Protection of Privacy Information in E-Government

Hemin Akram Muhammad, Msc., Ph.D.

Doctoral Thesis Summary

Tomas Bata University in Zlín

Tomas Bata University in Zlín
Faculty of Applied Informatics

Doctoral Thesis Summary

Ochrana osobních údajů v e-Governmentu

Protection of Privacy Information in E-Government

Author:	Hemin Akram Muhammad, MSc., Ph.D.
Degree programme:	P3902 / Engineering Informatics
Degree course:	3902V023 / Engineering Informatics
Supervisor:	Assoc. Prof. Ing. Martin Hromada, Ph.D.
External examiners:	Plk. Assoc. Prof. Ing. Petr Hrůza, Ph.D.
	Prof. Ing. Zdeněk Dvořák, PhD.
	Prof. Mgr. Roman Jašek, Ph.D., DBA.

Zlin, 2024

Published by **Tomas Bata University in Zlín** in the Edition **Doctoral Thesis Summary.**
The publication was issued in the year 2024.

Klíčová slova: *E-Government, Bezpečnost osobních údajů, SOAR, AHP*

Keywords: *E-Government, Personal Information Security, SOAR, AHP*

Full text of the doctoral thesis is available in the Library of TBU in Zlín.

ISBN 978-80-7678-260-0

Abstrakt

Služby e-governmentu jsou poskytovány ve vyspělých a většině rozvojových zemí. Tento výzkum reaguje na obavy a překážky, které ovlivňují bezpečnost osobních údajů v e-governmentu. S ohledem na většinu bezpečnostních hledisek, navrhuje nový model e-governmentu zohledňující aspekt ochrany osobních údajů. Studie je z hlediska metodologie kvalitativní, je postaven na případových studiích, obsahové analýze a srovnávací studii. Navrhovaný model zahrnuje metody, které vládám umožňují zvýšit úroveň ochrany osobních údajů v právní, sociální, organizační a technické oblasti. Kromě nastínění požadavků na ochranu osobních údajů pro každou úroveň, model poskytuje strategii zlepšování, pravidla a procesy a indikátory pro budoucí implementaci. Stejně tak byla v této práci navrhnuta a použita nová metoda pro hodnocení navrženého modelu. Využívá analýzu SOAR (Strengths, Opportunities, Aspirations, and Results) k vyhodnocení fází a kombinuje ji s procesem analytické hierarchie (AHP) k určení aplikovatelnosti modelu. Závěry práce ukazují, že model je vhodný k praktické aplikaci. Model je tedy použitelnou a vhodnou volbou pro budpvání e-governmentu v rozvojových zemích.

Abstract

E-government services are provided in developed and most of the developing countries. This research studies the concerns and obstacles that affect personal information security in e-government, considering the majority of security viewpoints, it proposes a new model of e-government from perspective of protecting personal data. The study is qualitative in terms of methodology, it depends on documentary studies, content analysis and comparative study. The proposed model includes methods that enable governments to increase the level of personal data protection in the legal, social, organizational and technical areas. The model provides an improvement strategy, rules and processes, and compliance indicators in addition to outlining the personal data protection requirements for each level. As well as, in this thesis a novel methodology has been used to evaluate the proposed model. It uses SOAR (Strengths, Opportunities, Aspirations, and Results) analysis to evaluate the stages and combines it with the Analytic Hierarchy Process (AHP) to determine the feasibility of the model. The study's findings demonstrate that the model is suitable for adoption and is acceptable. The model is thus a workable choice for establishing an e-government in developing countries.

Contents

Introduction

With the growing use of the internet and increasing its reliability, attacks on computer networks increased. The unauthorized access to personal data is one of the main concerns of data owners which happen sometimes without their consent. Therefore, personal information is more vulnerable to the risk of computer crime and computer misuse. Hence, security and protecting data have to be considered with designing and developing any kind of information systems. Attackers can access a large volume of data easily when there is a simple error in the information system. Protecting personal data and privacy confidentiality plays a great role in guaranteeing user trust in government information systems. Having an issue with privacy obstructs the progress of the e-government system and most possibly causes citizens to lose reliance on public e-services. Many factors are associated with privacy protection in e-government systems. According to the works of literature, Protecting private information requires four vital layers which are legal, organizational, technical, and social [2].

In developing countries, adoption and usage of electronic government (e-government) services is still a major challenge. Some of the significant difficulties faced with e-government initiatives include a digital gap among the people, inadequately delivered e-government services, and people's availability and access to technology. Although these challenges will inevitably arise in developing countries, governments will be able to gain more stakeholder engagement in e-government activities if suitable precautions are implemented when planning e-government programs. The design of e-government initiatives is guided by e-government maturity models, which are often named stage models. [4] said that a growing proportion of e-government projects in developing countries are failing to fit with e-government trends.

In order to identify the strengths, weaknesses, and success factors of e-government models, the authors have analysed various e-government stage models in the literature. Although they are based on different perspectives and employ a variety of e-government concepts, these models appear to vary from one another. For local governance in developing countries, the authors propose an e-government stage model based on several factors such as legal, organizational, technical, and social considerations. These are important to consider when starting an e-government project in developing countries. The six phases of the proposed e-government stage model (Requirements, Information, Awareness, Interaction, Transaction, and Integration) are cantered on protecting personal information [5]. To analyse both the supply and demand side, the SOAR (Strengths, Opportunities, Aspirations, and Results) technique is utilized as a tool. However, it is challenging to choose an e-government stage model using only the SOAR analysis, as many qualitative factors must be considered. These aspects are nearly linguistically ambiguous and have no definite value [6]. To overcome this challenge and analyse the SOAR components methodically, as well as take these variables into account in a hierarchical structure, the Analytic Hierarchy Process (AHP) approach is used.

Problem Description

Personal data is an important and growing concern when accessing information and services through the internet or intranet. More and more personal data are collected everyday by government websites and e-service providers. This data can potentially be aggregated and used to build personal profiles, raising the fears that it can be used for unauthorized purposes that may affect its owners. Most of researches has been done on legal aspect of protecting personal data while in many countries' government laws have not kept pace with technological and organizational structure change. However legal factors have role in protecting personal data but organizational, social and technical

aspect cannot be avoided because they have a great influence in increasing citizen's trust to e-government services. Therefore, having a model with embracing the four aspects (law, technical, organizational and social) is very necessary for protecting personal information in e-government. Since in most of the developing countries, national law for protecting personal data is missing and security controls of technical, organizational and social are not considered. Besides, there is a gap among e-government maturity models for protecting personal data because there is not a specific stage in the existing models that pay attention to personal data security while this factor has a crucial role in increasing citizen's participation in e-government services in developing even developed countries. The existing e-government models pay attention to technical security in transaction stage while this stage is in the third level in the most of the models. Therefore, it cannot play its role in raising citizens believe to the e-government services in the initial steps. According to our point of view, trust can obtain by providing privacy protection and security in terms of legislation, technical, organizational and social awareness is the key factor of protecting privacy. The figure (1) shows the Trust Architecture in e-government.

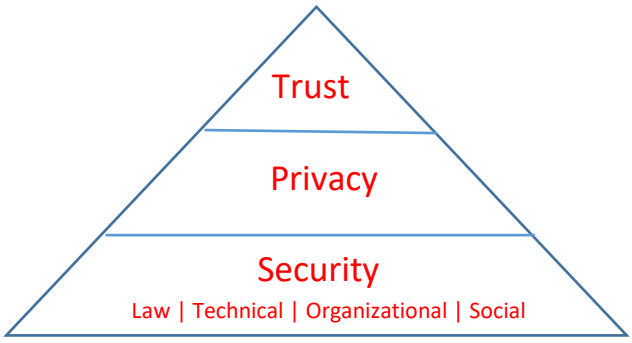

Figure 1 Trust architecture in e-government [1]

According to the literatures, the stage models that followed by most of developing countries are not considered the privacy principles, organizational requirements and social awareness while the national law for privacy protection is missed in these countries and they are not followed the international standard. As well as, high level of technical security is not performed in order to raise trust of citizens to the e-government. Thus, e-government model of developing countries must consider personal data protection in all stages.

Thesis Objectives

This thesis deals with privacy information within electronic forms of government organizations. The previous works on this field and the current situation of PPI in the world show that an e-government model based on privacy protection is necessary. Thus, the main goal of this dissertation is:

Propose an e-government stage model based on privacy protection in developing countries. To achieve the main goal, it will be necessary to meet the following sub-goals:

- Assessing existing e-government models in term of personal data security.
- Evaluating e-government websites in term of privacy principles.
- Identifying security requirements for e-government services.
- Investigating threats on personal information within e-government processes.
- Proposing a security model for protecting privacy information in government organizations.
- Proposing an e-government stage model for protecting privacy information.
- Verification of the proposed e-government stage model.

There is a serious issue in the digital era with the growing amount of personal data being collected by government websites and e-service providers. Legal actions are necessary, but they are not sufficient to handle the complex issues brought about by changing organisational structures and technological breakthroughs. Establishing trust in e-government services requires a comprehensive strategy that takes organisational, social, legal, and technical aspects into account. Therefore, maintaining personal data security and promoting public trust in e-government services require closing the gap in current models and placing a strong emphasis on privacy protection and security awareness in all domains.

1. State of the Art

1.1 E-Government Challenges

There are many different challenges in e-government. These challenges are influenced by different conditions including social, economic, political, cultural, education, etc. These can be grouped into human resources categories, which consist of training, motivating, educating, skill shortage, and unspecified other human resources. According to infodev.org, ”successful e-government is at most 20 % technology and at least 80% about people, processes, and organizations” [11]. On the other hand, some several challenges and barriers can delay the progress of e-government implementation. The variety and complexity of e-government initiatives imply the existence of a wide range of challenges and barriers to their implementation and management. The implementation of e-government faces some technological difficulties such as a lack of shared standards and compatible infrastructure among departments and agencies. Also, privacy and security are critical barriers to the implementation of e-government in citizen concerns [6]. The guarantee by the government will not suffice unless accompanied by technical solutions, transparency of procedures, and possibly

independent auditing. Also lack or weakness of ICT infrastructure is one of the major challenges for e-government implementation. Internetworking is required to enable appropriate sharing of information and open up new channels for communication and delivery of new services [12].

For a transition to electronic government, an architecture, that is, a guiding set of principles, models and standards, is needed. Many developing countries suffer from the digital divide[1] , and they are not able to deploy the appropriate ICT infrastructure for e-government deployment. E-readiness and ICT literacy[2] are also necessary in order for people to be able to use and benefit from e-government applications. Having the education, freedom and desire to access information is critical to e-government efficacy. Presumably, the higher the level of human development, the more likely citizens will be inclined to accept and use e-government services. Therefore, governments should work closely with the private sector to establish a modern infrastructure that will provide access opportunities to disconnected groups and individuals. This lack of infrastructure is cited as one of the primary barriers to e-government implementation [3]. Figure (2) show the challenges in e-government implementation.

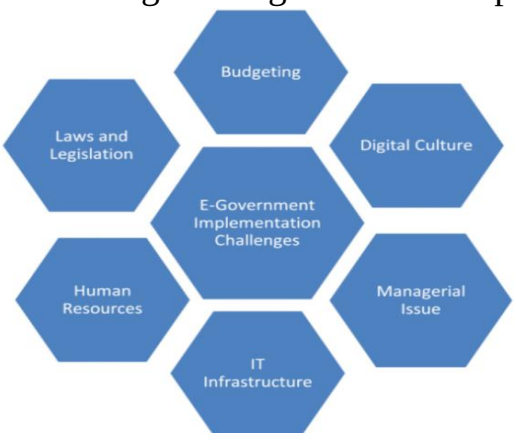

Figure 2 Challenges framework in e-government implementation [22]

[1] Digital divide refers to the gap in opportunity between those who have access to the Internet and those who do not.
[2] ICT literacy is: using digital technology, communications tools, and/or networks to access, manage, integrate, evaluate, and create information in order to function in a knowledge society.

1.2 E-Government Model Approaches

As electronic government projects are aimed to reduce costs and provide a greater range of services to their users compared to the traditional method, it is especially important to adopt an appropriate design and implementation approach. The electronic government projects could be distinguished as technology-centric and user-centric based on the design approaches. Generally, there are three main approaches to developing and designing e-government models as shown in figure (3). The first approach comes from international organizations such as; the UN (2001, 2003, 2005, 2008). The second approach is provided by consulting companies such as Gartner group, and Accenture, 2003. The third approach is proposed by researchers [12].

First approach: this approach has been designed by the UN (UN, 2001, 2003, 2005, 2008) for developing an e-government model [8].

Second approach: The second approach is by Gartner group that consists of four stages [14].

Third approach: The third approach as presented by individual researchers. The models that proposed by researchers are different in stages. [15].

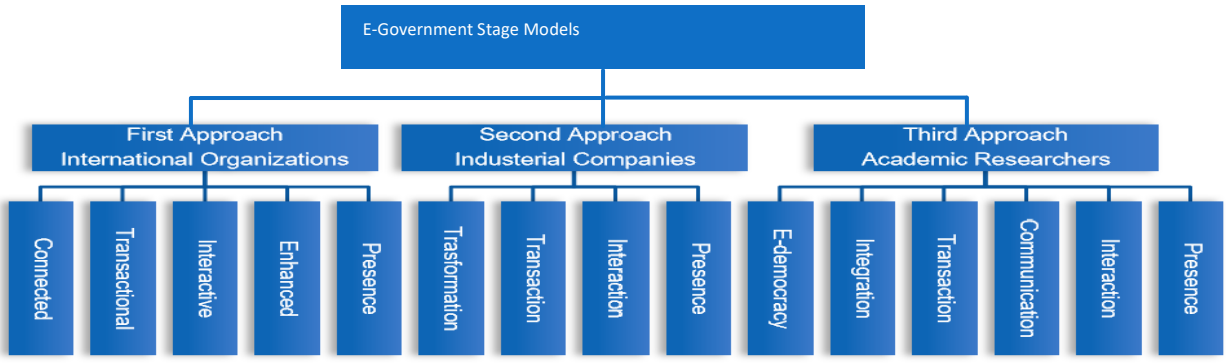

Figure 3 E-government stage model approaches [21]

1.4 Critical Analysis of Existing Stage Models

In the context of the UN's e-government model argued the automation of back office at the last stage. However, without automating front/back offices how can transaction occur? While stated in the transaction stage there is a two-way communication. Therefore, the researchers believe that the infrastructure of front/back offices should be initiated at the early stage at least for certain government institutions, in order to provide an opportunity for government authorities to process citizen's transactions accurately and promptly. Furthermore, the model made no reference to the availability of multi-channel delivery of services in any of the stages. While, protecting privacy information is not well demonstrated in order to motivate citizens to participate[18][16][19].

The second approach as proposed by the Gartner group which is a simple and brief state where it is not necessary to start at the first stage and work its way through all of the stages. The researchers believe that it is essential to start from the initial stage and develop the system step by step without skipping any stage to successfully complete the system. This is due to the fact, that all of the stages are interconnected together. Particularly in developing countries due to their cultural attitude and societal traditions towards technology[15]. It does not refer to the challenges that impact the success and failure of the model such as: technological, economic, political, and, societal. In addition, the model argues that transformative e-government initiatives commonly look for the removal of the organizational obstructions that encourage an institution-centric approach and, instead, encourage a customer-centric approach. However, because, in the initial stages the aspects that impact protecting privacy information are not considered particularly the law and organizational requirements. [14][10][13].

The third approach of an e-government model is that proposed by academic researchers. These models are not away from shortages. According to most of them, the models focus on the naming of stages, while security requirements are disregarded at

the stages. Some of the models have not considered the issues that influence the success and failure of e-government implementation such as; technology, political economy, organizational and, societal requirements. Almost all models in this approach emphasize that the assimilation of electronic governments occurred in a linear manner where the e-government project progresses from simple to complex technology. [17][20].

2. Protecting Personal Information in E-Government of Kurdistan Region of Iraq

Kurdistan Region is located in the North of the Republic of Iraq, it is an autonomous region with a population of 5 million approximately. Kurdistan Region Government (KRG) consists of 21 ministries and the region has four governorates. KRG has a long strategy plan for e-government deployment. There are only a few researches work on e-government in this area, [3] is one of the researches that has been done in (2015). It investigated citizen's attitudes to e-government acceptance in Kurdistan Region and shows some factors for not adopting e-government in the region without revealing the influence of privacy issues on Kurdistan e-government while people in this region are very cohesive to culture and traditions and they are very sensitive to their data. Besides the main objectives, this study targets in investigating PPI in Kurdistan Region Government [22].

To evaluate the current status of PPI in Kurdistan Region of Iraq, we made a research based on five principles which are the most used and necessary principles that repeated in all of these sets for assessing privacy protection in organizations. The five principal elements that we selected in our study are Notice, Access, Storage, Security, and Compatibility [23]. This research depended on two ways of methodology. The first

way was an online survey and the second way was website scanning. The online surveys have been done on two groups of participants for studying participant's attitudes in using government and commercial websites and investigating in using privacy principles by IT companies. The first group was online service users of both commercial and government websites. The second group is a small size group of respondents which are 16 respondents. Each of them is from an IT solution company and they are all IT specialists with different ages, gender, and business level. In general, the survey has been done by 16 IT companies in which they are the most powerful in the Kurdistan Region of Iraq. All participated companies developed IT solutions and websites for KRG organizations and private business companies. As well as, most participants in this survey are responsible for planning, managing, designing, and supporting IT solutions in their companies.

The second methodology of this research work was scanning those websites which collect personal information in term of privacy disclosures. For this purpose, the top of the most usable and dependable government and commercial websites were sampled. The number of government websites is (24) websites from a different government organization and (38) commercial websites are selected from various companies. In total (62) websites are scanned. However, this size is small but currently, only these websites are working on personal information because e-government in the region is in the beginning. We scanned the websites to find privacy disclosures. There are two main types of privacy disclosures: *Privacy Statement* and *Privacy Notice*. The simple definition of Privacy Notice is a place in the website that descript the site's practices which is reachable by a hyperlink or a button. But Privacy Statement is a separate statement that describes the website's policy of collecting data and how using it. In the first group survey, we assessed people's understanding of privacy protection and their preference for protecting their data. On the other hand, in total approximately

(83 %) of participants are government or private sector employee which means they are familiar with government and commercial websites. The questionnaire contains six questions that associated with three domains which are:

- law of protecting personal data,
- trust to websites,
- manipulating with personal data.

Questions one and two are about legislating data protection law and punishing disobeyed data controllers. As indicated in the figure (4) more than (75 %) of respondents prefer to legislate a law regarding protecting personal information. From figure (5) we understand that most of those people who prefer to have a law they would like to have strong law enforcement for punishing breaches.

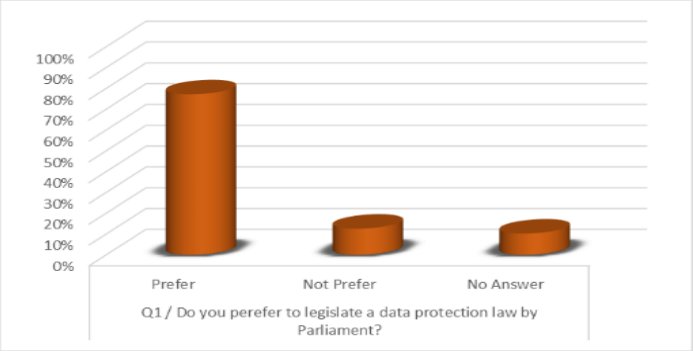

Figure 4 Legislating data protection law [23]

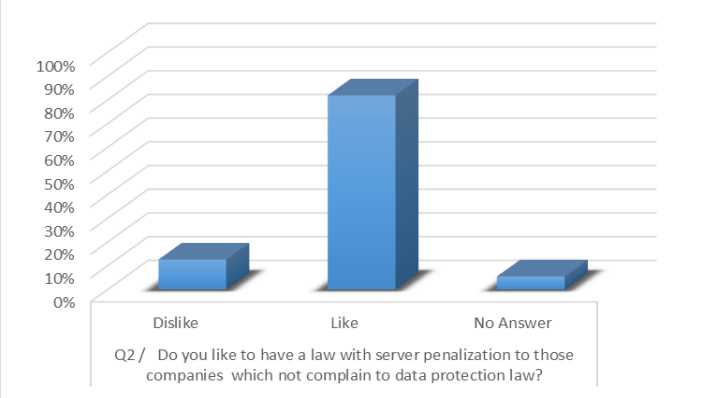

Figure 5 Penalty against disobeyed companies [23]

The participants are also asked about their trust in government and company websites. As it showed in figure (6) most of the respondents not trusted to the websites therefore they are not ready to give their real personal information. Besides, privacy disclosure has an important role in increasing trust in the websites. The answers to question four in the questionnaire indicate that most of the survey participants are not satisfied with those websites which collect personal data without any privacy disclosures. Rate of those participants is near to (75 %) of total participants as shown in figure (7)

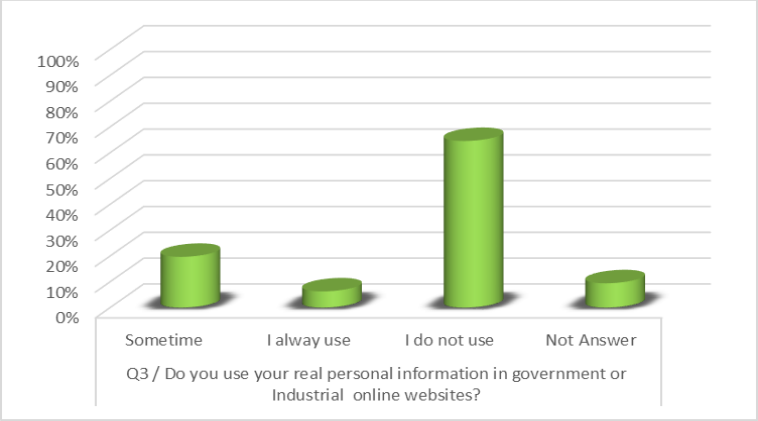

Figure 6 giving real personal information to websites [23]

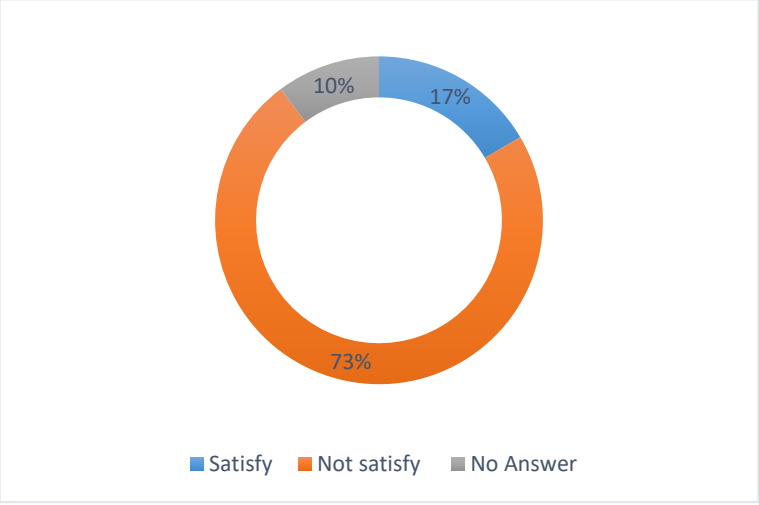

Figure 7 Satisfy websites without privacy disclosures [23]

The participants were asked about their attitudes about manipulating their personal information by the websites. As illustrated in figure (8) most of the survey participants do not agree with transferring their personal data to any third party without their knowledge or consent. Besides this, a high ratio of the respondents even not agree with transferring their data to the third party anonymous as shown in figure (9).

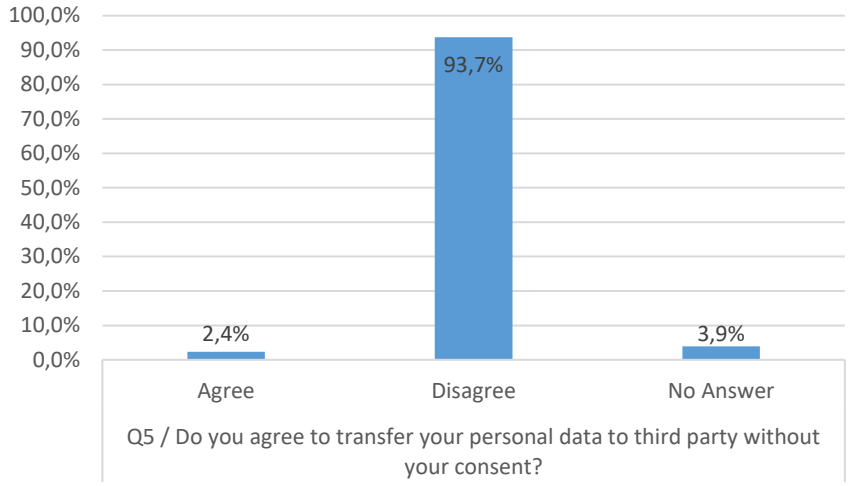

Figure 8 Transferring data to third party [23]

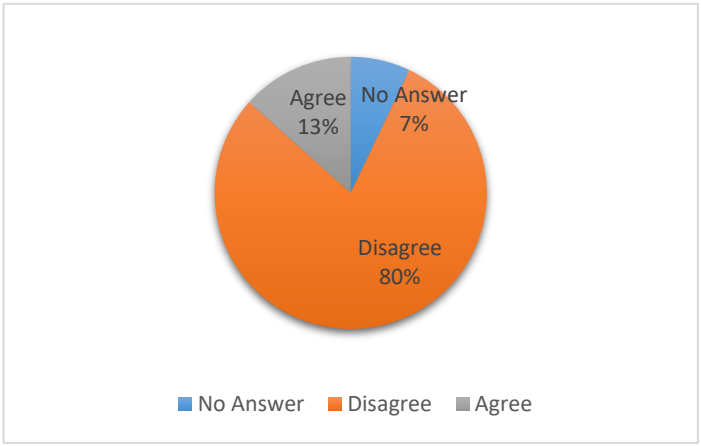

Figure 9 Transferring data with anonymous [23]

As discussed in the privacy principles section, there are a lot of privacy principles according to private agencies and organizations. In this study, only the most common

principles are selected which are available in all standards such as International Standard Organization (ISO), Federal Trade Commission (FTC), General Data Protection Regulation (GDPR), Fair Information Practice (FIP). The selected principles are Notice, Access, Storage, Security, and Accountability. These principles are concentrated in the second group survey. As described in the methodology section, the second survey has been done on 16 of the most famous IT companies in the Kurdistan Region of Iraq. According to the answers, however, most of the companies are have readiness for providing security layers for protecting personal information in their solutions as most of the answers for security principle is yes. But in implementing other principles they are insufficient because most of them did not follow the four principles (Notice, Access, Storage, and Accountability) in their works for government and companies. Figure (10) shows the ratio of implementing privacy principles by IT companies.

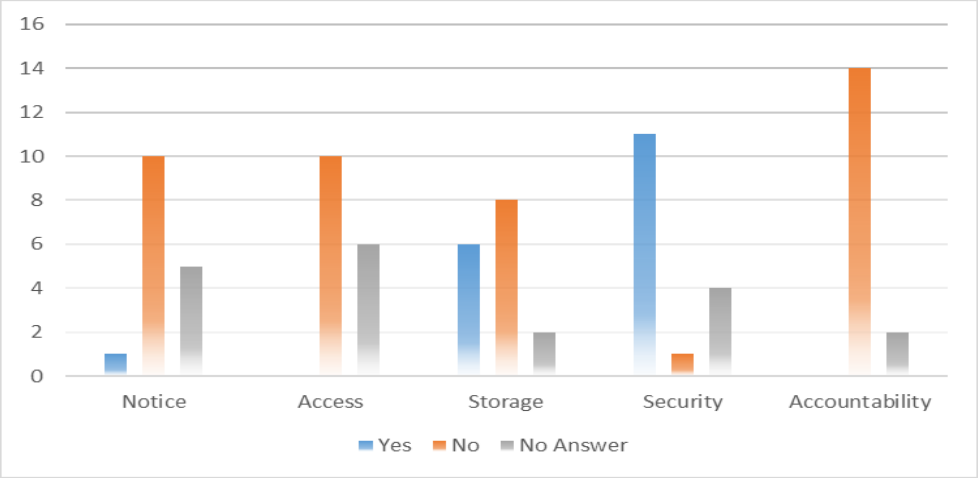

Figure 10 Implementing Privacy Principles by IT Companies [23]

The third investigation in this study is scanning websites to determine those which collect personal information. Based on this work principle we found 24 government websites and 38 commercial websites that providing electronic services

and collecting personal information. According to FTC, GDPR, ISO, and other agencies, data controllers should present privacy disclosures while asking for personal information. In our study, we noticed that most of the websites are collecting personal information without paying attention to their customers' rights. Figure (11) demonstrates that around (90%) of the websites collect personal data without having any privacy disclosures such as privacy notices and privacy statements only a small ratio of the websites have one of the privacy disclosures.

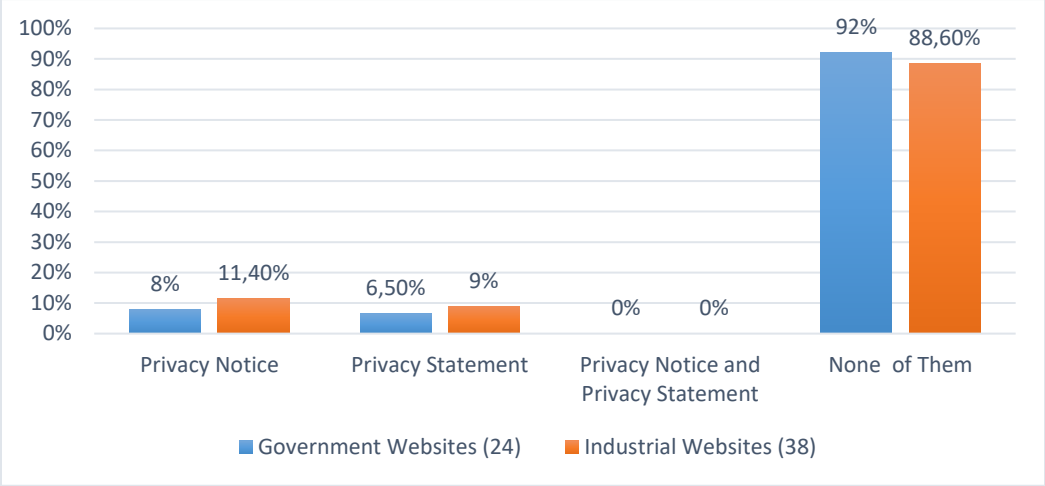

Figure 11 Privacy disclosures in the websites [23]

The study reveals that the majority of citizens in the Kurdistan Region are not ready to give their real personal information to governments and commercial websites and they are not satisfying government and commercial websites to access their personal data. Thus, they would like to have a strong law or regulation to protect their data and preventing data controllers from transferring or manipulating with their information without their consent. As it is clear that privacy principles play a great role in providing trust in e-government and commercial websites. The results in this research showed that most of the IT companies are not following privacy principles in their works for organizations. In another word, IT companies in the Kurdistan Region are not

obligated to follow any international privacy principles and they are not imposed to have security techniques for protecting personal information. On the other hand, most organizations are not carrying privacy disclosure on their websites which leads to losing their trust.

3. Methodology

To estimate the complex permittivity of single or multi-layered structures, this doctoral thesis utilizes a variety of techniques and methodologies. These are all described in this part. The subsections that follow provide a brief explanation of the scientific methodologies that have been employed, the data collection procedure, and the subsequent post-processing techniques that have been used to construct a mathematical model. The following techniques are employed to complete dissertation aims successfully. These methods are used in individual phases according to their needs.

3.1 Evaluation method

This is a systematic assessment of quality and value. The method is focused on the evaluation processes based on theory. This method is about collecting information and its professional processing to obtain documents for a possible decision. It also provides information for the initial consideration of options, and solutions and contributes to the formulation of a concrete conclusion. As well as, evaluation methods relate to the methodical procedures employed to judge the merit, utility, or significance of a given study, project, or intervention. These techniques are necessary to guarantee the reliability and validity of study findings. The following are some typical evaluation methods applied to this study:

3.1.1 Survey

Surveys on user satisfaction are carried out to get input from individuals and companies who have utilized e-government services. These surveys are used to measure

citizens' satisfaction levels, and trust to services, point out problems with service delivery, and gather suggestions for enhancements [24].

3.1.2 Expert Evaluation:

This is used to assess the usability and efficiency of digital platforms by experts in user experience design, data protection, human-computer interaction, or e-government systems. Their analyses assist in locating security layer problems and making suggestions for changes based on personal data protection. Besides, this method is used for evaluating the proposed e-government stage model in terms of personal data protection.

3.2 Analysis method

It is the process of decomposition of the whole into parts. There are an analysis property, examining relationships and facts from the whole to the parts. The analysis assumes, that each system examined can be decomposed into sets of elements that are connected by properties and individual bonds. This method will be used in examining security measures for e-government. Based on that examination and analysis, general requirements for protecting personal data in e-government processes is defined. Besides, Data analysis techniques are essential in the context of e-government studies for making sense of the enormous amount of data gathered through various evaluation methodologies [7]. Website analytics is used to examine website metrics such as page views, privacy principles, security, user demographics, and top content can yield useful information on user behaviour. Understanding which services are often used and how people interact with online platforms is made possible by website analytics.

3.3 Induction method

This method is depending on the derivation of general information. With the help

of induction, general conclusions are drawn on based on the findings about individual objects or phenomena. This method closely follows the previous methods. It is usually used to draw the conclusions from entire study. As well as, it is a logical process in which particular observations or examples are used to develop broader principles or ideas. Inductive reasoning entails drawing conclusions about the whole from small samples. In this study the following forms of inductive approach are used [1]:

3.3.1 Observation

This technique is used to study the e-government services, by taking instances or patterns, such as user behaviour, user trust to security of e-services [25].

3.3.2 Pattern Recognition

To discover patterns and regularities in how e-government services are utilized, what problems users encounter, and how governments address security problems this method is used. It has been used for close observation and analysis of particular cases. Data Gathering: Gathering information on certain e-government implementations or cases. Surveys, interviews, or case studies might be used in this [26].

4.4 Deduction method

New statements are deduced through deduction. So, the opposite is true induction. These methods will be used in the dissertation to determine conclusions, on the basis of the research carried out and the results obtained. Deduction technique, is a logical research procedure that involves deriving particular results from broader principles or hypotheses. In this thesis started with the hypothesis that already exists in the field of e-government, frequently obtained from published works of literature or the results of earlier studies. Thus, deductive reasoning is based on this principle [25].

3.5 Comparison method

This method is one of the experimental methods. They are assessed during the comparison of identical or different aspects of the examined objects or phenomena and

based on the results obtained, corrections are made. This approach is frequently used in many fields, including e-government research, to learn more about the relative efficacy, effectiveness, or impact of various approaches, initiatives, or policies. It is also used to compare e-government stage models in terms of personal data protection.

3.6 Modeling method

Modeling is a method often used in scientific practice in many fields. The aim of using this method is to mimic the behavior of the investigated system and influence its behavior in the desired way. The model is always only by approaching a real object, which can be unlike a model, much more complex. In this step, an e-government stage model will be proposed based on technical and non-technical security requirements. Moreover, it is used to better comprehend complex systems, make predictions, or test hypotheses, which entails generating simplified models of real-world occurrences. Modelling techniques in e-government research applied to replicate a variety of aspects of digital governance projects, such as user behavior, service delivery workflows, and policy consequences. In this thesis, system Dynamics Modelling is introduced to concentrate on the connections between various systems components.

4. Proposing an E-Government Stage Model

With improvements in Internet technology, the majority of governments throughout the world have adopted Information and Communication Technologies (ICTs) to deliver more efficient and effective services to their agencies, companies, and people. In general, e-Government refers to the use of information and communication technologies (ICTs) by government agencies to offer and improve public service delivery. Developing countries are extremely enthusiastic about implementing e-government. But these emerging countries are still in the beginning stages of development and suffer from shortages. In e-government, individuals are concerned

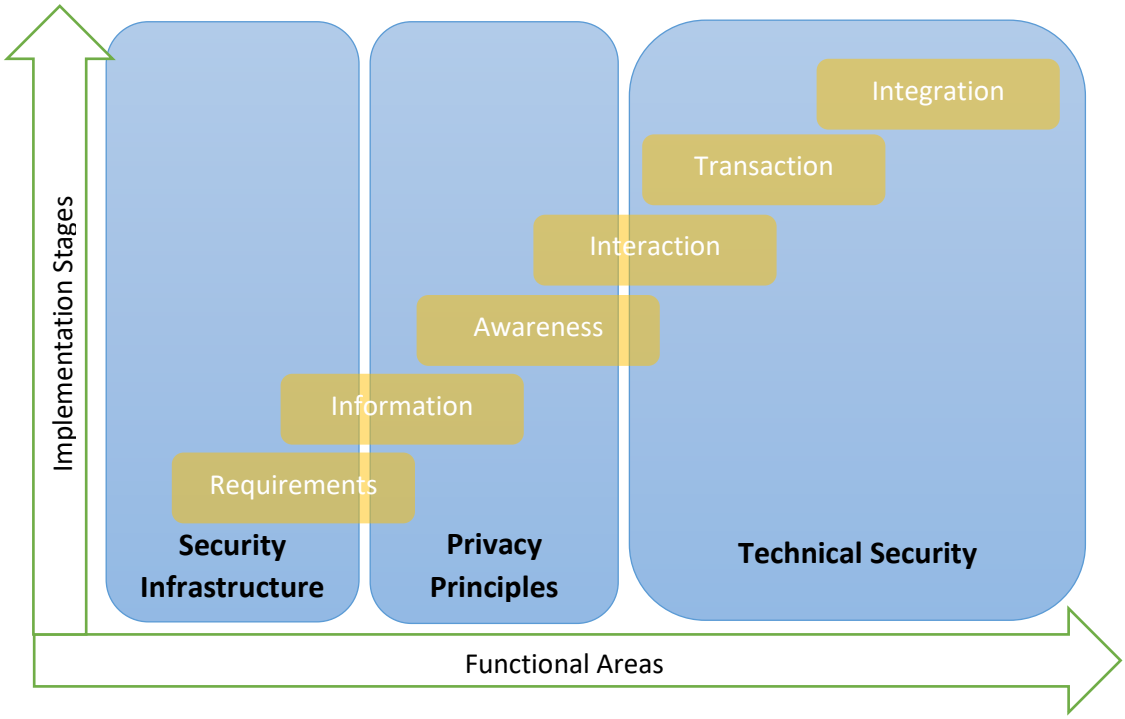

Figure 12 Functional areas of proposed model

about their privacy since e-government frequently deals with personal information. The figure (12) demonstrates the functional areas of the implementation stages of the proposed model. This article studies the concerns and obstacles that affect personal information security in e-government, considering the majority of security viewpoints, this research proposes models of e-government from the perspective of protecting personal data. The study is qualitative in terms of methodology, it depends on documentary studies, research techniques, content analysis, and comparative study.

5.1 Personal Information Protection Success Factors

Any e-government program must handle availability, confidentiality, integrity, and accountability concerning citizens' personal information, and information security is a critical obligation. A high degree of security will boost trust and confidence among all stakeholders (people, corporations, and government), providing a basis for a successful e-government initiative [4].

In most of developing countries, one of the major obstacles to the effective deployment and usage of e-government services is information security. Users will use e-government services only if they feel secure and trust that their personal information is protected, according to the studies, because using e-services requires exchanging sensitive personal data over the Internet. In case of applying and select the required and suitable security measures for protecting personal information, the system assets must be recognized, as well as the perceived threats and vulnerabilities analysed. It is critical to consider non-technical issues as well as technological aspects while attempting to increase the security level of personal information. The findings are then evaluated in terms of how they might be handled in order to improve people' online trust and, as a result, increase their participation [27]. Thus, personal information security is influenced by four main factors: law, social, organizational, and technical as showed in table (1). The weight of importance of each factor is calculated via Subject Weighting Method which is based on the judgment, opinions, and subjective impressions of individuals, experts, or stakeholders participating in a specific decision-making process, of giving weight or priority to certain aspects or criteria. Subjective weighting is qualitative in nature and relies on the qualitative judgment of people who have knowledge or experience connected to the issues being examined, in contrast to objective approaches that rely on statistical data and quantitative analysis. The technique was relayed on a survey that was made by over 20 information security specialists and academics. The weight of importance is categorized into four types which are Extreme Important (EI), Very Strong Important (VSI), Strong Important (SI), and Moderate Important (MI)[21].

Table 1 Impact Factors on Security of Personal Information [21]

Personal Information Security	Law Factors (VSI)	National Law (EI)
		Regulation (VSI)
		Self-Regulation (MI)
		International Standards (SI)
	Social Factors (MI)	Awareness (SI)
		Trust in Government (VSI)
		Attitude and Beliefs (SI)
		Education (SI)
		IT Literacy (SI)
	Organizational Factors (SI)	Flexible Strategies (SI)
		Plans (EI)
		Management (EI)
		Training (VSI)
	Technical Factors (VSI)	Perimeter Security (MI)
		ICT Infrastructure (EI)
		Internal Security (VSI)
		Access Management (VSI)
		Encryption (SI)
		Network and Cloud Security (VSI)
		IT Specialist (SI)

5.2 Proposed model

Many different e-government stage models have been presented by individual researchers. The models offered by researchers vary in terms of phases. They are offered models that are based on numerous terms and events. There are four to seven stages in

all. The general stages are web presence, interaction, communication, transaction, integration, and e-democracy [7]. These models are not mainly focused on security issues. The majority of them claim that the models place too much emphasis on stage names while ignoring stage security issues. Some models do not take into consideration the organizational, sociological, political, and technological needs that affect whether e-government implementations are successful or unsuccessful. The majority of the models in prior studies emphasize that the adoption of electronic government happens consistently, with e-government initiatives moving from basic to complex technologies. All current e-government maturity models recommend that the transaction stage be implemented before the integration stage. However, without the integration of e-government services at multiple levels and the current provision of sufficient security, transactions will not be completed. On the other hand, starting at the bottom and ascending from there up is not required. It is required to start at the beginning and build the system step by step, without skipping any stages, in order to correctly complete it. This is due to how intricately each step is woven into the others, due to their social and cultural views toward technology, particularly in developing countries [5]. The proposed stage model consists of six phases, as shown in figure (13).

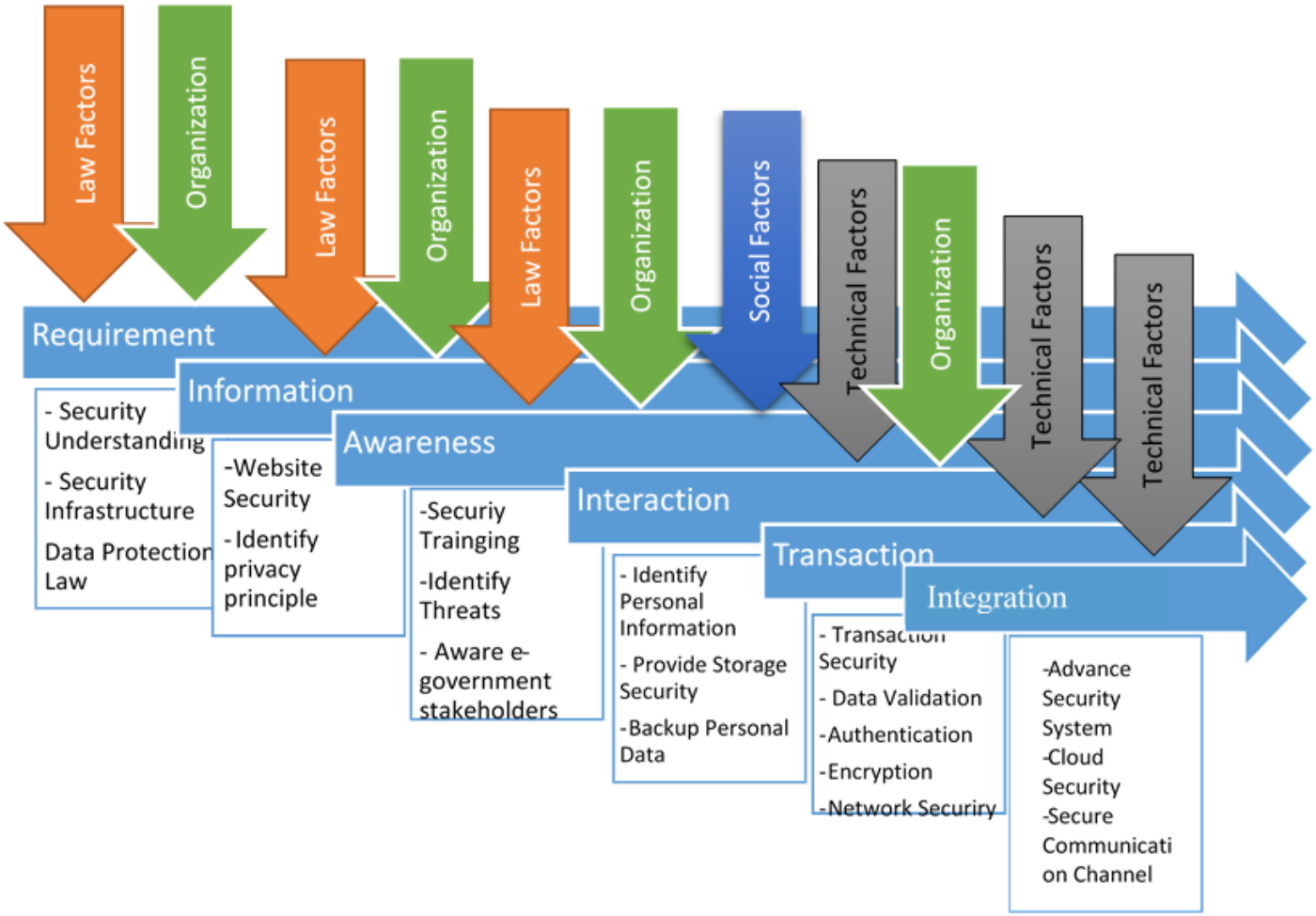

Figure 13 Six stage e-government model [21]

Based on international norms, the privacy concept should be addressed. The Requirements and Awareness phases are unique to this model since they were not present in prior models that were proposed to the developing countries. In countries where people have just opened up to new technologies, awareness is a different stage that requires greater attention. Employees of government stakeholders should be taught at this point to ensure that they have a sufficient understanding of security and the protection of personal information. After this step, the government may carry out everyday operations in their companies using forms, and consumers can download the forms and manually submit their requests. Personal information is backed up in each organization while maintaining a high level of storage. Organizations and technological factors are assessed at this stage. Because the transaction stage involves a two-way communication between government agencies and individuals, the most technical challenges arise in the transaction and integration stages. As a result, the majority of security techniques, such as transaction security, data validation, encryption, authentication, and network security, are necessary at this point. All government websites are shown on one page during the engagement stage.

5. Assessment of the Proposed E-Government Stage Model

5.1 Assessment Methodology

According to the literatures, it is crucial to assess e-government systems before they are put into use, since doing so would be a budget-wasting waste. Contributors who invest in e-government initiatives are increasingly insistent that the financed programs utilize qualitative and quantitative methods to assess their impact and performance. Over the past ten years, the Strength, Opportunities, Aspirations, and Results (SOAR) analytical approach has become a popular tool for planning and analysing strategic initiatives.

An organization can interact with its surroundings and develop business strategies by using this method to determine environmental correlations. For more than 20 years, SOAR has gained a reputation as a framework that offers an adaptable method for strategic thinking and strategy development. By involving pertinent stakeholders, SOAR facilitates planners' understanding of the entire system and encourages those in charge of strategic planning to involve stakeholders beyond top management. Citizens, workers, clients, suppliers, and the communities that the system affects can all be considered stakeholders. Therefore, it is very suitable for use in assessing e-government stage models [14,15]. On the other hand, it is crucial to utilize a calculating approach that aids decision-makers in order to determine the feasibility of the suggested model's parts for implementation. The Analytic Hierarchical Process (AHP) is a multi-criteria decision-making process that makes use of hierarchical formation to illustrate an issue and then generate priorities for alternatives depending on the user's decision [9].

5.2 AHP-SOAR Calculation

The hierarchical structure of the evaluation process is achieved at this section. The upper level is the main goal (G) which is evaluating proposed e-government stage model with considerations of protecting of personal data. The level below the upper level (second level) represents the essential targets (T) of the proposed model such as;

- T1: Improve security of personal Information
- T2: Achieve trust to E-government Services
- T3: Provide a reliable communication between Government and its stakeholders

Figure (14) illustrates the SOAR group factors. The SOAR group are represented at the lowest (third) level of AHP hierarchal.

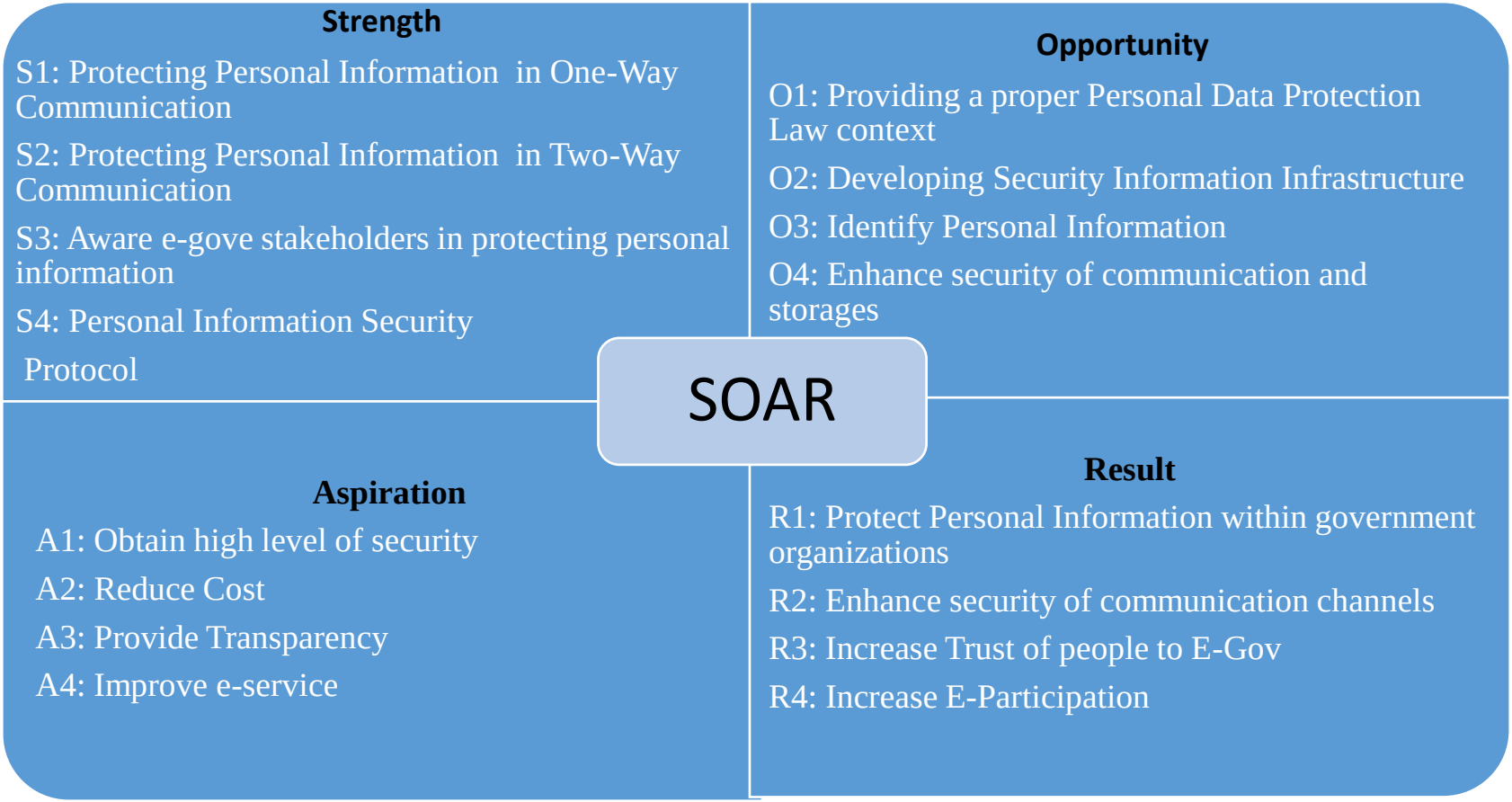

Figure 14 SOAR Group Factors for Proposed Model [28]

Figure (15) shows the hierarchical structure of AHP paired with SOAR factors of the proposed e-government stage model

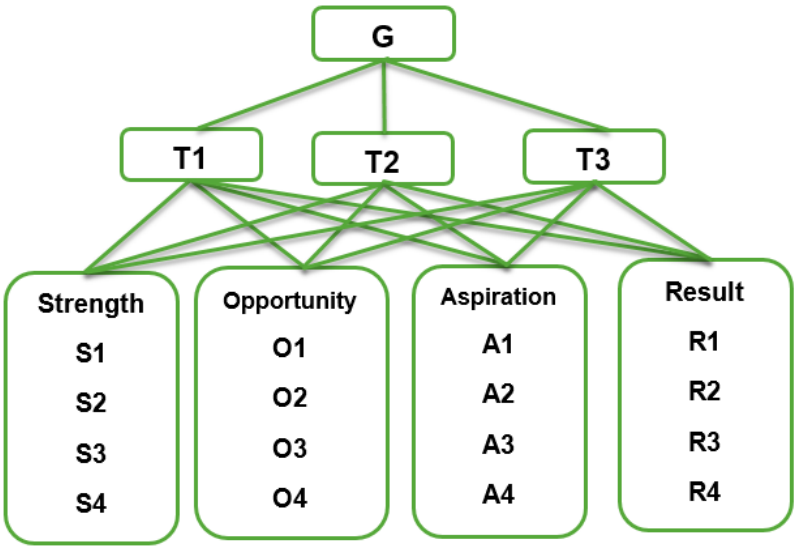

Figure 15 AHP Structure combined with SOAR Group Factors [29]

Numerous factors need be considered; in AHP, the number of pair-wise comparisons increases exponentially as the number of factors increases. As a result, the current method included four criteria for each of the four SOAR groups but only four of these factors will be used in this scenario. It is important to remember that, in accordance with [6], no more than 10 components should be included in each SOAR category. One comparison matrix will be used at level one to provide pair-wise comparisons of essential targets in relation to the assessment's goal. To determine the most important goal and use its values as a scaling factor, the first comparison matrix is 3 by 3 in size. Table (2) shows the local weight of the elements of each factor in the third level (Strength, Opportunities, Aspirations, and Results) calculated. The below table shows them along with their consistency ratios [28].

Table 2 local weight of the elements of each factor [28]

	Factor1	Factor2	Factor3	Factor4	CR
Strength	0.616	0.474	0.129	0.105	0.071
Opportunities	0.207	0.429	0.170	0.097	0.081
Aspirations	0.110	0.106	0.185	0.055	0.066
Results	0.068	0.125	0.204	0.063	0.059

The scaling of the second level's main targets is shown in table (3) of the AHP framework. In comparison to the other targets, the first target, which deals with protecting personal information, has a high degree. This element supports the main goal of the suggested approach, which is to protect personal information in e-government.

Table 3 The calculation essential Targets[29].

Targets/Criteria	T1	T2	T3	WS	CW	R	λmax	CI	CR
T1	0.723	0.50	1.44	2.660	0.587	4.532			
T2	0.103	0.07	0.04	0.215	0.081	2.671	3.066	0.033	0.057
T3	0.103	0.35	0.21	0.663	0.332	1.995			

The comparison of SOAR variables with respect to the first target (T1) is shown in table (4). The table demonstrates that strength and opportunity variables have higher worth than goals and accomplishments. It should be clear that all strength factors relate to protecting personal information to varied degrees. The stage model also allows the government additional opportunities to move toward creating a safe infrastructure for its e-services while adhering to the crucial objectives.

Table 4 The calculation of SOAR factors with Respect to T1[29]

Factors	S	O	A	R	WS	CW	R	λmax	CI	CR
S	0.516	0.929	0.403	0.362	2.209	0.605	3.652			
O	0.172	0.310	0.403	0.362	1.246	0.227	5.498	4.229	0.076	0.084
A	0.172	0.103	0.134	0.121	0.530	0.122	4.355			
R	0.057	0.034	0.027	0.040	0.159	0.047	3.413			

The importance of the factors within the SOAR groups can be observed in table (5). There are four elements in each group. The table demonstrates that the first strength component, which is concerned with protecting personal data in one-way communication, will be given top attention. This is crucial since, starting with the first form of communication, personal data is being stored by the government. The development of a secure information infrastructure, which is the second opportunity group factor, will be given high priority in the stage model that has been provided. On the other hand, successful e-government depends on secured communication and information infrastructure to achieve its objectives. One of the key successes of e-government is transparency. As a result, transparency will be given top emphasis in the suggested paradigm. The greatest value among the result factors is (0.059), which is represented by the four group factor values in the result group. This affirms that the model's implementation will increase the stakeholders' trust in e-government services, enhance the security of communication channels, provide a high level of security for Personal Information within government organizations, and increase E-Participation.

Table 5 Calculation of Factors within the SOAR Groups [29]

Alternatives (S Factors)	S1	S2	S3	S4	WS	CW	R	λmax	CI	CR
S1	0.627	0.596	0.989	0.499	2.712	0.627	4.321	4.192	0.064	0.071
S2	0.125	0.119	0.066	0.166	0.477	0.119	4.000			

S3	0.125	0.358	0.198	0.166	0.847	0.198	4.283			
S4	0.070	0.040	0.066	0.055	0.231	0.055	4.164			
Alternatives (O Factors)	**O1**	**O2**	**O3**	**O4**	**WS**	**CW**	**R**	**λmax**	**CI**	**CR**
O1	0.303	0.215	0.511	0.292	1.321	0.303	4.357	4.219	0.073	0.081
O2	0.606	0.429	0.511	0.292	1.839	0.429	4.285			
O3	0.101	0.143	0.170	0.292	0.707	0.170	4.151			
O4	0.101	0.143	0.057	0.097	0.398	0.097	4.083			
Alternatives (A Factors)	**A1**	**A2**	**A3**	**A4**	**WS**	**CW**	**R**	**λmax**	**CI**	**CR**
A1	0.655	0.741	0.925	0.491	2.811	0.655	4.295	4.179	0.060	0.066
A2	0.093	0.106	0.062	0.164	0.424	0.106	4.006			
A3	0.131	0.318	0.185	0.164	0.797	0.185	4.310			
A4	0.073	0.035	0.062	0.055	0.224	0.055	4.107			
Alternatives (R Factors)	**R1**	**R2**	**R3**	**R4**	**WS**	**CW**	**R**	**λmax**	**CI**	**CR**
R1	0.292	0.237	0.388	0.314	1.230	0.292	4.214	4.158	0.053	0.059
R2	0.584	0.474	0.646	0.314	2.018	0.474	4.255			
R3	0.097	0.095	0.129	0.209	0.530	0.129	4.106			
R4	0.097	0.158	0.065	0.105	0.424	0.105	4.057			

In the AHP technique consistency index must be less than (10 %). Figure (16) shows the Consistency Index of the SOAR groups. Since the value of CI of result factors is lowest among them, which means practically it has more chance to achieve in the proposed model in comparison with the other group factors. In the end, this study found that the outcomes of combining SWOT and AHP decision support were acceptable for adoption. Making pair-wise comparisons gives the decision-maker the ability to consider the relative importance of the criteria or elements and to analyze the situation more precisely and intensely.

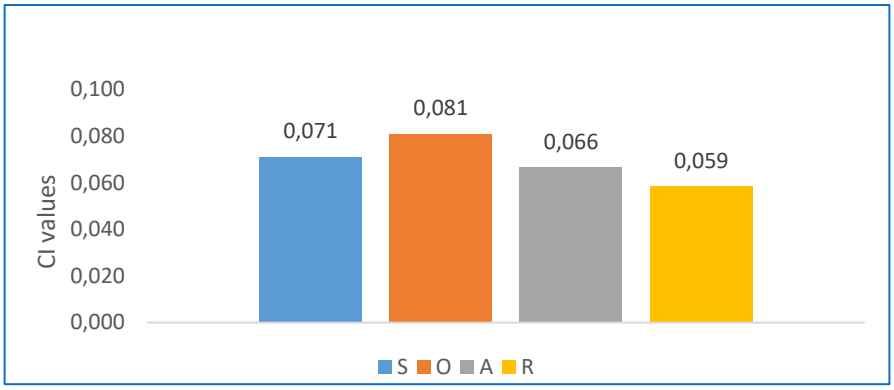

Figure 16 Consistency Index of SOAR Groups [28]

6. Conclusion

Numerous e-government stage models have been presented by individual academics. The stage structure of the models that researchers have proposed varies and generally, they are from four to seven stages. The primary focus of these models is not security-related. The majority of them argue that although stage security concerns are ignored, stage names are given excessive weight in the models. This study has nobility in considering security issues in designing an e-government model. In contrast to previous research, it particularly studies personal information security in all phases. This research considered the circumstances of developing countries in terms of impact factors on deploying technology. Therefore, the impact factors (law, social, organizational, and technology) are investigated.

The model covers each stage's data security requirement and provides an improvement plan, policies and procedures, and compliance indicators. In section (5.4) of this study, the evaluation of personal information security is calculated via a particular formula in each stage considering the impact factors of that stage. On the other hand, studies investigate e-government

implementation in developing countries. However, none of them considered the impact factors in developing countries. This research is the first to investigate law, organizational, sociological, and technological impact factors in developing countries. These factors are crucial to the effective deployment of e-government in developing countries. The sub-factors of the components are displayed in Table (4) of this research, along with the weight of importance of each element.

Additionally, this research examines the proposed model's strategic plan, which was overlooked by earlier models. SOAR framework (Strengths, Opportunities, Aspirations, and Results) is dependent on the strategic planning section. This framework provides a solid foundation for creating plans by enabling a strengths analysis to identify the model's strengths. Opportunities also allow firms to align their advantages with external conditions, ensuring that they are primed to capitalize on favourable trends. Aspirations articulate the organization's goals and vision, providing the strategic planning process with a clear direction and purpose. By defining precise, measurable, and attainable Results, organizations can also create realistic goals that align with their strengths and objectives. This approach aids in the development of a focused and effective strategic plan. Because of this, the SOAR framework not only evaluates the situation as it is now but also points organizations in the direction of a future in which their unique skills operate in tandem with outside opportunities to yield the intended outcomes.

Figure (18) in section (5.3) illustrates the SOAR group factors corresponding to the stages in the proposed model. As well as the combination of SOAR-

AHP has not been used yet in evaluating the e-government stage model in the literature. Which is academically a unique contribution of this research.

Another achievement of this study, providing a design of a data flow algorithm for the proposed model while such kind of algorithm is not available in previous studies as shown in Figure (17). The algorithm offers a secure channel across all websites and data operations.

This study is useful for developing countries, especially the regional governments of such countries in the world since the case study has been done on the Kurdistan region government in Iraq. Therefore, it is officially presented to the Department of Information Technology (DIT) of the Kurdistan Regional Government (KRG) in Iraq. DIT is the top management department and is responsible for stepping toward digital transformation in the Kurdistan Region of Iraq. This study will help KRG in securely digitalizing the organization and making a strategic plan based on protecting personal information which leads to gaining trust in e-services.

References

[1] H. Muhammad, "Protection of Privacy Information in E-Government," 2021.

[2] H. Muhammad and L. Ludek, "Managing Personal Data Security in E-Government Processes," *KOŠICKÁ BEZPEČNOSTNÁ REVUE* , vol. 10, no. 1, pp. 35–44, 2020.

[3] C. E. Azenabor, "Developing electronic government models for Nigeria: an analysis," 2013.

[4] N. K. A. Samara, "An information systems security framework for the e-government programme of Jordan," 2019.

[5] Y. Wu, "Protecting personal data in E-government: A cross-country study," *Government Information Quarterly*, vol. 31, no. 1, pp. 150–159, 2014.

[6] A. Y. Ni and A. T.-K. Ho, "Challenges in e-government development: Lessons from two information kiosk projects," *Government Information Quarterly*, vol. 22, no. 1, pp. 58–74, 2005.

[7] S. Sarwar, *Usage guidelines for CIECAM97s*. university of snderland, 2000, p. 224.

[8] S. M. Lee, X. Tan, and S. Trimi, "Current practices of leading e-government countries," *Communications of the ACM*, vol. 48, no. 10, pp. 99–104, 2005.

[9] A. Jawwad and X. Li, "User Trust in E-Government-management perspective," 2011.

[10] P. Joshi, "A Sustainability-Driven E-Government Maturity Model (SDEGM) from the Perspectives of Developing Countries," 2018.

[11] A. A. Hassan, "Status of E-Government in Iraq and what the challenges of development and implementation," *International Journal of Science and Research*, vol. 5, pp. 1511–1516, 2013.

[12] R. Meiyanti, B. Utomo, D. I. Sensuse, and R. Wahyuni, "e-Government challenges in developing Countries: A literature review," in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 2018, pp. 1–6.

[13] S. M. Shareef, "Electronic government adoption based on citizen-centric approach in regional government in developing countries: the case of Kurdistan Region of Iraq (KRI)," 2012.

[14] A. Fath-Allah, L. Cheikhi, R. E. Al-Qutaish, and A. Idri, "E-government maturity models: A comparative study," *International Journal of Software Engineering \& Applications*, vol. 5, no. 3, pp. 71–91, 2014.

[15] J. S. Hiller and F. Bélanger, "Privacy strategies for electronic government," *E-government*, vol. 200, no. 2001, pp. 162–198, 2001.

[16] A. Chaushi, B. A. Chaushi, and F. Ismaili, "Measuring e-Government Maturity: A meta-synthesis approach," *Seeu Review*, vol. 11, no. 2, pp. 51–67, 2015.

[17] D. Napitupulu, "e-Government Maturity Model Based on Systematic Review and Meta-Ethnography Approach," *Jurnal Bina Praja: Journal of Home Affairs Governance*, vol. 8, no. 2, pp. 263–275, 2016.

[18] N. M. Yaghoubi, A. Haghi, and S. Asl, "e-Government and citizen satisfaction in Iran: Empirical study on ICT offices," *World Applied Sciences Journal*, vol. 12, no. 7, pp. 1084–1092, 2011.

[19] H. Almuftah, V. Weerakkody, and U. Sivarajah, "Comparing and contrasting e-government maturity models: a qualitative-meta synthesis," *Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP WG*, vol. 8, pp. 69–79, 2016.

[20] N. Bhatt, “E-Governance Frameworks-Agenda Ahead,” 2007.

[21] H. Muhammad and M. Hromada, “Proposing an E-Government Stage Model in Terms of Personal Information Security in Developing Countries,” in *2022 IEEE International Carnahan Conference on Security Technology (ICCST)*, 2022, pp. 1–5.

[22] K. M. Ahmed and J. Campbell, “Citizen perceptions of e-government in the Kurdistan region of Iraq,” *Australasian Journal of Information Systems*, vol. 19, 2015.

[23] H. Muhammad and L. Ludek, “Evaluating Privacy Principles of Government and Commercial Organization Websites in Kurdistan Region of Iraq,” in *Studia Informatica*, Poland, Gliwice: Silesian University of Technology, 2020.

[24] J. W. Creswell and others, “Qualitative, quantitative, and mixed methods approaches,” 2003.

[25] L. K. Soiferman, “Compare and Contrast Inductive and Deductive Research Approaches.,” *Online Submission*, 2010.

[26] J. Saldaña, *The coding manual for qualitative researchers*. SAGE Publications Limited, 2012.

[27] J. P. Choi, D.-S. Jeon, and B.-C. Kim, “Privacy and personal data collection with information externalities,” *Journal of Public Economics*, vol. 173, pp. 113–124, 2019.

[28] H. Muhammad and M. Hromada, “Evaluating a Proposed E-Government Stage Model in Terms of Personal Data Protection,” *Applied Sciences*, vol. 13, no. 6, p. 3913, 2023.

[29] H. Muhammad and M. Hromada, “Evaluating an E-Government Stage Model by Using SOAR-AHP Process,” Transportation Research Procedia,vol. 74, pp. 1538–1545, 2023.

Abbreviations

AHP	Analytic Hierarchy Process
CDPR	General Data Protection Regulation
CI	Consistency Index
CR	Consistency Ratio
CW	Criteria Weight
DIT	Directorate of Information Technology
EI	Extreme Important
FIP	Fair Information Practice
FTC	Federal Trade Commission
ICT	Information and Communication Technology
ISO	International Standard Organization
IT	Information Technology
KRG	Kurdistan Region Government
MI	Moderate Important
POM	Practiced Organization Measure
PPI	Protecting personal Information
RI	Random Index
SI	Strong Important
SOAR	Strengths, Opportunities, Aspirations, and Results
UN	United Nations
VSI	Very Strong Important
WS	Weighted Sum

List Of Figures

List of Tables

Publications

Journals

1. Muhammad, H.; Hromada, M. Evaluating a Proposed E-Government Stage Model in Terms of Personal Data Protection. Appl. Sci. 2023, 13, 3913. https://doi.org/10.3390/app13063913
2. Muhammad, H.; Lukas, L. Privacy Protection in Conditions of Use CCTV Systems. Trilobit, 2021, Volume 2, ISSN 1804-1795, TBU FAI. Zlin, Czech Republic. http://trilobit.fai.utb.cz/privacy-protection-in-conditions-of-use-cctv-systems
3. Muhammad, H.; Lukas, L. Managing Personal Data Security in E-Government Processes. Kosice Security Revue, 2020, Volume 10, P35-44, University of Security Management in Košice, Slovakia. https://kbr.vsbm.sk/2020.html

Book Chapter

4. Muhammad, H.; Lukas, L. Evaluating Privacy Principles of Government and Commercial Organization Websites in Kurdistan Region of Iraq. Networking issues in innovative applications based on cyber-physical systems paradigm : praca zbiorowa, Chapter 8, P125-138, June 2020, ISBN:9788378807360

Conferences

5. Muhammad, H.; Hromada, M.Evaluating an E-Government Stage Model by Using SOAR-AHP Process. Transportation Research Procedia. 2023, Volume 74,Pages 1538-1545, ISSN 2352-1465, https://doi.org/10.1016/j.trpro.2023.11.131.
6. Muhammad, H.; Hromada, M. Proposing an e-government stage model in terms of personal information security in developing countries. Proceedings - International Carnahan Conference on Security Technology. 2022, vol. 2022-September,ISSN 1071-6572 (Sherpa/RoMEO, JCR), ISBN 978-1-6654-9363-5, DOI https://doi.org/10.1109/ICCST52959.2022.9896521
7. Hromada, M.; Bajera, Martin; Muhammad, H. Current Trends and Experience In Soft Targets Protection. The 34th European Safety and Reliability Conferences, Cracow Poland, 2024

Project

Number: IGMFAI/2020/005
Year: 2020.
Name: Identification and analysis of the information environment of the organization from the point of view of cyber security
Solvers: Miroslav Tomšů (tomsu@utb.cz)
Project guarantor: doc. Ing. Luděk Lukáš, CSc

Curriculum vitae

Hemin Akram MUHAMMAD

Address: **Iraq- Kurdistan Region – Erbil - Zanko**

Email: **hemnakram@gmail.com**

Mobile: ***+964 750 444 5565***

Marital Status: ***Married***

Date of Birth: ***19/05/1980***

EDUCATION

MSc. In Computer Systems Engineering **Kurdistan-Hawler University 2014 - 2016**

Rank: **First Class Honors**

BSc. In Information Technology **Kurdistan-Hawler University 2006 - 2010**

Rank: Second Class Honors

BSc. In Physics **Salahaddin University – Science 1999 - 2003**

Rank: **Second Class Honors**

HONORS AND AWARDS

- ✓ University of Kurdistan Hawler (UKH) - Dean's Certificate for superior academic achievement, 2015
- ✓ University of Kurdistan Hawler (UKH) - MSc Classification: First Class Honours, 2nd rank, 2016

RESPONSIBILITY AND EXPERIENCE

✓ **IT Systems Administrator**	**Czech Academic City (Czac)**	**2018-2022**
✓ **IT Engineer and Webmaster**	**Kurdistan24 Channel (K24)**	**2015 – 2018**
✓ **Database Manager**	**HSD Organization**	**2010-2014**
✓ **System Administrator**	**RCUPS Company**	**2007- 2010**
✓ **IT Support Officer**	**ETC**	**2004 – 2006**
✓ **Computer Instructor**	**Java Office**	**2004- 2005**

VOLUNTEER WORKS

• **2003 - 2004**	Blind Union of Kurdistan	**Radio Broadcasting Assistance**
• **2004 - 2005**	Awat Society for Fertility	**IT Officer**
• **2005 - 2018**	Physician Syndicate	**Head of Hawler Branch**

Ochrana osobních údajů v e-Governmentu

Protection of Privacy Information in E-Government

Doctoral Thesis Summary

Published by: Tomas Bata University in Zlín,
nám. T. G. Masaryka 5555, 760 01 Zlín.

Edition: published electronically
1st edition
Typesetting by: Hemin Akram Muhammad, MSc., Ph.D.

This publication has not undergone any proofreading or editorial review.

Publication year: 2024

ISBN 978-80-7678-260-0