter “High” in the column (Articles), and the characteristic “Traffic compare” is a little bit less than high classification so that the researcher gave letter “Low”. The lowest classification, the researcher removed the characteristics in class “C”. Same procedure is done with the scheme classification in Table (4.10).

Table (4.11) Illustrates the Measuring Schemes Types

Seq.	Characteristics	Schemes	Articles	Measuring Scheme Type
1.	Encryption,	H	H	HH
2.	Cryptography,	H	H	HH
3.	Decryption,	H	H	HH
4.	Cipher text,	H	H	HH
5.	Cryptoanalysis,	H	H	HH
6.	Access Control,	H	H	HH
7.	Security Services,	L	H	LH
8.	Security Policy	H	H	HH
9.	Selective field protection	L	H	LH
10.	Privacy	H	H	HH
11.	Data Integrity	L	H	LH
12.	Data Origin Authentication,	L	H	LH
13.	Trusted Functionality	H	H	HH
14.	Authorization	L	L	LL
15.	Availability	L	L	LL
16.	Authentication	L	L	LL
17.	Active threat	L	L	LL
18.	Passive threat	L	L	LL
19.	Key Management	H	L	HL
20.	Cleartext	H	L	HL
21.	Physical Security	L	L	LL
22.	Confidentiality	L	L	LL
23.	IND-CPA	H	H	HH
24.	IND-CCA	H	H	HH
25.	IND-CCA1	L	L	LL
26.	IND-CCA2	L	L	LL
27.	IND-CTXT	L	L	LL
28.	IND-CCA3	L	L	LL
29.	INT-PTXT	L	L	LL

Table (4.11) illustrated the results of classification. the results consist of (High-High, Low-High, High-Low, and Low-low).

High-High (Scheme, Articles): the researcher combined the proposed measuring scheme components from the class 1. According to the standard of measuring scheme architecture, the building process is implementing by High-High. The researcher selected the High-High because the researcher has two reasons: First, it is the most important among the characteristics of schemes and articles. Second, it is the minimal characteristics which any OPEs must have these characteristics, and the best schemes of Popa.

Hi-Low (Scheme, Articles): The researchers are applied the characteristics of the schemes more than the characteristics of articles and the articles are discussed them but not too much.

Low-Hi (Scheme, Articles): The researchers are not applied the characteristics of schemes more than the characteristics of articles and also the articles are discussed them but not too much.

Low-Low (Scheme, Articles): the researcher ignored this class because the worst case.

Accordingly, the first measuring scheme contains all of most important characteristics and INDs standards in the schemes and articles. The researcher named a first measuring scheme as "***Must Measuring Scheme*** " which consists of 11 characteristics as the below:

The must Measuring Scheme	Encryption, Cryptography, Decryption, Cipher text, Cryptoanalysis, Access Control, Privacy, Trusted Functionality, Security Policy, IND-CPA, IND-CCA

The researcher also integrated High-High with High-Low classifications which means: **(Must Measuring Scheme + High-Low)** to create a new measuring scheme which named as "***Applied Measuring Scheme***" for the researchers who concerned with the applied articles more than the theoretical articles. This measuring scheme has 13 characteristics.

The Applied Measuring Scheme	Encryption, Cryptography, Decryption, Cipher text, Cryptoanalysis, Access Control, Privacy, Trusted Functionality, Security Policy, Key Management, Cleartext, IND-CPA, IND-CCA

The researcher also integrated High-High with Low-High classifications which means: **(Must Measuring Scheme + Low-High)** to create a new measuring scheme which named as "***Theory Measuring Scheme***" for the researchers who concerned with the theoretical articles more than the applied articles. This Measuring scheme has 21 characteristics.

The Theory Measuring scheme	Encryption, Cryptography, Decryption, Cipher text, Cryptoanalysis, Access Control, Privacy, Trusted Functionality, Security Policy, Security Services, Selective field protection, Data Integrity, Data Origin, Authentication, IND-CCA1, IND-CCA2, IND-CTXT, IND-CCA3, INT-PTXT, IND-CPA, IND-CCA

The following will give a brief definition for most important characteristics reached in these three schemes with a full description. The definitions and descriptions have been adopted from [(Stallings, 2005), (Committee, 1991)]

1. Encryption**:** is the process that the sender wants to send a message to receiver without the third party can read the message properly because this message is converted it into coded form mathematically. The encryption and decryption processes have same algorithm to be implemented that called Symantec system. AES built as an encryption support Symantec System Recovery 2013 includes built-in software encryption that enables

administrators to ensure the security and integrity of their critical business data when it is protected by Symantec System Recovery and stored to disk in the form of backup files known as recovery points.

2. Cryptography: Is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.
3. Decryption: When the receiver gets the ciphertext he needs to decode it to obtain the plaintext, this process is called decryption and is achieved by using the corresponding decryption algorithm. This criterion deals with several issues related to considerations of both encryption and decryption. If the encryption and decryption algorithms differ, then extra space is needed for the decryption. Also, whether the two algorithms are the same or not, there may be timing differences between encryption and decryption.
4. Cipher text: Is the result of many operations that happened to the plaintext or real text to transform to be difficultly understand or Data produced through the use of encipherment. The semantic content of the resulting data is not available. Note – Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.
5. Cryptanalysis: It is a study of analyzing the security of information systems in order to study the hidden of the systems. Cryptanalysis is used to break cryptographic security systems and verify access to contents of encrypted messages, whether the encrypted key is unknown. The mathematical analysis of cryptographic algorithms, cryptanalysis includes the study of side-channel attacks that do not target weaknesses in the

cryptographic algorithms themselves, but instead exploit weaknesses in their implementation. Many techniques applied to analyze security systems or attack them like Zombies in distributed systems which is often used to spread e-mail spam and launch denial-of-service attacks (DOS attacks).

6. Access Control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
7. Privacy: Provides a user with protection against discovery and misuse of his or her identity by other users, or the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
8. Trusted Functionality: It can be used to either extend the scope or to establish the effectiveness of other security mechanisms. Any functionality that directly provides, or provides access to, security mechanisms should be trustworthy
9. Security Policy: It is a legal document that discover some or all of the ways party gathers, uses, and manages a client’s data. It fulfills a legal requirement to protect a customer or client's privacy. Personal information can be anything that can be used to identify an individual, not limited to the person's name, address, date of birth, marital status, contact information, ID issue and expiry date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services.
10. Security Services: It is a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.
11. Selective Field Protection: The safeguard of particular fields inside a message which is to be transmitted.

12. Data Integrity: As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.
13. Data Origin: It is also called message authentication. In a connectionless transfer, provides assurance that the source of received data is as claimed. It is also a property that a message has not been modified while in transit (data integrity) and that the receiving party can verify the source of the message.
14. Authentication: is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. There are three types of authentication as following as:

    • The first type of authentication is accepting proof of identity given by a credible person who has first-hand evidence that the identity is genuine

    • The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph.

• The third type of authentication relies on documentation or other external affirmations. In criminal courts, the rules of evidence often require establishing the chain of custody of evidence presented.

15. , IND-CCA1: indistinguishability under (non-adaptive) chosen ciphertext attack.
16. IND-CCA2: indistinguishability under adaptive chosen ciphertext attack or leads to NM-CPA (non-malleability under chosen plaintext attack) or equivalent to NM-CCA2 (non-malleability under adaptive chosen ciphertext attack).
17. IND-CCA3: notion is formulated using real or- random indistinguishability.
18. IND-CTXT: Integrity of Ciphertext to be computationally infeasible to produce a ciphertext not previously produced by the sender.
19. INT-PTXT: Integrity of Plaintext to be computationally infeasible to produce a ciphertext decrypting to a message that the sender had never encrypted.
20. IND-CPA: Iindistinguishability under chosen plaintext attack or It is NM-CPA (non-malleability under chosen plaintext attack). For schemes based on computational security, the adversary is modeled by a probabilistic polynomial time Turing machine, meaning that it must complete the game and output a ”guess” within a polynomial number of time steps.
21. IND-CCA: Indistinguishable against chosen ciphertext attack However, in addition to the public key (or encryption oracle, in the symmetric case), the adversary is given access to a” decryption oracle” which decrypts arbitrary ciphertexts at the adversary’s request, returning the plaintext.
22. Key Management: is the name of management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, destruction and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling, which typically refers to the internal handling of keys within the

operation of a cipher. Successful key management is critical to the security of a cryptosystem. It is the more challenging side of cryptography in a sense that it involves aspects of social engineering such as system policy, user training, organizational and departmental interactions, and coordination between all of these elements, in contrast to pure mathematical practices that can be automated.

23. Cleartext: It refers to data that is transmitted or stored unencrypted. For example, the name of an organization may be shown in cleartext in a digital certificate so that humans can read the certificate and understand who it belongs to.

The contribution of This thesis can be summarized in the following

1. As far as we know, that there is no one that apply ITU-800 and IND- on the OPEs schemes. The volume of this work is very huge and needs time. The only work that is close to ours is Popa’s work. They added new characteristics and apply them on some schemes. This thesis applied the 38 and INDs standards (including the Popa’s work) on 11 OPEs schemes.
2. The authors table helps to compare among the schemes and characteristics to reflect the properties of articles. The authors table shows the number of articles which discussed a certain characteristic. it is also reflecting which the characteristics are very important than the other.

3. The schemes table helps to know the best schemes via the results which will present the comparison among each scheme. The schemes characteristics reflect how many schemes are based on the main scheme. The result of scheme characteristic gives which the characteristic is very important than the other.

4. This thesis proposes three types of measuring scheme s in the OPEs domain. These are the must, the applied, and the theoretical fireworks. These Measuring Scheme s could be used to enhance the ability to use, compare understand, study, evaluate, and create OPEs schemes and characteristics.

Chapter Five

Conclusions and Future Works

5.1 Conclusions

This thesis defined the main problem of cloud security in particular processing encrypted data over un-trusteed environment such as cloud computing. This thesis focused on certain type of encryption that can preserve the ordered of data. There were several OPEs algorithms and this thesis built Measuring Schemes which compere these algorithms. This thesis studied the previous Measuring schemes and designed a new Measuring Scheme. This thesis answered a main question about the main characteristics can be applied on OPE algorithms by using the proposed measuring scheme which answered How we can compare among these OPES algorithms?

Several institutes built general measuring schemes that highlighted the security aspect and identified specifications and properties of security algorithms. As far as we know, an accurate measuring scheme that clearly identifies characteristics and properties for Order-Preserving Encryption Schemes (OPES) remains unavailable. This thesis provided an in-depth meta-comparative by utilizing available research in this area in an attempt to propose a standardized Measuring scheme.

This thesis is based on three surveys covering the period (1991 – 2017) as well as over 180 research papers. This thesis studied the main characteristics of ITU-X800, Popa, Chenette, and OPES characteristics and proposed a new OPES Measuring scheme.

According to the outcomes, the researcher proposes three OPES Measuring schemes. This thesis called the first Measuring scheme as the “Must Measuring Scheme” which consist of the mandatory properties that must be available in all OPE schemes. The “Must Measuring Scheme” characteristics have been identified as the most characteristics which have been used in real OPES system as well as the most cited characteristics in the OPES and security literature. This thesis called the second Measuring scheme as the “Applied Measuring Scheme”. This Measuring

Scheme consists of all characteristics in the must formwork in addition to the most characteristics that have been used in real OPES systems. This thesis called the third Measuring Scheme as the "Theoretical Measuring scheme". This Measuring scheme consists of all characteristics in the must Measuring scheme in addition to the most characteristics that have been cited the OPES and in security literature. The "must" has been identified in This thesis by using certain cutting point for the number of OPES or literature that have been used or cited this characteristics. Fifty nine ITU-X800 characteristics, 11 Popa's characteristics , 11 OPES, 3 surveys, 200 papers, and 30 OPES papers have been carefully examined thus leading to the proposal of the three Measuring scheme.

This thesis finds the following outcomes:

.

1. Through carefully studied charts, OPEs have some problems. This thesis choose the best scheme from among these selected schemes which were studied by researchers.
2. Through the tables that were built and compare in the previous chapters, many indicators and ideas were given through which it can be concluded that the researchers gave more attention to Popa and Chenette schemes. There are less attrition was given to the schemes of Kadhem and Boldyreva.
3. The classifications process presented some of satisfied results due to the data collecting and the characteristics that are taken precisely from the references so that the building of Measuring scheme contains the most important-minimal characteristics.
4. The researcher faced many challenges to build a Measuring scheme and to achieve its main functions so that the tables of characteristics and schemes have supported to solve these problems.
5. The primary results of classification (High-High) in chapter 4 Table 4.15 can be used to check the quality for any new OPES scheme.

6. The thesis studied the OPE's schemes between (1991-2017). It provides details for the best thirty articles and it finds that the best OPE scheme is for Popa.
7. This thesis is a reference for many OPEs researchers wishing to do a quick test of their algorithms.
8. The researcher concluded that the High-High classification for those (characteristics and schemes) can be used to build "good" OPEs algorithm with high quality.
9. According to This thesis, any programmer can build an algorithm with applied specification needs to focus on schematic specifications that is the (Hi-Low) Measuring Scheme. The researcher who wishes to construct a theoretical algorithm needs to choose the measuring scheme Low -Hi.

(Bellare, 2000)The recommendation and suggestion for future work for the new Measuring Scheme is as following:

1. The new Measuring scheme has not tested the real OPE systems for these characteristics. The future work is to check the availability of these characteristics for these systems.
2. Questionnaires for the new Measuring scheme can be prepared to collect data from OPEs developers to test the Measuring schemes quality and applicability.
3. Can be tested many algorithms and evaluated it using the new Measuring scheme
4. May be inserted additional types of characteristics to be more comprehensive for building and evaluating any algorithms.
5. New Measuring scheme can be considered as base for developing new algorithms , in addition to the old algorithms

5.2. Indexing

Table 5.1 Shows the Selected Articles as References for Tables 4.2, 4.3, 4.4.

Ref.	The Articles
[1]	Alexandra Boldyreva, N. C. (2012). Order-Preserving Symmetric Encryption. *A. Joux ed., LNCS* (pp. 28th Annual International Cryptology Conference,). CA, USA: Springer.
[2]	Benjamin Fuller, M. V. (2017). SoK: Cryptographically Protected Database Search. *NSF Grant*, 1-20.
[3]	Carlo Curino, E. P. (2010). Relational Cloud: A Database as a Service for the Cloud. *ACM*, 235-240.
[4]	Cetin Sahin, A. E. (2017). Data Security and Privacy for Outsourced Data in the Cloud. *20th International Conference on Extending Database Technology (EDBT),* (pp. 606-609). Venice, Italy: OpenProceedings.org.
[5]	Chenette, N. (2015). Modular Order-Preserving Encryption, Revisited. *ACM*, 1-14.
[6]	Eyad Saleh, A. A. (2016). Processing Over Encrypted Data: Between Theory and Practice. *SIGMOD Record,*, 5-16.
[7]	Hossein Shafagh, A. H. (2015). Talos: Encrypted Query Processing for the Internet of Things. *ACM*, 1-14.
[8]	Jan Mohd Najar, A. S. (2015). Multi-Round Encryption Algorithm- A Review. *Review*, 6488-6491.
[9]	K. Srinivasa Reddy, S. R. (2014). A New Randomized Order Preserving Encryption Scheme. *International Journal of Computer Applications*, 41-46.
[10]	Kadam Sandip Parashram Kadam, K. D. (2016). A Survey on KNN Query Processing In Cloud and Anonymity with ABE. *International Journal of Innovative Research in Computer and Communication Engineering*, 20988-20992.
[11]	Liangliang Xiao, O. B.-L. (2012). Security Analysis for Order Preserving Encryption Schemes. *IEEE*, 1-13.
[12]	Harshali et al. :Secure Multi-keyword Search using OPE over Cloud, International Journal of Advance Research in Computer Science and Management Studies. Vol.5 2017. 65-70
[13]	N.Jayashri., T. (2015). Effective Modular Order Preserving Encryption on Cloud Using MHGD. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16-24.
[14]	Nathan Chenette, K. L. (2016). Practical Order-Revealing Encryption with Limited Leakage. *Rose-Hulman Institute of Technology*, 1-27.
[15]	Patrick Grofig, I. H. (2014). Privacy By Encrypted Databases. *SAP*, 1-14.
[16]	Raluca Ada Popa, C. M. (2011). CryptDB: Protecting Confidentiality with Encrypted Query

	Processing. *ACM*, 85-100.
[17]	Raluca Ada Popa, F. H. (2013). An Ideal-Security Protocol for Order-Preserving Encoding. *NSF award IIS-1065219, Google*, 1-15.
[18]	Rima Saleh, D. P. (2016). Analysis of efficient storage Technique for financial data in Cloud. *International Journal of lastest trends inEngineering and Technology*, 214-220.
[19]	Vladimir Kolesnikov, A. S. (2012). On The Limits of Privacy Provided by Order- Preserving Encryption. *Bell Labs Technical Journal, Wiley Periodicals, Inc*, 135–146.
[20]	Harshal,Agutale (2015): A Survey and Security Analysis on One-To-Many Order Preserving Technique on Cloud Data, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 11, 6127 – 6131
[21]	Nasrin Dalil , Ahmed Al-Kayed (2015): Preserving Data in Cloud Computing, IJCSI International Journal of Computer Science Issues, Volume 12, Issue 2, 296-300
[22]	**Hossein Shafagh, A. H. (2017):** Talos Encrypted Query Processing for the Internet of things, MobiArch ’17, Los Angeles, CA, USA, ACM, Page 1-6
[23]	**Nathan Chenette et, al. (2011)**: “Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions”, 31th Annual International Cryptology Conference, A. Joux ed., LNCS, Springer, 1-9
[24]	**Tobias Boelter et. al. (2017):** A Secure One-Roundtrip Index for Range Queries. A Secure One-Roundtrip Index for Range Queries. http://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-7.html.
[25]	**Timo Schindler (2016):** Secure Parallel Processing of Big Data Using Order-Preserving Encryption on Google BigQuery, Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK, Lecture Notes in Informatics (LNI), Gesellschaft f ¨ur Informatik, Bonn 3433-52
[26]	**Vanita Gadekar, Baisa Gunjal.** Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing, Vol-2 Issue-1 IJARIIE-ISSN(O)-2395-4396
[27]	**Wenting Zheng, et. al. (2017):** MiniCrypt: Reconciling Encryption and Compression for Big Data Stores, EuroSys ′ April 23-26, 2017, Belgrade, Serbia. Copyright held by the owner/author(s). ACM ISBN 978-1-4503-4938-3/17/0417
[28]	**TimWaage (2016):** Order Preserving Encryption for Wide Column Stores, M. Meier, D. Reinhardt, S. Wendzel (Hrsg.): Sicherheit 2016, Lecture Notes in Informatics (LNI), Gesellschaft f ¨ur Informatik, Bonn 209-214
[29]	**Suha Wasof Omar** , “Analytical Study for the Mutable Order-Preserving Encoding with Periodically Encryption Key Changing”, Msc. Thesis, Middle East University, Amman, Jordan, May, 2016
[30]	**Amro Akram Bazoon**, “Investigation on Order-Preserving Encryption for Database in Cloud Computing”, Msc. Thesis, Middle East University, Amman, Jordan, January, 2016

References:

Alexandra Boldyreva, N. C. (2012). Order-Preserving Symmetric Encryption. *A. Joux ed., LNCS* (pp. 28th Annual International Cryptology Conference,). CA, USA: Springer.

Anderson, R. (2001). *Security Engineering.* Cambridge: Wiley.

B. Sunar, W. J. (2007). A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Trans. Comput.*, 109–119.

Benjamin Fuller, M. V. (2017). SoK: Cryptographically Protected Database Search. *NSF Grant*, 1-20.

Carlo Curino, E. P. (2010). Relational Cloud: A Database as a Service for the Cloud. *ACM*, 235-240.

Cavoukian, A. (1995, November 23). *Who knows: Safeguarding Your privacy in A nelworked Word* . Retrieved from Random House of Canada: www.businessdictionary.com/definition/privacy-policy.html

Cetin Sahin, A. E. (2017). Data Security and Privacy for Outsourced Data in the Cloud. *20th International Conference on Extending Database Technology (EDBT),* (pp. 606-609). Venice, Italy: OpenProceedings.org.

Chenette, N. (2015). Modular Order-Preserving Encryption, Revisited. *ACM*, 1-14.

Cocks, C. (2001). An Identity Based encryption scheme based on Quardratic residuse. *IN IMA int. Conf* (pp. 360-363). 2001.

Committee, T. i. (1991). *Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure, and Application.* Geneva: International Telecommunication Union.

Dan Boneh, A. S. (2012). Functional Encryption: A New Vision for Public Key Cryptography. *ACM* (p. 8). ACM.

DrLecter. (2014, 06 25). *Cryptography*. Retrieved from https://crypto.stackexchange.com/questions/17893/what-is-attribute-based-encryption

Eyad Saleh, A. A. (2016). Processing Over Encrypted Data: Between Theory and Practice. *SIGMOD Record,*, 5-16.

Franklin, D. B. (2003). Identity Based encryption from the Weil pairing. *In Proc.vol. 2139*, 10-20.

Ghemawat, J. D. (2004). Sixth Symposium on Operating System Design and Implementation. *OSDI'04* (pp. 14-20). San Francisco: Google Inc.

Harry B. Santoso, M. S. (2016). Measuring User Experience of the Student-Centered e-Learning Environment. *The Journal of Educators Online-JEO January 2016*, 58-79.

Hossein Shafagh, A. H. (2015). Talos: Encrypted Query Processing for the Internet of Things. *ACM*, 1-14.

ITINERARIES, H. &. (2010). Retrieved from www.VisitJordan.com: www.VisitJordan.com

Jan Mohd Najar, A. S. (2015). Multi-Round Encryption Algorithm- A Review. *Review*, 6488-6491.

K. Srinivasa Reddy, S. R. (2014). A New Randomized Order Preserving Encryption Scheme. *International Journal of Computer Applications*, 41-46.

Kallet, R. H. (2004). "How to Write the Methods Section of a Research Paper." . *Respiratory Care 49* , 1229-1232.

Liangliang Xiao, O. B.-L. (2012). Security Analysis for Order Preserving Encryption Schemes. *IEEE*, 1-13.

Ling Dong, K. C. (2012). *Cryptographic Protocol Security Analysis based on trusted Fresheen.* New york: Spring.

Mavroforakis, C., Chenette, N., O'Neill, A., Kollios, G., & Canetti, R. (2015). Modular Order-Preserving Encryption. *ACM*, 1-5.

N.Jayashri., T. (2015). Effective Modular Order Preserving Encryption on Cloud Using MHGD. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16-24.

Nathan Chenette, K. L. (2016). Practical Order-Revealing Encryption with Limited Leakage. *Rose-Hulman Institute of Technology*, 1-27.

Nir Bitansky, V. V. (2015). Indistinguishability Obfuscation from Functional Encryption. *FOCS*, 1-36.

Patrick Grofig, I. H. (2014). Privacy By Encrypted Databases. *SAP*, 1-14.

Raluca Ada Popa, C. M. (2011). CryptDB: Protecting Confidentiality with Encrypted Query Processing. *ACM*, 85-100.

Raluca Ada Popa, F. H. (2014). An Ideal-Security Protocol for Order-Preserving Encoding. *NSF award IIS-1065219, Google*, 1-15.

Rima Saleh, D. P. (2016). Analysis of efficient storage Technique for financial data in Cloud. *International Journal of lastest trends inEngineering and Technology*, 214-220.

Sevalioglu, A. S. (2010). WorrFunctional Encryption with public keys. *ACM Conference on Computer and Communication Security* (pp. 463-472). ACM.

Shamir, A. (1984). Identity Based Cryptosystems and signature schemes. *CRYPTO*, 47-53.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices.* Newyork: Prentice Hall.

Vladimir Kolesnikov, A. S. (2012). On The Limits of Privacy Provided by Order- Preserving Encryption. *Bell Labs Technical Journal, Wiley Periodicals, Inc*, 135–146..