REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

AN INTELLIGENT MODEL FOR VULNERABILITY ANALYSIS OF SOCIAL MEDIA USER

Master's Thesis

FIRYA RASHID ABUBAKER

ISTANBUL, 2016

REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

AN INTELLIGENT MODEL FOR VULNERABILITY ANALYSIS OF SOCIAL MEDIA USER

Master's Thesis

FIRYA RASHID ABUBAKER

Supervisor: Assist. Prof. Dr. PINAR SARISARAY BÖLÜK

İSTANBUL, 2016

REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

GRADUATED SCHOOL OF NATURAL AND APPLIED SCIENCES
INFORMATION TECHNOLOGY

Name of the thesis: AN INTELLIGENT MODEL FOR VULNERABILITY ANALYSIS OF SOCIAL MEDIA USER
Name/Last Name of the Student: FIRYA RASHID ABUBAKER
Date of the Defense of Thesis: 26-05-2016

This thesis has been approved by Graduate School of Natural and Applied Science

Assoc. Prof. NAFIZ ARICA
Graduate School Director
Signature

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Information Technology.

Prof. ADEM KARAHOCA
Program Coordinator
Signature

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Arts.

Examining Committee Members	Signature
Thesis Supervisor	
Assist. Prof. Dr. PINAR SARISARAY BÖLÜK	----------------------------------
Member	
Assist. Prof. Dr. TARKAN AYDIN	----------------------------------
Member	
Assoc. Prof. Dr. ERSIN OZUGURLU	----------------------------------

ACKNOWLEDGEMENTS

First of all, I like to all mighty god to give me this opportunity to finish this MSc thesis. Secondly, I would like to thank my advisor Assist Prof. Dr. Pinar Sarisaray Bölük for great supporting for my thesis, her kind and constrictive comments during my MSc thesis.

I would like to thank my jury members (Assist Prof Dr. Tarkan Aydin) and (Assoc. Prof. Dr. Ersin Ozugulu) for their valuable comments.

Special thanks goes to my family especially my parents who were always there for me to finish this MSc thesis.

I would also like to thank my cousin Dr. Saman Abdullah who helped and guided me from the beginning till the end.
Lovely thanks goes to all other friends who encouraged and helped in one way or other.

Istanbul, 2016 Firya Rashid Abubaker

ABSTRACT

An Intelligent Model for Vulnerability Analysis of Social Media User

Firya Rashid Abubaker

Information Technology

Supervisor: Assist. Prof. Dr. Pinar Sarisary Bölük

May, 2016, 89 pages

Every day, the number of online social network (OSN) users over the world are increasing, and the type of activities that performed by such users over online networks are increasing too. Such increase brings the interest of attackers and threats to penetrate network and computer systems more. These increase also affects the trends and the policies of attackers to get advantages from user vulnerabilities rather than system vulnerabilities to overcome systems and defeat OSN users. Studies have been done to investigate the policy of attackers that aimed to get over the OSN users, firstly, and then provide some awareness to OSN users, secondly. The aim of those studies is to educate OSN users with such awareness to minimize system infections. However, awareness is difficult for common users to understand, besides, there was no measureable figure for users to find out their vulnerability degrees against OSN based attacks and threats.

Our goal is to build an intelligent based model that is able to evaluate the vulnerabilities of an OSN user against the most common attacks and threats that are related to OSN user behaviors. The study has utilized Artificial Neural Network as an intelligent model, and has depended on the feed forward back propagation learning method. In this work, we have identified the relations between the policy of each focused attack and the behavior of OSN users. Our work has collected behaviors among 1000 OSN users in two countries, and through this process behaviors of (703) OSN users have been recorded. The collected records become an input data set to train and test the proposed intelligent model.

The accuracy of the proposed model has been tested against unseen data through training the model with the dataset that obtained from a country and testing it by the dataset that obtained from other country. The performance of the model has been checked through two different indicators; the first is root mean square errors (RMSE) and the second is mean absolute error (MAE). The best performance among indicators and tests is (1.5153e-08). The work has done another test by validating the model against an important intelligent models, which is SVM. Both performance indicators showed that ability of BPNN is better than SVM in this model.

KeyWords: OSN, Privacy and Security, User Vulnerability, User Behavior, ANN.

ÖZET

Sosyal Medya Kullanıcı Güvenlik Açığı Analiz için Akıllı Modeli

Firya Rashid Abubaker

Bilgi Teknolojisi

Tez Danışman: Yrd. Prof. Dr. Pinar Sarisary Bölük

Mayıs, 2016, 89 Sayfa

Her geçen gün, dünya üzerindeki Çevrimiçi Sosyal Ağ (ÇSA) kullanıcılarının sayısı çoğalmakta ve buna bağlı olarak da bu kullanıcılar tarafından çevrimiçi ağlar üzerinde gerçekleştirilen aktivite sayısı da artmaktadır. Bu artış saldırganların ilgisini çekerek, ağ ve bilgisayar sistemlerine nüfuz etmek için geliştirilen tehdit sayısını fazlalaştırmaktadır. Bu artış aynı zamanda saldırganların eğilim ve politikalarını da şekillendirerek, sistem açıklarından ziyade kullanıcı açıklarını yakalayarak ÇSA sistemlerine ve kullanıcılara karşı bir avantaj yakalama durumu yaratmaktadır. Bu alandaki çalışmalar birincil olarak ÇSA kullanıcılarını aşmayı hedefleyen saldırganların politikasını araştırmak için, ikincil olarak ÇSA kullanıcılarına farkındalık sağlamak için gerçekleştirilmiştir.

Bu çalışmanın amacı, ÇSA kullanıcılarının davranışlarındaki açıkları en yaygın saldırı ve tehditlere karşı değerlendirebilecek bir akıllı model oluşturmaktır. Bu çalışmada, akıllı model olarak ileri beslemeli geri yayılım öğrenme tekniğini kullanan

Yapay Sinir Ağlarından (İGYSA) yararlanılmıştır. Yapılan çalışmada, çeşitli saldırı politikaları ile ÇSA kullanıcı davranışları arasındaki ilişkiler tespit edilmeye çalışılmıştır. Çalışmada, Türkiye ve Irak'tan 1000 ÇSA kullanıcısının davranışları toplanmış ve bu süreçte 703 ÇSA kullanıcısının davranışları kayıt altına alınmıştır. Toplanan kayıtlar önerilen akıllı modeli eğitmek ve test etmek için girdi verisi olarak kullanılmıştır.

Önerilen modelin doğruluğu yine Türkiye ve Irak'tan toplanan, eğitim ve test için kullanılmamış yeni bir veri kümesi ile ölçülmüştür. Modelin performansı iki farklı gösterge aracılığıyla kontrol edilmiştir. Bu göstergelerden ilki karekök hatalar ortalaması (KHO), ikincisi de mutlak hata ortalaması (MHO) 'dır. Göstergeler ve testler arasındaki en iyi performans (1.5153e-08) 'dir. Yapılan çalışmada ayrıca önerilen model diğer bir önemli akıllı model olan Destek Vektör Makineleri (DVM)'ne karşı test edilerek onaylanmıştır. Tüm performans göstergeleri önerilen model olan İGSYA'nın DVM'den daha üstün performans gösterdiğine işaret etmektedir.

Anahtar Kelimeler: ONS, Gizlilik ve Güvenlik Kullanıcı Açığı, Kullanıcı Davranışı, ANN

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

AI	:	Artificial Intelligent
ANN	:	Artificial Neural Network
API	:	Application Programming Interface
Apps	:	Applications
BPNN	:	Back Propagation Neural Network
CSRF	:	Cross Site Request Forgery
DoS	:	Denial-of-Service
EU	:	European Union
FB	:	Facebook
FF-BPNN	:	Feed Forward Back Propagation Neural Network
FFNN	:	Feed Forward Neural Network
GUI	:	Graphical User Interface
IM	:	Instant Messaging
KRD	:	Kurdish Dataset
LAMSN	:	Location-Aware Mobile Social Network
MAE	:	Mean Absolute Error
NASAA	:	North American Securities Administrators Association
NN	:	Neural Network
OSN	:	Online Social Network
P2P	:	Peer-to-Peer
RMSE	:	Root Mean Square Error
SVM	:	Support Vector Machine
TPAs	:	Third Party Applications
TP	:	Third Party
TR	:	Turkish Dataset
URL	:	Uniform Resource Locator
XSS	:	Cross-Site Scripting

1. INTRODUCTION

1.1 OSN INTRODUCTION

Nowadays, the use of Online Social Networks (OSNs) is widely spread among the global internet community, with many people using various OSN platforms, such as Facebook (FB), Twitter, LinkedIn, etc. Every day millions of users from different countries, with different perspectives and interests, are active on OSNs, e.g. by uploading emotional information and downloading applications, as well as sharing and disclosing private information (Zhang and Zhang, 2012). In recent years, the use of OSNs has increased dramatically. People find OSNs very attractive as they offer many services, such as virtual relations with persons with similar hobbies and backgrounds. These interests make users spend more and more time on OSNs, also sharing sensitive data and updating their OSN profiles (Sadeghian et al., 2013, Fire et al., 2013). FB for example currently has more than 1.39 billion active members, 1.19 billion of which are mobile based users. This includes many adults. These numbers confirm that many people spend much time on communication (Facebook, 2014, Fire et al., 2013). However, many kinds of online behavior encourage threats and attacks, which are intended to penetrate systems through users' vulnerabilities rather than technical susceptibilities. Such kinds of penetrations are more frequent through OSNs due to the many new users. Only few users of OSNs are fully aware of privacy and security policies. All these factors make OSNs fertile areas for threats and attacks, and facilitate intrusion of the systems. Therefore, researchers are trying to study the behavior of OSN users and analyze attacks and threats to discover the relations between them. The main objective of researchers has always been to increase OSN users' awareness of privacy and security. In most cases, researchers have classified threats and attacks on OSN into privacy and/or security penetrators or intruders (Fire et al., 2014, Gao et al., 2011, Sadeghian et al., 2013, Daniel et al., 2014, Zhang et al., 2010, Guha et al., 2008). Furthermore, it provides recommendations and suggestions as solutions for OSN users to protect their privacy and security. A study presented by author (Fire et al., 2013) perfectly defined four groups of threats and attacks. In that study, the authors offered many commercial and scientific solutions for OSN users. However, it is not easy for users to understand the solutions suggested by researchers, because most OSN users are teens and young adults, who often do not have enough knowledge about privacy and security tools. In other studies (Daniel et al., Zhang et al., 2010), privacy, security, and users' behavior were discussed. They focused on one type of user vulnerability, namely Third Party Applications (TPAs). The authors of both studies highlighted the unique security and privacy design challenges posed by the core functionalities of OSNs, and some opportunities of utilizing social network theory to mitigate these design conflicts and provide possible solutions to limit the information disclosure. For both of the above cases it is difficult for users to understand and use those models and theories, as they are not sufficiently clear, and users would need plenty of time to learn them.

This study considers most common types of OSN attacks and threats. The OSN features and their mechanism are extracted thoroughly by threats and attacks which can be penetrate the systems. Those features are used to build several simple and understandable questions. From these questions, users will be able to check their vulnerability level through using an intelligent system, such as an Artificial Neural Network (ANN). The questions can also teach OSN users to avoid different types of undesirable behavior that increases their level of vulnerability. Furthermore, the questions can also provide users with knowledge about privacy and system security protection through minimizing undesirable behavior.

1.2 PROBLEM STATEMENT

The OSN phenomenon has become more popular among different ages of internet users and is targeted by many attacks every day. This leads researchers to work hard in this field to investigate different privacy and security related issues. According to various studies in the field of OSNs, researchers have attempted to find the best way to reduce the impact of OSN based threats to computer systems. The researchers defined various types of threats and risks facing OSN users during the registration and daily use. Although they built different models and recommended a variety of solutions to improve the users' privacy and security, those solutions could not help users to protect themselves or guide them away from hackers and other threats (Fire et al., 2013, Daniel et al., 2014, Sadeghian et al., 2013, Guha et al., 2008, Zhang et al., 2010). This is because most theories and models suggested by researchers need skills and experience in the security field. The usability of the suggested models is limited due to users' lack of awareness; hence there is no effect on OSN based threats.

None of the scientific studies have developed a simple model to analyze OSN users' behavior in relation to their privacy and security; hence they have no opportunity to review the level of their vulnerability on OSNs, and understand about desirable and undesirable behavior on OSN.

It is very necessary, as targeted by this study, to build a model that increases the awareness of users, identifies the vulnerabilities, and distinguishes between good and bad OSN user behavior.

1.3 RESEARCH QUESTIONS

The main research questions in this study could be summarized as below:

1. Is there any relation between the attacker's policies and OSN user behaviors?
2. How attacker's policies and user behavior interpreted to measurable levels?
3. How much the users' behaviors affect the privacy and security of OSNs?
4. How an Artificial Intelligent (AI) tools be learned to define user vulnerability level?
5. How users of different cultures can be utilized to generalize the proposed model?
6. Does the change in cultures affects the policy of attacks?

1.4 OBJECTIVES

The main objective of this study is to build an AI model that is able to identify the vulnerability level of OSN users through studying and analyzing their behavior. The model will identify the factors and parameters that are mainly associated with OSNs threats and attacks. Another objective of the work is increasing the privacy and security awareness of OSN users through using the proposed model. The objectives of this work can be achieved through the following targets:

1. To study attacks that are penetrating systems through the behavior and vulnerability of OSN users.
2. To investigate the relation between different threats and attacks with OSN user vulnerabilities.
3. To build an AI model that can detect the vulnerability level of OSN users.
4. To test and validate the proposed model against some performance indicators.

1.5 CONTRIBUTIONS

Researchers tried to enhance the security awareness of OSN users through classifying and identifying the threats themselves. Understanding security aspects and issues still require skills and experiences, which are not found among the wide range of OSN users. This research proposes an easy and intelligent model that teaches users the gaps where threats and attacks can penetrate their systems, and identifies the vulnerability level of the users. The study achieves this contribution through utilizing Back Propagation Neural Network (BPNN), as an artificial intelligence tool, to design the vulnerable identification and security awareness building model for OSN users.

1.6 ORGANIZATION OF THE THESIS

1. In chapter one, general information about OSNs and the popularity among internet users has presented. whereas, this chapter illustrated the main gap that this study wants to address it. The objectives that are designed to address the gap has been showed. Moreover, some questions that are to be answered, are also indicated in this chapter. Finally, the contributions of this work are stated as well.
2. In chapter two, a more detailed information is given on the works that have been done previously in the field of OSN security and privacy. The chapter gives the important solutions that have been proposed by pervious researchers. The chapter shows the gaps that have not been captured by previous researchers. The chapter also shows theory details about the tools and algorithms that are utilized by this work during building the proposed model.
3. In chapter three, the steps of proposed methodology have been explained in details. The explanation will be supported by different graphs and drawings to more visualizing the idea. The chapter explains the model in a sequenced approach. At each step, the role of the step will be illustrated and the impact of this step on the whole model is explained as well.
4. Chapter four explains the implementation of the model. The chapter shows graphs that are related to the code implementation. A part of this chapter shows the results of this implementation. Moreover, some detail on the findings are provided.
5. Chapter five is explaining and discussing the conclusion, the chapter also recommends some future works that could be done as a complementary extension for this work.

2. LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter, we discuss the work that has been previously been done in the field of OSN security and privacy in more detail. The chapter also reiterates an important solution that has already been proposed by researchers. Furthermore, it shows the gaps that have not been captured by the researchers. Moreover, this chapter illustrates theory details about the tools and algorithms that are utilized by this work while building the proposed model.

2.2 ONLINE SOCIAL NETWORKS (OSNs)

An Online Social Network (OSN) is a type of web platform (portal) that provides communication and information for internet users. Although they have a common structure, there are different types of OSNs with a variety of user interfaces (Joe and Ramakrishan, 2014), such as Facebook, Twitter, Myspace, Google+, Instagram, etc. Most of these OSNs provide and facilitate an interface which is officially called a profile. Under their profiles, registered users have the opportunity to exchange, share, and manage their activities with others (friends). Most activities are shared in the form of photos, videos, documents, events and feelings.

It becomes easy to find friends with the same interests through OSNs. The latest survey on OSNs shows that the number of active users has surpassed hundreds of millions. As an example, the famous OSN Facebook has 1,550 million of active users every month (Facebook, 2015). And every day, 19.6 billion information sharing activities are generated. This exchange of activities and data amounts to more than 300 Petabytes (Ho, 2015).

These vast activities, that occupy the internet and communication channels with such large volumes of information, are caused by the daily behavior of active users on OSNs. Day by day, more personal activities are uploaded and private information is disclosed. Even the facilities and services that provide OSNs set no limitations and constraints to this. This behavior puts the privacy of users at risk, as other users can abuse these facilities to extract private information. Information scams performed by hackers by means of certain techniques and tools are usually known as attacks or threats. Besides breaching users' privacy, the attackers are used to overcome systems with the intention to steal important data. As a result, the breach of privacy and system intrusion through OSNs could be considered as a second of intrusion is based on events over the internet.

In recent years, the increasing use of Online Social Networks (OSNs) has caused major concerns about security issues and privacy within these networks. This is why most researchers focus on this area. Most of the studies try to define and recommend the best model and mechanism for OSNs users to protect their sensitive and private personal information.

A study by (Zhang et al., 2010) discusses a general design and structure of OSN with reference to privacy and security requirements. The authors of that study propose a new infrastructure of OSNs in order to address a wide range of issues relating to privacy in order to prevent data mining and attacks (Zhang et al., 2010). Although the study provides good solutions for maintaining OSNs privacy and security, a decision on an issue needs a kind of collaboration among experts from the social science and network security communities, industry, regulatory bodies, and all other relevant communities, only OSN users can not have this access. Some studies have more specifically discussed threats and their impacts on systems through OSNs. One study explores the impact of third party applications on opening a back door for disclosing private information of OSN users (Daniel et al.). The work analyzes the behavior of OSN users through a survey among undergraduate and postgraduate students. The survey displays some statistics that demonstrate the relations between OSN user behavior and many threats that might attack systems through Third Party Applications (TPAs). The researchers show that users' low level of privacy concerns makes them vulnerable to malicious entities that pretend to be legitimate users. At the same time, the lack of basic security knowledge and negligence of prospective threats lead to maximizing the visibility of users' profiles. Despite the presence of that scenario and the solutions provided, that study offers no solutions to OSN users that would enable them to measure their levels of security and indicate their vulnerability.

More studies have been published that provide recommendations and suggestions for the problems that OSN users may face, however, the risks caused by users' behavior still cause privacy leaks and will result in leaking personal information.

2.2.1 Structure of OSN

As mentioned in the previous section, OSN sites are usually run by individual corporations (e.g. Google and Yahoo!) and are accessible for users through the web. Users of one OSN are connected to others through that OSN's web. Every OSN has features and functionalities that attract the interest of users. The nodes in this network are the users, and the functionalities of OSNs are the links that encouraging users to maintain their accessibility.

Users of OSNs usually access the pages through two different forms, individual user and group users (Mislove et al., 2007). For users to fully participate in an OSN, they have to register on a site; in some cases, by using a pseudonym, as some websites permit browsing of public information without the straightforward "explicit" requirement to sign up. Users may freely contribute information about themselves (e.g. their date of birth, home town, or habits), that is added to their profiles. For groups, most web pages encourage users to create and join particularly attractive groups. Users can post comments and texts to groups and upload shared content to the group. Definite groups are temperate; admission to such a group and postings to a group are controlled by a user created as the group’s admin "moderator". Other groups are unlimited, permitting any member to participate and share messages or content (Mislove et al., 2007).

The features and the functionalities of the OSN are other parts of the structure. Features of any OSN include allowing users to create a private profile, manage their connections and profile, and forge new connections based on common interests, location, and activities (Zhang et al., 2010). Below are some features that an OSN should have:

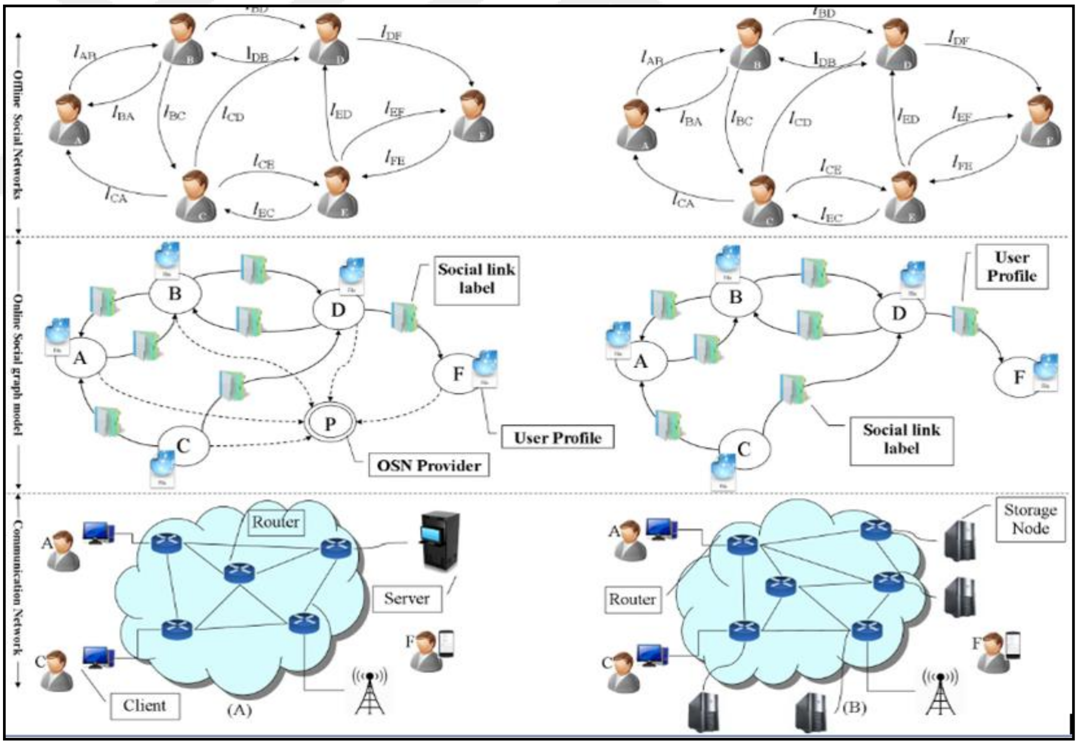
1. Personal Space Management: The OSNs have to support a user in creating/deactivating his/her account. This means that a user should be

permitted to easily setup or creates a new account on OSNs. At the same time, it is also necessary that the OSN should allow the user to change and modify his/her profile information. Moreover, the OSN should permit the user to upload/edit the uploaded content. The OSN’s profile and uploaded information will be the privacy of the user that through them activities will be seen by other registered friends.

2. Social Connection Management: The connection of OSNs users is provided with the official intent for them to keep in touch with their connections, a.k.a. "friend lists". Furthermore, to maintain existing social ties, the OSNs should support their users in restoring lost connections, and in making new connections with whom they have interests in common. Therefore, OSN should support users in creating/preserving/revoking a social relationship.
3. Means of Communication: The main purpose of OSNs is communicating with others. Therefore, there are diverse paths of connection among registered users. The first style is to post a public text, for example to share a video or upload photos on a profile by using personal space. This process could be achieved by setting up a specific user profile and joining via social connections. This process is known as a digital personal space. The second type is sending messages through private channels, i.e. one on one chatting in private. The final type is via Third Party Applications (TPAs), for communication such as online games.
4. Exploring Digital Social Space: OSNs support communication among their users to search for friends and create new social relationships (Fong et al., 2009).
5. Global Keyword Search (or Social Search): The main aspects of global keywords search are for finding the unknown users and listing them.
6. Social Graph Traversal (or Social Traversal): The concept of searching by means of a graph is that users can search for other contacts from friends' lists or a specific list of users.

In the real world, people have many relations and connections with each other, such as family, relatives, teachers, classmates, colleagues, etc. Some of these relations have been established because of common interests or area of work (physical or technical). However, in virtual life, like on OSNs platforms, people can make and get new friends without knowing them or meeting them in real life. These friendships may build on common habits and behaviors, or are just made for investigating and gathering new contacts. The OSN platforms offer more and more facilities and functions for their users. Therefore, the users can use these to communicate easily with each other, as shown in Figure 2.1. The type of communication will vary, for example, when users communicate privately with a friend no one can see what they talk about or what information is exchanged. Therefore, the users can communicate publicly, where most OSN users can see the information. The social networks have been used for different purposes in human life since they have been built to communicate but from that notion, it can be also used for other communication relations among individuals who may not know each other.

Figure 2.1: Types of communication and structures of OSN



Although communication in real life differs from that in virtual life, the process and mechanisms of communication in virtual life are more complex, as more experience and knowledge about tools and technology is needed for the sake of communicating with others (Strufe, 2009). On OSNs platforms the most important thing for the users' connections is a network. However, to build a strong network requires a lot of substance. The main parts of OSN networks are servers for storing data, creating policy/rules, and managing all users and information. Furthermore, the routers are used for connecting clients to servers or client to client to exchange data among users, in addition to using firewalls and security platforms for protecting the servers. Moreover, the users need some tools or devices and some software applications for opening and accessing the OSN platform. And all these types of equipment, tools and applications in OSNs need a channel or way to work as well as machines. This channel is the internet.

2.2.2 Architecture of OSN

There are two standards of actualizing an OSN, client-server architecture and peer-to-peer (P2P) (Buchegger and Datta, 2009, Buchegger et al., 2009) (Website, August, 2014) architecture .

1. Client-Server Architecture: The OSN are centralized based on a web-server. All functionalities, such as storage, maintaining accessibility, and keeping profiles are managed by the OSN enterprises. This conventional architecture has the benefit of being straightforward and simple to execute, while suffering from all the hitches (drawbacks) of centralized systems. For instance, every central entity can simply be a single point of failure, a single target for Denial-of-Service (DoS) attack, and moreover, a tailback "bottleneck" for network performance.
2. Peer-to-Peer (P2P) Architectures: There are several strong approaches to maintaining P2P architectures for new OSNs generations. They embrace decentralized structure planning, depending on collaboration among various free parties who are likewise clients of the OSNs. Typically, P2P applications enable users to dominate many elements of processes and operations, such as number of member connections to seek or allow at one time; whose systems to connect to or avoid; what services to offer; and how many system resources to devote to the network.

2.3 SECURITY AND PRIVACY (OSN)

It is not easy to define the required domain for security and privacy in any OSN. However, in general, privacy could be explained as the personal security and privacy level that covers the information that is shared through the OSNs' account. It covers a widespread variety of factors, mechanisms, and technologies utilized to preserve private and sensitive information, communication, and preferences.

Many people believe that it is only necessary to defend privacy and sensitive data from unauthorized disclosure. However, computer security provides a much broader explanation of the terms privacy and sensitive information; any loss of information, abuse, or illegal access or change might adversely influence the users (Whitman and Mattord, 2011).

When a user is performing daily activities on their profile, some loss of information might be recorded. For instance, entering a user to an unknown group through clicking a link or opening an offered application may cause a loss of sensitive information. In some cases, attackers may be secretly trying to extract private information with pertinent details to abuse those data for their benefit. Information that is stolen or missed through this process could be photos, full name, locations, birthday, school and many other records or data. Attackers may use the stolen information to create a fake account so that they can establish a fake network among the friends of the hacked user. The purpose of this fake network is to steal more sensitive information from other users.

Such a study (Hogben, 2007), shows different aspects about privacy disclosure issues and security penetrated processes, the researchers explain how the threats work and some technical solutions that can stop or minimize threats. As a conclusion, the study also supported to improve the education of OSN users, without mentioning any procedure for that, however, building or increasing such awareness needs time and should be continued for new users. A handy model is necessary for such education so that every user can learn how to improve security and privacy. Surveys focusing on explaining OSN, including threats and solutions have been conducted, and one article has nicely classified all threats and attacks into several groups: classical threats, modern threats, combination threats, and threats targeting children (Fire et al., 2013).

The study even shows several types of threats and attacks for each group. Moreover, for each subgroup the study provided more solutions in the same classification structure of that used for threats and attacks. In contrast to previous work, the solutions provided covered some commercial tools that can solve the problems which may face OSN users. The authors also recommended some academic solutions for giving more attentions to OSN users. It is not easy to provide and collect all these solutions over one system, especially as the author suggested different types of solutions for different threats. Sometimes a system even has security tools in place, but even so, the unawareness of users or out-of-dated security tools create loopholes. Another study conducted surveys on the current state of security issues of OSN and the defense systems that work against OSN threats (Gao et al., 2011). The authors organized these attacks into four main categories, and they offered an in-depth discussion of each category. The work also adopted an analysis of the connections among the different security issues involved. The authors ended with the hope that OSN users will learn from their study how to protect their accounts from those risks, and that it will improve their knowledge about maintaining their privacy and security. Another study was conducted with two groups of OSN users who are using OSN services between friends (Sadeghian et al., 2013). In the first part of this article, the authors examined various common types of threats and attacks, and in the second part they offered combination solutions to mitigate the security risks of using social networks. The main goal of this article is a pure understanding of the security risks in the OSN which can assist the user in learning how to better mitigate the security issues. There are many ways to infect OSN users rather than using OSN applications, such as through the devices for using OSNs. Although the researchers defined different types of OSNs and attacks, they focused more on two types of attacks, namely Location leakage and Clickjacking (Nei et al., 2014). Accessing OSN through a smart phone, tablets and Wi-Fi make the users share more information via these devices; hence it will be easier for attackers to get information from users. The authors talked about the security issues and proposed a solution for each of them. As well as a solution, they also proposed two specific solutions to raise the OSNs users' awareness. Additional studies have addressed security and privacy in Location-Aware Mobile Social Network (LAMSN) systems. (Beach et al., 2009); the researchers address several types of privacy and security issues, after which they propose a design and a solution for these circumstances. This solution is restricted to protecting user identity and preventing the violation of users' privacy and security when using mobile devices to access OSNs, furthermore it supports the anonymous interchange of social network information with real world location-based systems, enabling context-aware systems that do not compromise users' security and privacy. It is the time for building some tools that provide solutions easily to OSN users, and can teach them some principles of keeping their security and privacy (Creese et al., 2012, Dave et al., 2013, Daniel et al.). (Zhang, L. and W. Zhang) (Zhang and Zhang, 2012) proposed and designed a method to combat attacks and threats related to extracting information from the profile of an OSN user. The study explains a type of attack that abuses web engine methods to extract information, using data mining techniques from private information that is hidden on a social network. The study extracted features from those attacks and built vectors. Then the method was tested to detect similar attacks, using the same features. The work depended on the precision of the information retrieval method to test the detection rate of similar invisible attacks. Another study used encryption and decryption methods to keep privacy as secure as possible while personal information for a user needs safe access of the network they are in (Guha et al., 2008). The authors tried to encrypt personal data for those who need to be analyzed through that data. The encryption changed the original data to cipher text looking like legitimate data. This article surveys the current state of security issues and available defense mechanisms regarding popular online social networks. It covers a wide variety of attacks and the corresponding defense mechanisms, if available. The authors organize these attacks into four categories — privacy breaches, viral marketing, network structural attacks, and malware attacks — and focus primarily on privacy concerns. They offer an in-depth discussion of each category and analyze the connections among the different security issues involved.

2.4 THREATS AND ATTACKS (OSN)

While a threat is anything that can interrupt the process, performance, integrity, or availability of a network or system, an attack is a specific technique that is used to exploit vulnerability. For OSNs, an attack is a kind of technique that brings threats to social network users and puts them at risk.

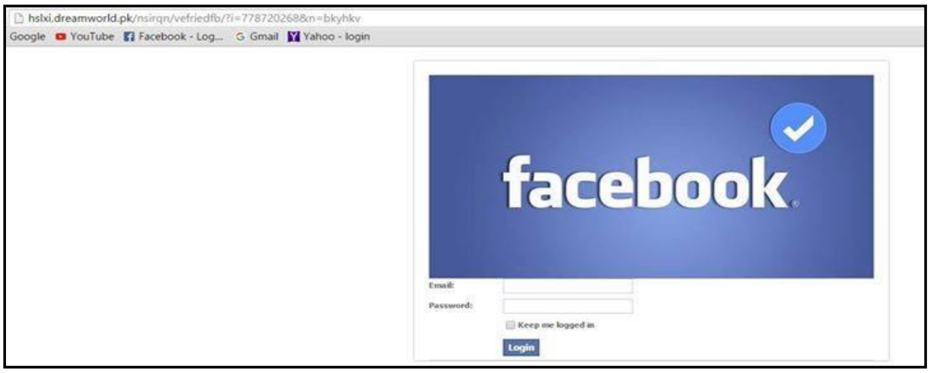
In general, attacks can cause many types and groups of threats. The first group involves ***classic threats*** (Fire et al., 2014). Those threats are known as privacy and security threats. These threats do not only threaten OSN users, but also threaten internet users not using social networks. C***lassic threats*** have been growing along with the internet. The most popular classical threats are listed below:

1. **Malware:** Malicious software created to interrupt computers. In Online Social Networks, malware utilizes the framework of OSNs to disseminate "propagate" among OSN users and their friends. This software can collect info from your account, send status updates or messages that look like they are from you, or cover your account with ads that crash your computer. In some cases, the malware can use the obtained credentials to impersonate the user and send contagious messages to the user’s online friends. Koobface was the first malware successfully propagated through OSNs. This malware attempted to obtain "collect" login information and then enter the infected computer in order to be part of a botnet (Baltazar et al., 2009).
2. **Spam and Spammers:** Spamming is a method of flooding the internet with copies of the same message. Spammers of the OSNs utilize the platforms of social networks to launch ads messages to other users by creating fake profiles (Fire et al., 2012). Spammers can also utilize the platforms for adding comments to different pages viewed by OSN users on the network.
3. **Cross-Site Scripting (XSS) attacks:** Cross-site Scripting (or XSS) is one of the most common web application attacks. The main concept of XSS is to exploit the security of the web-client in the web application through executing malicious code to aggregate sensitive data and cookies of users. XSS can attack OSN and separate among users as a viral worm (Livshits and Cui, 2008). During April 2009, a XSS based worm called Mikeyy rapidly transmitted

through tweets across Twitter and infected the profiles of many users (Paul, 2009).

4. **Cross Site Request Forgery (CSRF):** An attack that makes an end user's web browser implement actions of the attacker's choosing without the knowledge of the user. By inserting a malicious link in a web page or forwarding a link through chat or emails, an attacker may prompt the users of a web application to execute unwanted actions. For example, the attacker causes the users' browsers to perform requests to a website from which it has accepted 'cookies', without the web site's or the users' knowledge. These actions may compromise end user data and operations (e.g. sending an email, changing a password) (Mao et al., 2009), or even an entire server or network.
5. **Phishing:** A phishing attack is a type of social engineering to obtain a user's private and sensitive data by representing an accurate Third Party (TP). A survey (Amin et al., 2010) revealed that those users who interact on OSN web pages are more likely to fall for phishing scams because of their social and trusting nature. For example, one phishing attack happening on FB, diverting users to fake FB login pages, as shown in Figure 2.2. Then the phishing attack propagated through users by asking friends to click on a link posted on the main user's profile (Mills, 2009). Fortunately, FB stopped this attack.

Figure 2.2: A fake login used by Phishing Attackers



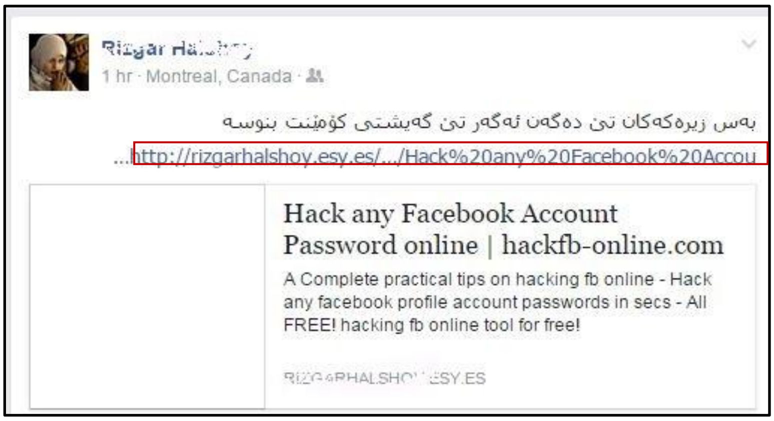
6. **Internet fraud:** The phrase internet fraud refers to any attempt to fraud online users or obtains advantages, and is also recognized as "cyber fraud". The attacker uses social engineering techniques to attempt to trick OSN users into

making strong friendships, or installing software that can spy on what the user types. Recently, according to the North American Securities Administrators Association (NASAA) ((NASAA), 2011), scammers have turned to OSNs to set up trusting relationships with their victims to get access to private information that is shared in the online users’ profiles. And recently scammers have for instance hacked the accounts of FB users traveling in foreign countries. Once they manage to log into a victim's account, the fraudsters cunningly ask the user’s friends for assistance in transmitting money to the fraudster's bank account.

Modern threats are the second group of OSN threats. They are exclusively related to the OSNs’ environment. These threats are often collecting information of a user, friends of the user, and mutual friends. There are many kinds of modern threats which include:

1. **Clickjacking:** This a virulent "malicious" method that tricks OSN users into clicking on something else than what that they intended. Through this attack, the attackers can influence and manipulate targets through posting and sharing spam messages on their FB profiles/timelines, ‘liking’ links unknowingly or inadvertently. It is also called likejacking, and even opens a microphone and web camera to record the user (Lundeen et al., 2011). An example of a clickjacking attack took place on Twitter in 2009, when Twitter was plagued by a Don’t Click attack. The predator tweeted a link with the message Don’t Click with a masked URL (the real URL domain was invisible).When the users clicked on the Don’t Click message, the message spontaneously went viral and was shared onto their Twitter accounts (McMillan, 2009).

Figure 2.3: Clickjacking



Rizgar Ha[redacted]

1 hr · Montreal, Canada ·

بەس زیرەکەکان تێ دەگەن ئەگەر تێ گەیشتی کۆمێنت بنوسە

...http://rizgarhalshoy.esy.es/.../Hack%20any%20Facebook%20Accou

Hack any Facebook Account Password online | hackfb-online.com

A Complete practical tips on hacking fb online - Hack any facebook profile account passwords in secs - All FREE! hacking fb online tool for free!

RIZGARHALSHOY.ESY.ES

2. **De-Anonymization Attacks:** A data mining strategy in which anonymous data are cross-referenced with other data sources to re-identify the anonymous data source. In several OSN platforms such as MySpace and Twitter, the users have the ability to protect their personal information and anonymity by utilizing anonymous "pseudonyms". De-anonymization attacks use such techniques as network topology, user group memberships, and tracking cookies to reveal the user's original identity. In this technique, attackers want to identify the social network group that the victim belongs to (Gunatilaka, 2011).

3. **Face Recognition:** Many internet users use OSNs for uploading and sharing their pictures with their friends. Every day a huge numbers of images are shared and uploaded to FB. Moreover, many FB user profile pictures are available for viewing and downloading in public. For example, the "Faces of FB" website (Rojas.) permits internet users to open and view the profile pictures of more than 1.2 billion FB users. Those images could be used to create a biometric database, which can then be utilized to recognize OSN users without their permission.

4. **BotNet and SocialBot:** A botnet is a set of computers associated with a coordinated form for malicious performance. Each computer in a botnet is called as a Bot. Usually is a malicious software and executable file, capable of performing a set of functions, each of which could be triggered by a specific command. A Bot, when installed on the victim machine, copies itself into the configurable install directory and changes the system configuration each time the system boots. Recognized as a SocialBot (Boshmaf et al., 2011) is the software program that

simulates user's behavior in automated interaction on OSN such as Facebook and Twitter. It spreads by convincing other users that a social bot is a real person. Therefore, such attack is also known as FakeProfile makers attack.

5. **Identity Clone (Identity Theft) Attacks:** The main conception of identity theft that the attacker is pursuing is to steal people's identity, personal information, or users' online behavior, and then pretend to be that person, or apply that identity in a malicious way in the same networks, or through different networks, to fraud the cloned user's friends. With this policy the attacker is trying to establish a trust relationship with the cloned profiles (Gunatilaka, 2011). The attacker might use this trust for aggregating personal data about the user's friends or to achieve different types of online fraud.

6. **Inference Attacks:** The conception of inference attacks in OSNs is used for predicting personal, sensitive data or any users' attributes that are undisclosed (Heatherly et al., 2013), such as posting status updates, photos, or sexual orientation. These various attacks are achieved by using data mining and machine learning methods combined with publicly available OSN data, such as the topology of networks and information from users' friends (Mislove et al., 2010).

7. **Information Leakage:** OSN allows their users to easily exchange and share personal information with others in public. Therefore, users become good targets for attackers. The leakage of personal and sensitive information might have negative implications for the OSN users. The OSNs allow Third Party Application (TPA) providers to design applications for OSN, which can run them on their platforms, such as the Application Programming Interface (API) in FB. These TPAs are extremely common among OSN users. As the users connect and permit TPAs to access their privacy information, these apps can reach users' information automatically. In addition, TPAs are able to post on users' profiles or users' friends' profiles, or might be able reach other users' data without those users' knowledge (Gunatilaka, 2011). This causes a breach of privacy.

8. **Location Leakage:** A type of information leakage that can expose the user's location. With the growing use of smartphone devices and technologies such as GPS, 3G and 4G, users are encouraged to share their location. OSN user may unknowingly share their location when they are sharing private and sensitive

information such as images and videos on smart phones; this could then lead to loss of property and a security issue in real life as well (such as burglary). For instance, "Israel Hyman from Arizona tweeted that he was looking forward to his family vacation to St. Louis. He tweeted once again he had arrived in Missouri". After returning home, he found that his house had been burglarized (Humphreys et al., 2010).

9. Socware: It needs false and possibly harmful messages and posts from friends in OSN. It might be appeal "lure" targets by suggesting fake proceeds "rewards" to the OSN users who set up Socware connected malicious FB applications or going to doubtful website of Socware. When the users have lunched "cruised" the Socware websites or setting up to the relevant applications, the messages will be sent by the installed Socware on the user's behalf to the user's friends, in order to virally spread the Socware (Rahman et al., 2012).

The last group is **Threats Targeting Children**; this group of threats focuses on children or teenagers. These threats intentionally and particularly target younger users of OSNs.

1. **Online Predators:** The main concern is the safety of children's personal data in relation to sexual exploiters of children, "pedophiles", and online predators. In (UNICEF, 2011) The EU Kids Online organization described a typology in order to recognize risks and injury relating to online behavior: harm from content - a child's vulnerability to pornography or hateful sexual content; injury from contact - a child who has been contacted by an adult or other children for the reason of sexual abuse; and abuse from conduct - "the child as an active initiator of smutty or risky behavior”. Activities ("behaviors") that are classified to be internet related sexual exploitation of children involve adults utilizing children for child pornography, the consumption of child pornography, and the use of the internet as a way to trigger online sexual exploitation or real life "offline" sexual exploitation.

2. **Risky Behaviors:** Potentially dangerous behaviors and activities of children may involve direct online communication with strangers, as well as the use of chat rooms for communication, sexual talk, and delivering data and images to strangers. It should be noted that while each of the above-mentioned behaviors alone contribute to the risk, the combination of several of these behavior patterns can justifiably cause massive concerns regarding a child’s safety. In (Wolak et al., 2008b) preserves that risky online behaviors and specific populations who are more exposed to them can be identified. Additionally, there is a well-established link between online and offline behavior. In some cases, researchers contend that victims of Internet abuse are very often vulnerable children, i.e. with a history of physical or sexual abuse or who suffer from depression or social interaction problems (Wolak et al., 2008b). All children living with these kinds of issues are at a higher risk of sexual abuse on the Internet or through online-initiated encounters (Wolak et al., 2008b).
3. **Cyberbullying:** Also referred to as "cyber abuse", it is the abuse of communication technology platforms by minors to bully internet users by means of email, chats, videos, photos, posting harmful messages, OSNs, phone conversations, or the use of any interactive technology with the intent to frighten, embarrass, harass or otherwise target another minor. The attackers send repeated harmful messages, sexual comments or threats, publish embarrassing photos or videos of the victim, or engage in other kinds of inappropriate behavior. Cyber bullying has recently become a common phenomenon on OSNs, as the attacker can use the network’s structure to propagate harmful tales about the victim and distribute embarrassing photos to the victim’s network of friends (DEAN, Oct. 2012). Due to children spending extra time on the internet and OSNs, engaging in many activities on the internet, and discovering new relationships with unknown people, they face more problems and attacks which make them suitable victims. For example, by using risky behavior a victim may inadvertently establish a connection with a sexual predator; furthermore a victim may share sensitive information such as photos or sexually explicit data (Fire et al., 2014).

2.5 USER VULNERABILITY (OSN)

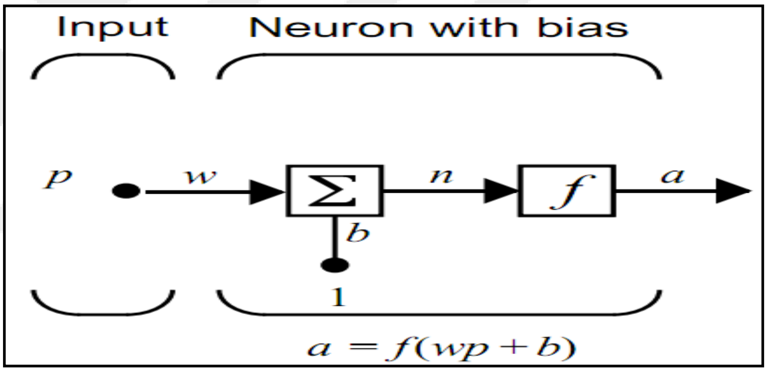
The previous section explains that there are many different threats and attacks that are easily applied to OSNs users and make them good victims. The OSNs still lack safety modules, hence their users are more vulnerable. The facilities and functions offered by OSNs lead users to share more personal information, their own pictures, etc. These data are freely available and accessible for other OSN users. Hackers are able to directly access information of OSN users and download it without the knowledge of the user. Photos and data could be misused in a number of ways, such as creating fake profiles, and pictures can be sold to other nuisance web pages. This kind of data hacking activities in OSNs even leads to rescue situations among users. There some common vulnerabilities of OSN users that facilitate hacker attacks: (Damen and Zannone, 2013, Strufe, 2009, Symantec, APRIL 2015):

1. Too trusting to friends or strangers.
2. Spending much time on OSNs.
3. Using tagging, check-in and places.
4. Downloading unknown content
5. Playing online games.
6. Downloading apps.
7. Joining too many groups.
8. Adding, accepting and making friends with unknown users.
9. Sharing too much personal information and photos.
10. Clicking on links and attractive videos and photos.
11. Chatting and calling and exchanging data through OSNs.
12. Not choosing social networks carefully.
13. Not caring about customizing privacy options.
14. Not having enough knowledge of security and privacy.

2.6 ARTIFICIAL NEURAL NETWORK (ANN)

ANN is a mathematical and computational model that is inspired by biological neural networks. This network consists of many interconnected neurons that can process and compute information through the connections approach. Neurons in an ANN are distributed on three types of layers: an input layer, hidden layer/s, and an output layer. Each neuron receives a vector of scalars (ρ) that are multiplied by a vector of weights (ω). The result of adding a bias value *b* to the product of vectors ($\rho\omega$) will be applied to an activate function *f*, which is also called transfer function. Figure 2.4 represents a typical diagram of a neuron (Sivanandam, 2006).

Figure 2.4: Mathematical Model of Typical Neuron

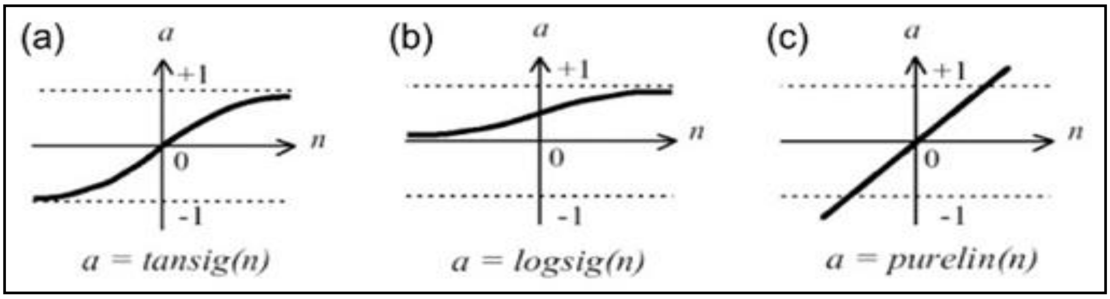


As shown in Figure 2.5, several shapes can be employed for the transfer function in ANN models. Each function may fit a specific application. The current study uses the logistic function (Figure 2.5.b) in the neurons of all layers for predicting the level of OSN user vulnerability level. This function is selected because it is a robust differentiable function over an infinite range.

The hyperbolic tangent transfer function (Figure 2.5.a) which has an output in the range of -1 to +1, is related to a bipolar sigmoid in the neural networks.

Pure-line function (linear function) is a linear transfer function (Figure 2.5.c), also known as a simple linear function that produces the same output as input (Rutka, 2015).

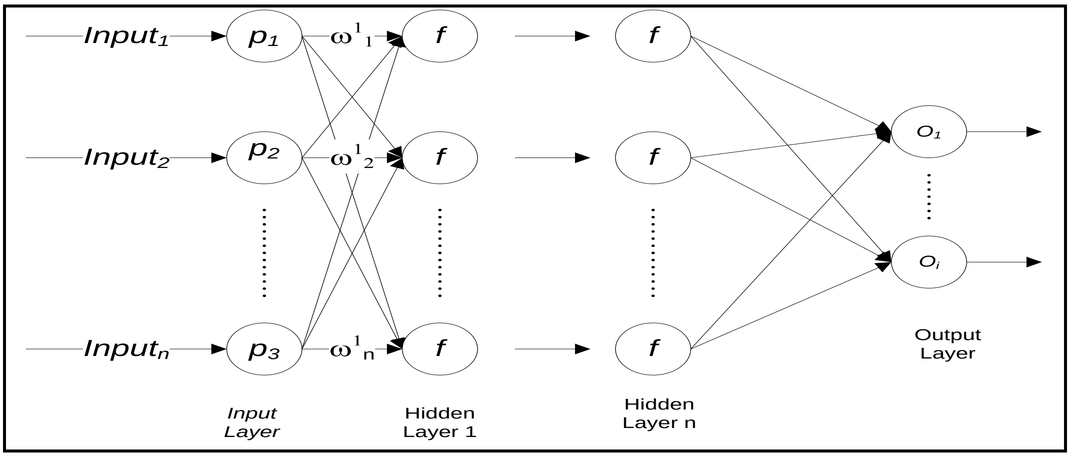
Figure 2.5: Transfer functions



Connecting neurons inside a layer and between layers can be performed in various ways. The simplest way is to connect neurons from the layer directly above a current layer to those in the layer below, as in the case of a Feed Forward Back Propagation Neural Network (FF-BPNN). However, a neuron can receive its inputs from the neurons below and can send its output to neurons above in a strictly forward manner.

The structure is called Feed Forward because no backward connections exist between neurons from different layers. Figure 2.6 illustrates a typical structure of an FF-BBNN. Equation 2.1 shows the expression of the output of any neurons in such a type of neural network (Ivancevic, 2010).

Figure 2.7: Typical structure of FFBB-NN with an n hidden layers and i-th neurons at the output layer.



$$\boldsymbol{O_k(t+1) = F_k(s_k(t)) = F_k\left(\sum_1^j \omega_{jk}(t) O_j\,(t) +\ b(t)\right)} \qquad \textbf{(2.1)}$$

$O_k(t+1)$ is the output of k^{th} neuron, *$y_j(t)$* is the output of the j^{th} neurons forwarded to the k^{th} neuron, *b(t)* is the bias value for the j^{th} node, and ω_{jk} is the weight value that determines the effect neuron j on neuron k. Each neuron receives an input for the neighboring neurons or external resources. Then it computes the output by using the activation function, and finally it forwards the result to the next neighboring neurons. The activities of ANN neurons include training on processing an input set and obtaining the desired output. Therefore, the term “back propagation” describes the way that an ANN acquires training. The training process adjusts the weights of any ANN so that it can perform a specific application.

Various methods are used to achieve ANN weight configuration. One way is to set and initialize the weight value depending on prior knowledge. Another way is to train the ANN by feeding it teaching patterns and forcing it to change its weights according to the learned rules. The methods for training and learning can be classified into two distinct categories: supervised and unsupervised learning. Both learning paradigms result in the adjustment of weight values between neurons (Ivancevic, 2010, Zhang, 2005).

One of the most important learning methods is back propagation, which mostly depends on the training function (Sivanandam, 2006). Back propagation involves supervised learning, and adjusting the weight value between two neurons depends on the delta rule. Through the delta rule, the adjustment of a weight can be defined by computing the difference between the actual y_k and the desired d_k output, as shown in Equation 2.2. The delta rule can determine the error between the actual and the desired output at each neuron, and γ represents the learning rate. Moreover, error adjustments for the neurons of the hidden layer are determined by back propagating the errors of the output layer neurons.

$$\boldsymbol{\Delta\omega_{jk} = \gamma y_j(d_k - y_k)} \qquad \textbf{2 (2.2)}$$

Therefore, the back propagation algorithm has two phases. In the first phase, the input data are clamped to the NN, propagate toward the output, and then generate an error signal between the desired and the actual outputs. The second phase involves a backward pass through the network during which the error signal passes to each neuron in the network and then appropriate weight changes are calculated (Yegnanarayana1, 1994).

The rate of error between the actual and the desired outputs will be minimized by adjusting the value of the neuron’s weight. This process indicates that the ANN will be trained to map a certain input to the desired output. This mapping ability makes ANN an efficient tool for many pattern recognition and classification applications.

In this study, all OSN attacks and threats are considered, and their features and mechanisms are examined thoroughly by threats and attacks which can be penetrate the systems. Those features are used to build some simple and understandable questions. From these questions, users will be able to assess their vulnerability level through using an intelligent system, such as an Artificial Neural Network (ANN). The questions can also teach OSN users how to protect their privacy and system security through minimizing some undesirable behavior.

2.7 PERFORMANCE METRICS

There are a lot of performance indicators a work can use them for checking and evaluating the performance and the efficiency of models. In this work, we need to evaluate the accuracy using two different methods.

1. For the Prediction sub-model, this work depends on computing the Root Mean Square Error (RMSE) rate for the model, which mentioned in equation 2.3 (Balsamo et al., 2004a).

$$RMSE = \sqrt{(A - \bar{A})^2} \qquad \mathbf{(2.3)}$$

   Where:

   A is the proposed output the prediction model, and $\overline{A}$; is the actual output that obtained from the prediction sub-model.

2. Mean Absolute Error (MAE) (equation 2.4) is an indication of the average deviation of the predicted values from the corresponding observed values and can present information on the long-term performance of the models; the lower MAE the better is the long term model prediction(Balsamo et al., 2004b, Vastrad, 2013).

$$(MAE) = \frac{1}{n}\sum_{i=1}^{n} |\ \overline{y} - y| \qquad \mathbf{(2.4)}$$

3. PROPOSED WORK

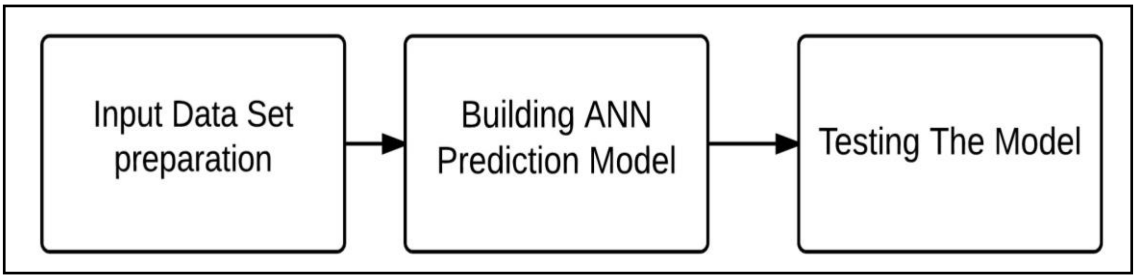
3.1 INTRODUCTION

In chapter three the steps of the proposed methodology will be explained in detail. The explanation will be supported by different graphs and drawings to further visualize the idea. This chapter explains the model in a sequenced approach. The role of each step is illustrated and the impact of this step on the whole model is explained.

3.2 OUR FRAMEWORK

The framework of this project comes in three main parts. The first part relates to building the input dataset, which is achieved through some sub-steps. The second part relates to building the Artificial Neural Network prediction model. The last main part is related to testing the accuracy of the proposed model. Figure 3.1 shows the sequence of these three parts.

Figure 3.1: The main three parts of the work



The coming subsections explain the content of each sub-part.

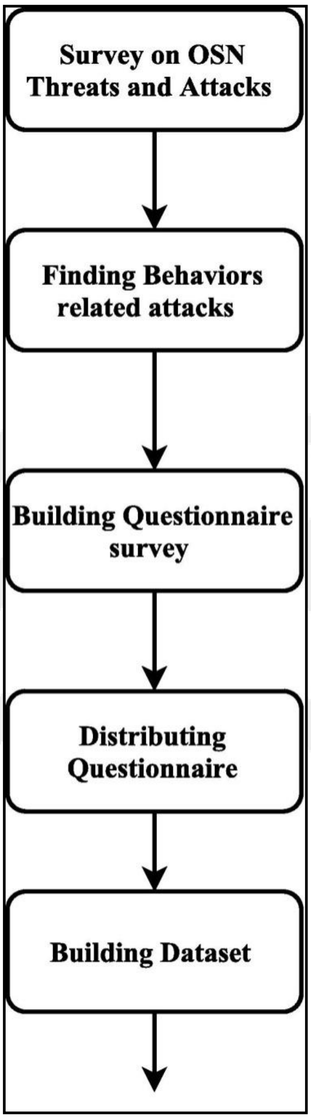
3.3 INPUT DATA SET PREPARATION

This part relates to building the input data set that is used to train the ANN model. The description is divided into several sub-sections, starting with building the questions and ending with completing the data set. The following steps explain the steps in preparing the input data set:

1. Conducting an extensive study on different threats and attacks that might penetrate systems through OSNs.
2. Finding the relations between every kind of attack identified in step (1) and the vulnerability of an OSN or OSN user.
3. Drafting questions that can reflect the relations obtained in step (2). When the drafting is complete, double checking the draft for privacy, security, and awareness considerations.
4. Distributing the questionnaires in two different cultures (Turkey and the Kurdistan region of Iraq).
5. The results of the survey carried out in step (4) need to be tabulated, refined, and cleaned from any unwanted outliers.
6. The output of step (5) is an Excel sheet that is used to train the ANN based model in the following sections.

This work depended on conducting a survey among two different cultures, in order to train the proposed model on two different behavior patterns. The framework consists of a five-step process under the first main part of the framework. The first part is about data collection on OSNs threat and attacks, finding behaviors that are related to attacks, then building the survey, distributing it among OSNs users, and input dataset preparation. Figure 3.2 illustrates, in general, the process of building the input dataset for the proposed model.

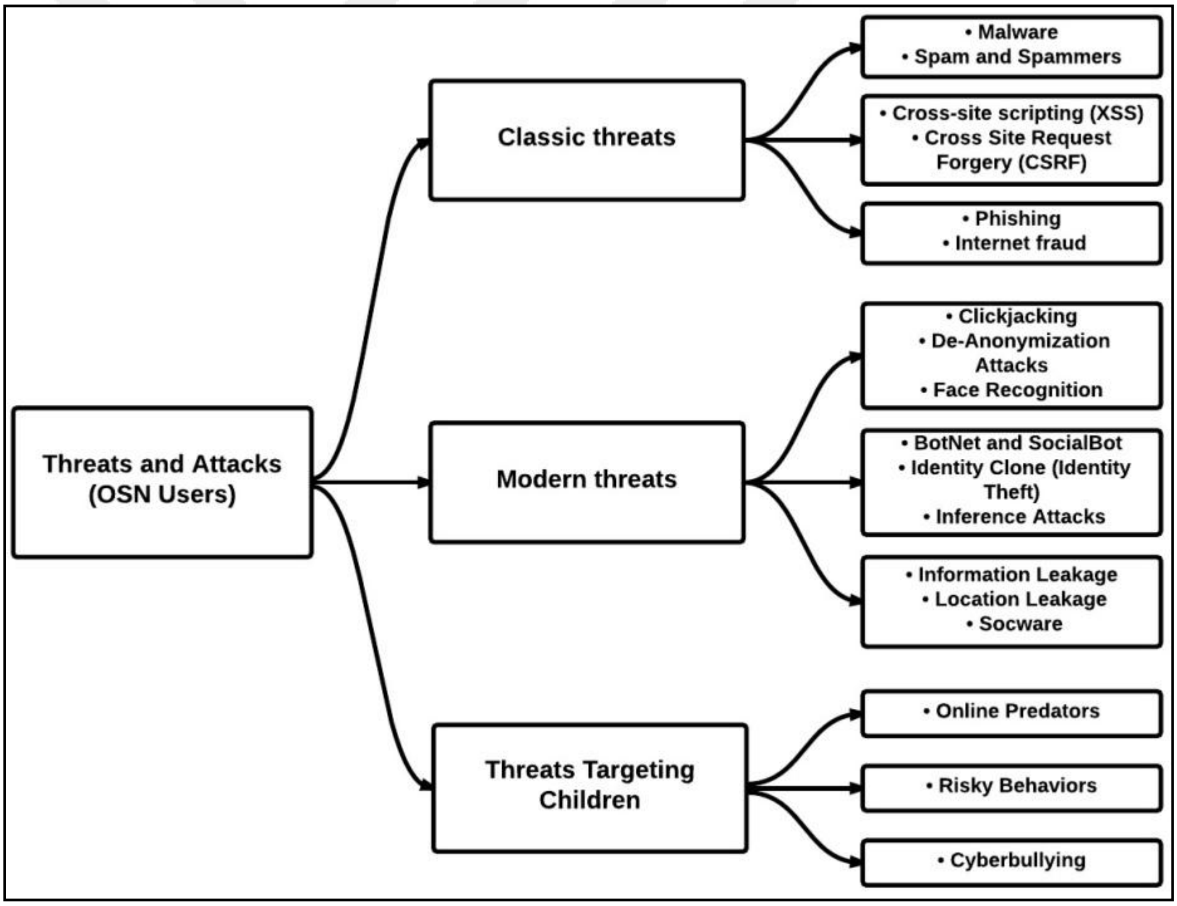
Figure 3.2: The steps of the first main part of the model


Survey on OSN Threats and Attacks
Finding Behaviors related attacks
Building Questionnaire survey
Distributing Questionnaire
Building Dataset

3.3.1 OSN Threats and Attacks

The methodology of this work starts with a comprehensive study on most threats and attacks of OSNs that may have negative impacts OSN users (Sadeghian et al., 2013, Fire et al., 2014, Hogben, 2007, Gayathri et al., 2012). The study covered a wide range of various threats and attacks from previous studies. Accordingly, many types of OSN attacks were found and classified into different groups. As mentioned in Section 2.4, there are three categories of threats (Fire et al., 2014); classic threats, modern threats, and finally threats targeting children. All groups have eighteen threats in total that are able to penetrate systems through OSN users. Figure 3.3 shows these eighteen attacks with reference to their respective groups.

Figure 3.3: OSN attacks and threats



The first types of threats penetrate both websites and OSN, depending on the activity of and information about the users. In the past, hackers needed more time to collect data on internet users in order to invade their privacy or steal their credentials. However, now the OSN have become the best and easiest places for aggregating data and penetrating users' accounts.

The second group is modern threats, which are directly related to OSN threats. In this group the attackers get advantages from the publication of private information, as well as users' activities and communication. OSNs built for easily sharing and communicating among internet users and establish new friendships negate all national and religious borders. In this case, the intruders are capable of establishing networks with others and get close to them, then breach their privacy and steal their credential with ease.

The last group refers to the threats targeting children. These threats target the behavior of children. The attackers try to establish strong relations with children and to gain their trust, which leads children to share more sensitive information about themselves (Hogben, 2007).

The launch of one of these attacks on OSN users leads to a loss of much sensitive information. Many studies have referred to the seriousness of those threats and attacks (Kayes and Iamnitchi, 2015).

These threats and attacks work on OSNs because of users' behavior and lack of awareness of these kinds of risks. All these attacks could take place when users trust unknown sources or links from strangers, as the hackers always try to persuade their potential victims by using attractive lures to access channels in order to be able to infiltrate the users' systems.

3.3.2 Attacks Based on OSN Users' Behavior

The previous section identified eighteen attacks as OSN based attacks. In this section these attacks are investigated to identify the method they use for penetrating systems. In most cases, attackers try to find open channels to access or to connect with OSN users. Each attack mentioned in Figure 3.3 has its own method of finding an open channel(s) to the victim's system.

1. Malware penetrate systems through injecting a malicious code in an interested application(s). The system of an OSN user can get injected through

downloading a malicious application and files (Bossler and Holt, 2009a). Sometimes, users will be injected when they want to update their application through links forwarded or shared with their friends. More online presence increases the possibility of malware injections (Bossler and Holt, 2009b). **(Malware)**

2. Spams are another form of malware. They penetrate systems through posts, links, or tags from friends. The phenomenon relates to the management of the OSN user's account (Jin et al., 2013, Huang, 2013). If an account is public to all, spammers can easily target its system and inject it with different types of malicious codes. **(Spams)**
3. Setting and managing cookies is another issue that opens channels for attackers. Through existing cookies an attacker can find or learn the type of cookies that are accepted by the user's browser. The attacker can then design such cookies and use them maliciously. Such scenario is related to the **XXS** and **CSRF** attacks (Mao et al., 2009, Maxwell Chi, March 16, 2011).
4. Phishing is another method that attackers use for stealing IDs and passwords. Attackers may drop a link that directs users to another site to login (Amin et al., 2010, Sadeghian et al., 2013). Once the user has logged in, his or her ID and password are no longer confidential as the attacker has a copy. **(Phishing)**
5. Internet fraud is a technique in which an attacker exploits a friendship with the victim, first through sending a friend request, and then by persuading the victim to exchange sensitive data. Through this process, the attacker can collect and override the privacy of the victim and most of his/her friends. **(Internet Fraud)** (Fire et al., 2013).
6. Click jacking is another type of attack in which the attacker tricks OSNs users to click on something different from what the victims perceive, such as new ads. That process enables an attacker access to confidential data or to take control over the users’ computers (Lundeen et al., 2011). **(Clickjacking)**
7. De-anonymous is another type of attack. It uses social groups in which OSNs user participate in with unknown sources of groups. The attacker tries to re-identify the OSNs user to identify users from an anonymized social graph

and disclose the private information by using the history "Social graph" of the user (Peng et al., 2014). **(De-anonymous)**

8. In Face Recognize, an attacker uses software to identify the ID of OSN users through uploaded personal pictures. The vulnerability that is used by this attacker is making uploaded photos public instead of customizing them as private (Al Hasib, 2009). (**Face Recognize).**
9. SocialBot and Botnet are considered as dangerous attacks in OSN. Attackers try to send fake friend request through malicious applications or through sending malicious links (Simonite, March 23, 2015) **(SocialBot)**.
10. The mechanism of Identity Clone (Identity Theft) is through collecting personal information from a victim's profile by clicking a follow button. Through this process, the attacker can get most of the data, then they uses them for their advantages to create a fake account to persuade victim's users (He et al., 2014). **(Identity Clone).**
11. Inference attack - this type of attack tries to guess the sensitive data of the user by using some techniques for collecting the privacy of the users (Ahmadinejad and Fong, 2014).**(Inference attack)**
12. Information leakage attack is another popular type of OSNs attack, in which the attacker tries to collect information to breach users' confidentiality. The attacker uses different ways for getting access to personal information. This attack can happen if a user does not adapt the privacy settings, and shares much sensitive data over OSNs on a daily basis. (Molok et al., 2010) **(Information Leakage)**
13. Location leakage is a type of information leakage in which the attacker is focusing on a location of the user. It happens when the user shares private data or "checks in" with a smart mobile. The attacker attempts to track the most popular and the second most popular places of the users. (Krishnamurthy and Wills, 2010) The impacts of such attacks on the target users are more physical than virtual. (Nei et al., 2014) **(Location leakage)**
14. The Socware attack approaches the users by posting messages or installing those OSN applications that ask for permission to see the private information of the user. Socware spreads among the user's friends as a virus, but if the user applies

the security tools the possibility of Socware attacks will decrease. (Rahman et al., 2012, Huang et al., 2013). **(Socware)**

15. Online Predators. This kind of attack targets children and teens. They are most vulnerable in chat rooms, through emails and exchanging sensitive data with the attacker. A young child is always interested in knowing the content of every IM, email, and chat, which leads them to become victims of sexual prey and abuse. It also cheats children into spending money (Duncan, 2008). **(Online Predators)**
16. Another attack is Risky Behavior. The main concept of this is accepting strangers using fake identities as friends, and (Wolak et al., 2008a) (opposite gender), then chatting and exchanging photos with them. Through this mechanism, the strangers incite young children into pornographic activities (Moreno et al., 2009). **(Risky Behavior)**
17. The most popular attack among teens is cyber bullying. Such attackers abuse communication tools in order to bully the OSN and internet users. A cyber bullying attacker continuously sends harmful messages to known or unknown users to victimize them or their friends. In opening such a message, the target will see some "sexual videos" for example, or embarrassing pictures of a friend. Through this process a link will be established so that the bully attacker can recognize the victim's friends over networks. More online presence increases the possibility of cyber bullying injection (Marinos et al., 2011). (**cyber bullying**).

The seventeen scenarios above explain most behavior based OSN attacks. The next section shows the process of translating these scenarios into questions, which will enable the study and tabulation of records on individual behavior of OSN users.

3.3.3 Questionnaire Sheet Preparation

To build an appropriate input data set, this work depends on investigating the behavior of OSN users in two different cultures. The most important point that should be considered in preparing the questionnaires is the relation between each question to the scenarios mentioned in Section 3.3.2. At least one question should relate to each scenario. To make them understandable, the questionnaires are prepared in three languages, Turkish, Kurdish, and English. Appendix (B) shows all versions of these questionnaires. The table shown in Appendix (A) presents the relation between each question with the attack scenario mentioned in the previous section.

The distribution of the questionnaires is explained in the next section.

3.3.4 Distributing Process

Two different cultures have been selected for this survey, Turkey and the northern part of Iraq (the Kurdistan Region). The purpose of selecting two cultures is to collect as much information as possible about OSN user behavior. Thousand sheets were distributed, five hundred to each cultural group. In order to diversify the responses, they were distributed to people of different ages, genders, occupations, educational levels, schools or companies or homes, private and government offices, academics or non-academics, etc. The participants' details are explained in Table 3.1.

Table 3.1: The survey participant details

Culture	Gender		Age					Education Level				
	Male	Female	10-20	21-30	31-40	41-50	51-60	School	Diploma	Bch	MSc	PhD
TR	111	228	280	57	2	0	0	243	0	94	3	2
KRD	193	194	287	74	10	3	13	239	86	53	9	0

This process resulted in seven hundred and fifty (750) sheets. However, among these sheets were many incomplete sheets, where some questions had been left empty or answered incorrectly. The number of complete returned sheets were (344) in Turkey and (388) in Iraq.

3.3.5 Tabulating Sheet (Records)

The collected questionnaires needed to be tabulated. For each group, a separate sheet was prepared. However, the attributes of both sheets were the same. Each sheet had (30) attributes (features), which is the number of questions selected as significant in the process of building the proposed model. As a result, two different data sets were obtained. The first data set has a dimensional size of (364x30), and the second has a dimensional size of (339 x30). The first sheet was named TR dataset, and the second sheet KRD dataset.

The record for each attribute ranged between 1 and 5, which indicated the security awareness or the vulnerability level of a user with reference to a specific question (a scenario or attack-behavior relation). The range is distributed over Strongly Agree (level 5), Agree (Level 4), Fair (Level 3), Disagree (Level 2) and Strongly Disagree (Level 1). As each question tied with a type or more of the vulnerability that a user may have, an individual that answered (1) for a specific question is fully aware or has less vulnerability than a user who answered (5) for the same question. The model should use this calculation to obtain the vulnerability level of a user with reference to all types of attacks and threats that have been mentioned in the previous sections.

The process of calculating the vulnerability level for OSN users will not be a linear mathematic calculation, as each question has a different impact or weight on the overall vulnerability rate of an OSN user. This means that each type of the scenarios mentioned in Section 3.3.2 has been tied with each question in (Appendix A) through a specific weighted value. The values of these weights are necessary in the process of target identification. The next section explains the process of target identification for each observation.

3.3.6 Target Identification

In the previous section, two different data sets have been built. The sets are different in size and records. However, both sets represent the behaviors of OSN users, each for different cultures. Each observation in both sets represents (30) different behaviors (features) for a user. Each behavior is an observation that indicates that relation with one or more threats or attacks that use OSN and their users' vulnerabilities to penetrate systems or individuals' personal information. This section provides the calculation process for each user's vulnerability level through giving a weight for all scenarios mentioned in (Appendix A). Ticking each question is explaining the existence or non-existence of the relation between the question and the scenario. If the tick exists the relation exist too, and vice-versa. The ticking process is used for computing the weight value of a question based on its relation with all scenarios. A full weight ($\frac{18}{18}$ = 1) is given to a question that is related to all scenarios. For questions that are not fully connected with scenarios different calculations have been used. First, for a specific question, the core scenario for a question will be identified and a score of 50% of the weighted value will be given to that scenario. Second, the rest 50% of the weighted value will be distributed over those scenarios which is equivalent with the research question. Table-3 shows that value of each weight-question relation. The end column of Table-3 shows the overall value of weight for each question.

After identifying the weight of each question, the target of each observation will be computed based on Equation 3.1.

$$T = (((\sum_{i=n}^{i=1} X_i \ W_i)/150) * 100)/150 \qquad \mathbf{(3.1)}$$

Where T is the label value for each observation in the range of (0,1), n is the number of behaviors in an observation, X_i is the level value of the i^{th} question, W_i is the weight's value of the i^{th} question on the target.

Based on Equation 3.1, a vulnerability level for an observation will be estimated. As an observation represents a user behavior, the obtained label for an observation represents the vulnerability of the corresponding user behavior. Via this equation, a user behavior may have (0) or (1). Zero vulnerability level means no vulnerability records in the behavior of an OSN user, while (1) mean a user is fully vulnerable to threats and attacks.

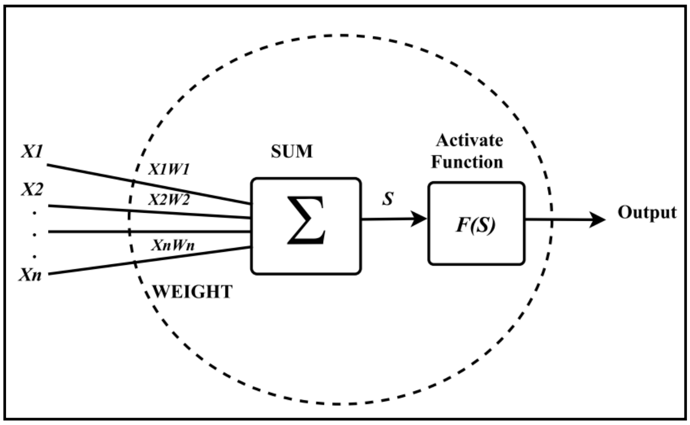
3.4 OSN VULNERABILITY ANALYZING MODEL

There are many intelligent systems used to build models for various applications. One of these applications can predict some hidden events, namely an Artificial Neural Network (ANN) (Bataineh, 2012). In this study, the ability of the ANN is utilized for predicting the vulnerability level of OSN users through analyzing the users’ behavior with reference to

the exploitation policies of threats and attacks.

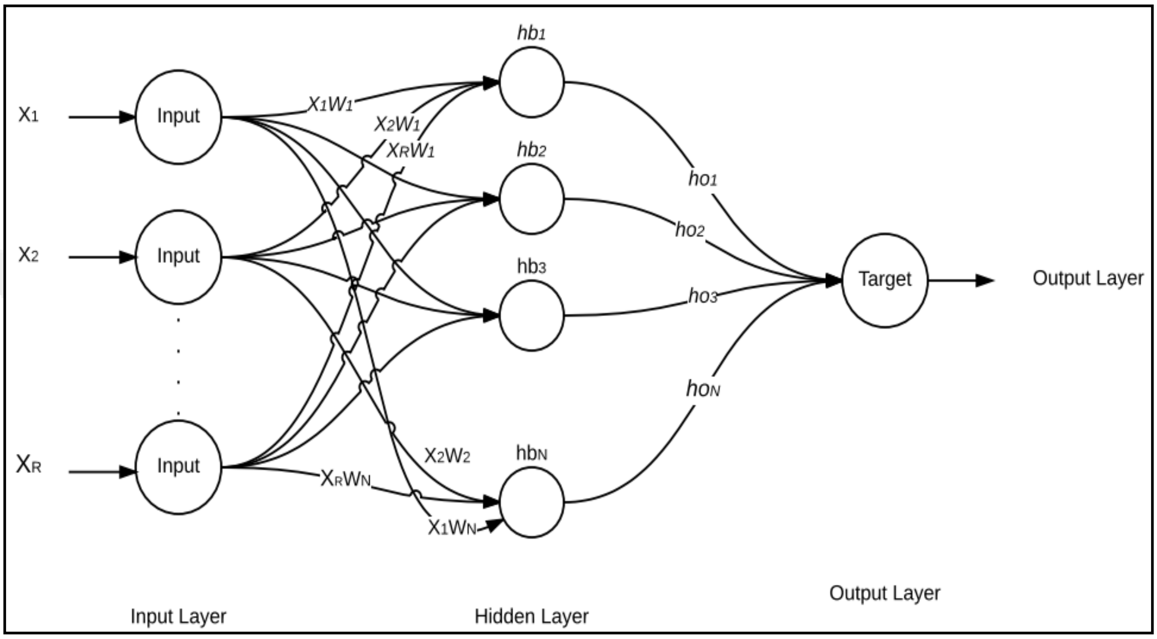
ANN is an intelligent system that artificially mimics the functionalities or operations of the human brain. The simplest unit in ANN is called node. Each node in an ANN structure can receive *n* numbers of input (X_1 to X_n) in which each input (X_i) is associated with a weighted value (w_i). The sum of input-weight product (X_iw_i) will feed to the node, and it will be the input (S) to the activate function *F(S)* of the node. All these details about a single node are shown in Figure (3.4).

Figure 3.4: Single node



The structure of an ANN contains many nodes arranged over three layers; input layer, hidden layer, and output layer. These three layers are connected in a forward based manner through weights. Figure 3.5 shows a typical structure of an ANN.

Figure 3.5: Typical structure of an ANN



Each layer of the ANN contains a number of nodes. A node in a layer is connected to all nodes in the next layer. The number of nodes in each layer varies based on the type and the complexity of the problem. For the problem that is addressed by this work, the input layer has (30) nodes which represent the number of questions asked against each individual (OSN users) (Sivanandam, 2006). The output layer for this application has only one node, which is enough to show the vulnerability level of an OSN user. The hidden layer of utilized ANN has five nodes, which are used to get better accuracy of the predicted vulnerability.

The operation of the ANN has two phases. The first phase is learning or training. The second phase is testing. There are many algorithms for training an ANN. The most common and efficient algorithm is called Feed Forward Back Propagation (FFBP), and is simply called feed forward neural network. The core fundamental of FFBP is adjusting the weighted values that exist between nodes based on the error rate obtained at the output node. The error rate at the output node is computed based on the difference between desired output and actual output (Equation-3.2). As in Equation 3.2, E is the error rate obtained due to the difference between the desired output (y) and the actual output($\bar{y}$).

$$E = (y - \bar{y}) \qquad \textbf{(3.2)}$$

This study used two different data sets to train the FFBP, which means training the network on two different cultures of OSN user behavior. Each data set has been divided into three groups for training, validation, and testing. The training group represented 70 percentage of the dataset while for testing and validation only 15% are used for both respectively. The training part of data is used to teach the network to predict the vulnerability level of OSN user behavior. The 15 percentage of the validation are used to test the network with visible data, while the 15 percentage of testing are used to test the network with invisible data. The FFBP has been trained to use the :*trainlm"* function, which depends on the *Levenberg-Marquardt* training algorithm. This work selected this function, although it needs more memory size than other functions, because it is the fastest learning function for FFBP (Sivanandam, 2006). The activate function, sometimes called transfer function, utilized by this work for the nodes in the hidden layer is *tan-sigmoid*, while for the node at the output layer the *linear* function is used.

3.5 TESTING AND VALIDATION

As mentioned in Section 2.8, two different performance indicators have been used to measure the error rates and the accuracy of the model (Vastrad, 2013), which are means square error and mean absolute error. These two methods indicate the accuracy rate of the BPNN based model in predicting the vulnerability level of OSN users to threat and attackers. However, these two indicators are not enough to validate the ability of the BPNN against other intelligent tools. Intelligent tools are divided into supervised and unsupervised groups (Reddy, 2013). Supervised techniques are usually used for prediction and forecasting, while the unsupervised group is usually used for clustering and classification applications. The model proposed by this work should be compared with tools in the regression and prediction group. Therefore, the work will be validated with an important AI based technique, which is the Support Vector Machine (SVM).

Through two performance indicator methods and results from other intelligent methods, the accuracy and the validity of BPNN as a detector of OSN user vulnerability could be discussed

4. VULNERABILITY LEVEL IDENTIFICATION

4.1 INTRODUCTION

This chapter explains the code and implementation of the model that identifies the level of OSN user vulnerability. Each step of the implementation will be supported by some graphs and results. At each step, the ability of the artificial neural based model is explained. Graphs and results of these steps are analyzed.

The chapter shows two types of validations. First the training validation, for which the same data set has been divided into ten groups. Each time some of these groups are considered for testing. The second is model validation, by which the accuracy of the BPNN will be compared with another technique.

Finally, the model has been generalized over different situations to check whether or not the culture has a negative effect on the model.

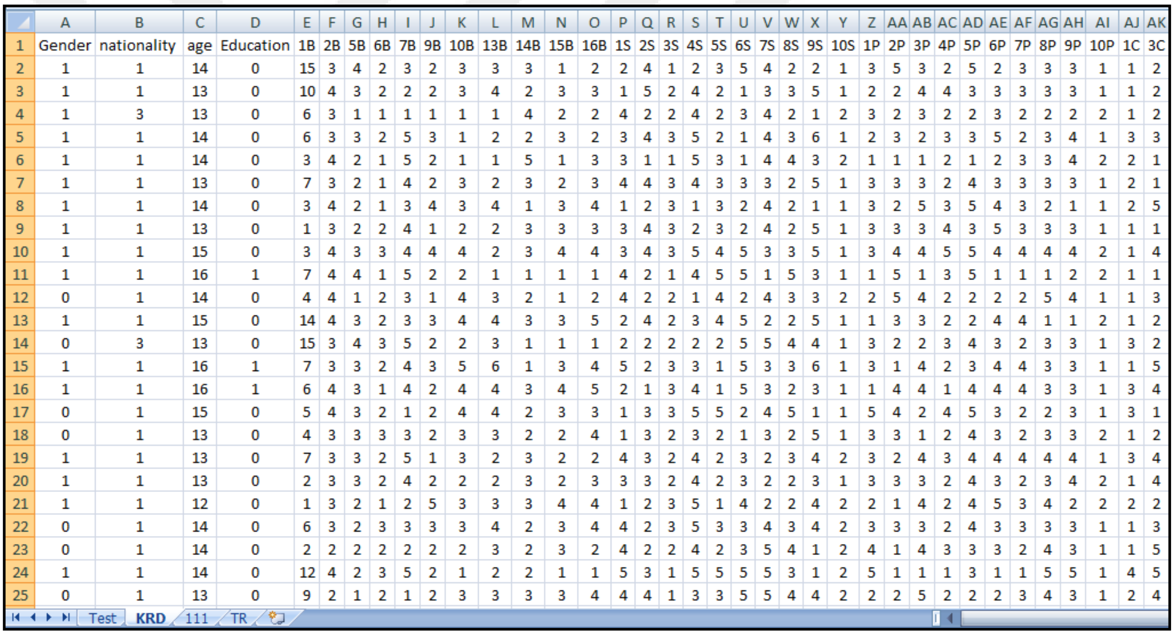
4.2 VULNERABILITY IDENTIFICATION MODEL

Section 3.5 reviews many studies using intelligent systems to build models for different applications. This thesis proposes an Artificial Neural Network (ANN) as a vulnerability identification method, by testing the ability of the ANN to predict the vulnerability level of OSN users. The work uses ANN to build a model that can analyze OSN users' behavior with reference to exploitation policies of threats and attacks. The next subsections explain the process of building the proposed ANN model.

4.2.1 Input Data Set

This work has two types of input data sets, which are collected or obtained from two different cultures as mentioned in Section 3.3.5. The input dataset includes 30 independent variables, where each is a feature of OSN user behavior. The first data set, collected from the Kurdistan region of Iraq, has a dimensional size of (364x30), while the second has a dimensional size of (339 x30) and was collected from Turkey. The first sheet is labeled KRD dataset, and the second sheet TR dataset. The number of features in both data sets is the same, the only difference between them is the number of observations. Figure 4.1 shows a part of these data sets.

Figure 4.1: A part of the input data set



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK
1	Gender	nationality	age	Education	1B	2B	5B	6B	7B	9B	10B	13B	14B	15B	16B	1S	2S	3S	4S	5S	6S	7S	8S	9S	10S	1P	2P	3P	4P	5P	6P	7P	8P	9P	10P	1C	3C
2	1	1	14	0	15	3	4	2	3	2	3	3	3	1	2	2	4	1	2	3	5	4	2	2	1	3	5	3	2	5	2	3	3	3	1	1	2
3	1	1	13	0	10	4	3	2	2	2	3	4	2	3	3	1	5	2	4	2	1	3	3	5	1	2	2	4	4	3	3	3	3	3	1	1	2
4	1	3	13	0	6	3	1	1	1	1	1	1	4	2	2	4	2	2	4	2	3	4	2	1	2	3	2	3	2	2	3	2	2	2	2	1	2
5	1	1	14	0	6	3	3	2	5	3	1	2	2	3	2	3	4	3	5	2	1	4	3	6	1	2	3	2	3	3	5	2	3	4	1	3	3
6	1	1	14	0	3	4	2	1	5	2	1	1	5	1	3	3	1	1	5	3	1	4	4	3	2	1	1	1	2	1	2	3	3	4	2	2	1
7	1	1	13	0	7	3	2	1	4	2	3	2	3	2	3	4	4	3	4	3	3	3	2	5	1	3	3	3	2	4	3	3	3	3	1	2	1
8	1	1	14	0	3	4	2	1	3	4	3	4	1	3	4	1	2	3	1	3	2	4	2	1	1	3	2	5	3	5	4	3	2	1	1	2	5
9	1	1	13	0	1	3	2	2	4	1	2	2	3	3	3	3	4	3	2	3	2	4	2	5	1	3	3	3	4	3	5	3	3	3	1	1	1
10	1	1	15	0	3	4	3	3	4	4	4	2	3	4	4	3	4	3	5	4	5	3	3	5	1	3	4	4	5	5	4	4	4	4	2	1	4
11	1	1	16	1	7	4	4	1	5	2	2	1	1	1	1	4	2	1	4	5	5	1	5	3	1	1	5	1	3	5	1	1	1	2	2	1	1
12	0	1	14	0	4	4	1	2	3	1	4	3	2	1	2	4	2	2	1	4	2	4	3	3	2	2	5	4	2	2	2	2	5	4	1	1	3
13	1	1	15	0	14	4	3	2	3	3	4	4	3	3	5	2	4	2	3	4	5	2	2	5	1	1	3	3	2	2	4	4	1	1	2	1	2
14	0	3	13	0	15	3	4	3	5	2	2	3	1	1	1	2	2	2	2	2	5	5	4	4	1	3	2	2	3	4	3	2	3	3	1	3	2
15	1	1	16	1	7	3	3	2	4	3	5	6	1	3	4	5	2	3	3	1	5	3	3	6	1	3	1	4	2	3	4	4	3	3	1	1	5
16	1	1	16	1	6	4	3	1	4	2	4	4	3	4	5	2	1	3	4	1	5	3	2	3	1	1	4	4	1	4	4	4	3	3	1	3	4
17	0	1	15	0	5	4	3	2	1	2	4	4	2	3	3	1	3	3	5	5	2	4	5	1	1	5	4	2	4	5	3	2	2	3	1	3	1
18	0	1	13	0	4	3	3	3	3	2	3	3	2	2	4	1	3	2	3	2	1	3	2	5	1	3	3	1	2	4	3	2	3	3	2	1	2
19	1	1	13	0	7	3	3	2	5	1	3	2	3	2	2	4	3	2	4	2	3	2	3	4	2	3	2	4	3	4	4	4	4	4	1	3	4
20	1	1	13	0	2	3	3	2	4	2	2	2	3	2	3	3	3	2	4	2	3	2	2	3	1	3	3	3	2	4	3	2	3	4	2	1	4
21	1	1	12	0	1	3	2	1	2	5	3	3	3	4	4	1	2	3	5	1	4	2	2	4	2	2	1	4	2	4	5	3	4	2	2	2	2
22	0	1	14	0	6	3	2	3	3	3	3	4	2	3	4	4	2	3	5	3	3	4	3	4	2	3	3	3	2	4	3	3	3	3	1	1	3
23	0	1	14	0	2	2	2	2	2	2	2	3	2	3	2	4	2	2	4	2	3	5	4	1	2	4	1	4	3	3	3	2	4	3	1	1	5
24	1	1	14	0	12	4	2	3	5	2	1	2	2	1	1	5	3	1	5	5	5	5	3	1	2	5	1	1	1	3	1	1	5	5	1	4	5
25	0	1	13	0	9	2	1	2	1	2	3	3	3	3	4	4	4	1	3	3	5	5	4	4	2	2	2	5	2	2	2	3	4	3	1	2	4

The number of these features identifies the number of input nodes of the proposed model. Next section defines the structure of the proposed ANN.

4.2.2 Our Proposed Model

This section identifies the specific structure of the proposed model. The input layer of this model has 30 nodes. Each node represents a behavior of an OSN user. A set of features (i.e. 30 elements, which represent an observation) will be fed to the input layer, each node receives a feature. Each observation describes the overall behavior of an OSN user.

The input layer only has one function, which is to receive the input information (set of elements or features) for an observation and forward them to every node in the hidden layer. According to Figure 3.3, all elements in an observation will be associated with their corresponding weighted values. Then, the summation of all product results (elements' product weight) will be the input information for every node in the hidden layer. For this application, the defined network only has one hidden layer with five nodes.

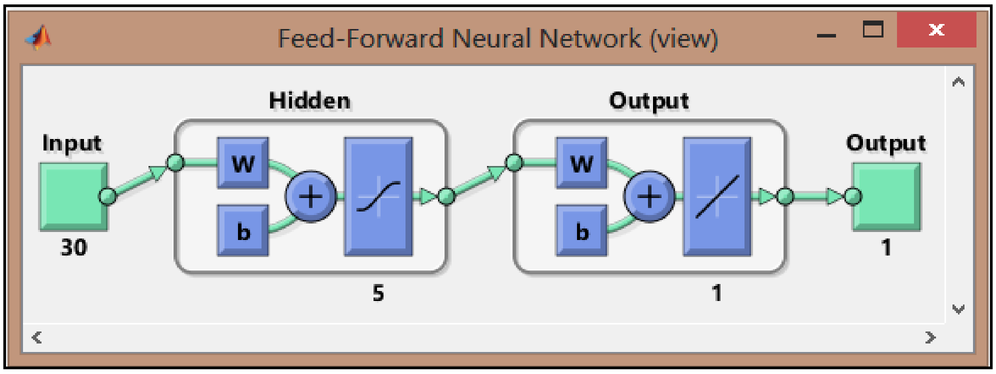
Again, nodes in the hidden layer are associated to the nodes in the output layer through some weighted values. The output layer of this application has only one node. Through this single node the model can display the level of an OSN user's vulnerability.

Statement-1 in the Matlab code shown below can create an ANN with the above-mentioned specification. Through Statement-2 in the code below, the structure of the proposed model can be illustrated, as in Figure 4.2.

```
net = feedforwardnet(5,'trainlm'); ..... Statement-1
```

```
view(net) ..... Statement-2
```

Figure 4.2: The Specific ANN structure of the proposed model



Some details in Statement-1 also belong to the type of ANN learning algorithm and function that is proposed by the work. In the figure, other functions could explain the type of active functions that can be found inside the nodes of the network.

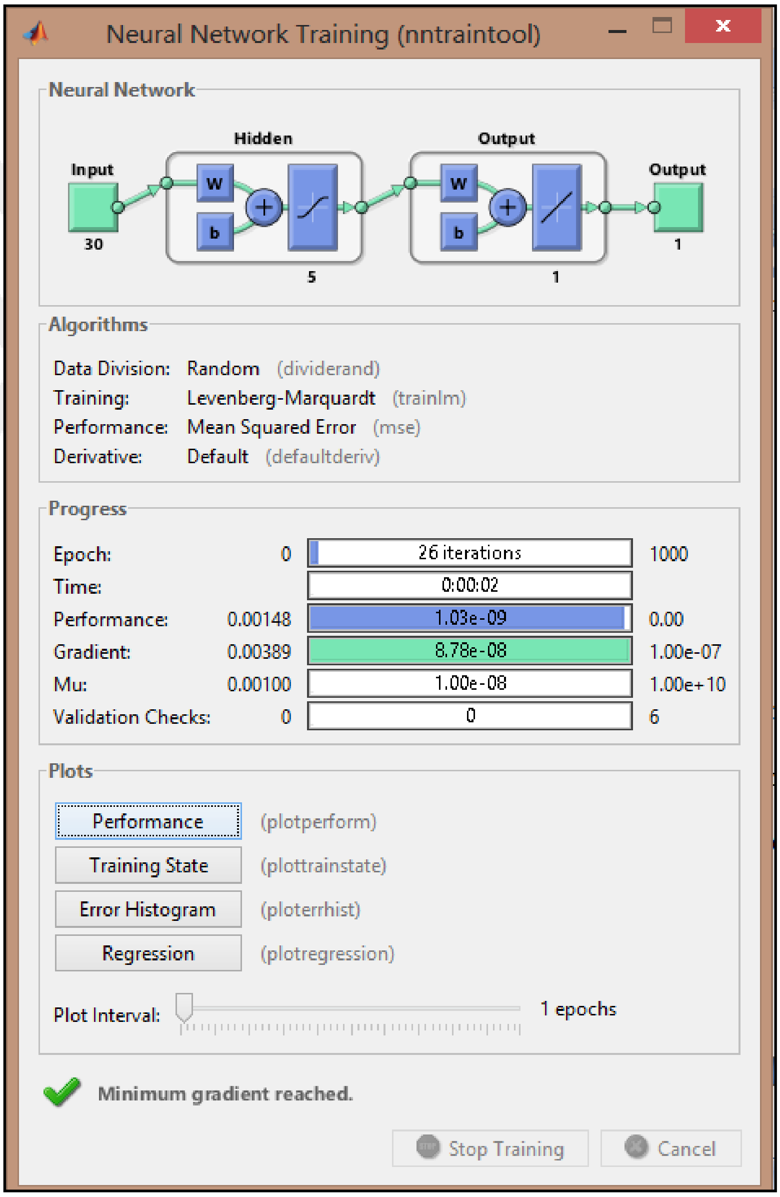
4.2.3 Model Training

Two important training related parameters can be captured from Statement-1 (Section 4.2.2). The first parameter is (*feedforwardnet*). Through this part of the statement, the study declares the type of learning on which the network depends, which is the *Feed Forward Back Propagation* neural network. The second part or parameter is (*'trainlm'*). This part shows that the proposed network uses Levenberg-Marquardt optimization to update the weights and biases values during the training or learning process. Statement-3 shows how Matlab code instructs the created (net) to start training.

net = train(net,in,tr);...... Statement-3

Statement-3 has three parameters. The first parameter is the name of the neural network created by Statement-1. The second parameter (in) refers to the input features (independent variables). The third parameter refers to the target (dependent variables). Each time the training is executed, the input data set has been randomly divided into three groups. The first group is called training, which represents 70 percentage of the whole data set's observations (i.e. for the TR data set, which has 339 observations, only 237 observations are used for training). The second group is validation, in which only 15 percentage of the whole data set is considered (i.e. 51 observations). These observations are considered as seen data. Like the validation, the testing group also takes 51 observations, which means 15 percentage of the whole data set's observation number.

Figure 4.3: Training Progress of the model



Neural Network Training (nntraintool)

Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Derivative: Default (defaultderiv)

Progress

Epoch: 0 26 iterations 1000
Time: 0:00:02
Performance: 0.00148 1.03e-09 0.00
Gradient: 0.00389 8.78e-08 1.00e-07
Mu: 0.00100 1.00e-08 1.00e+10
Validation Checks: 0 0 6

Plot Interval: 1 epochs

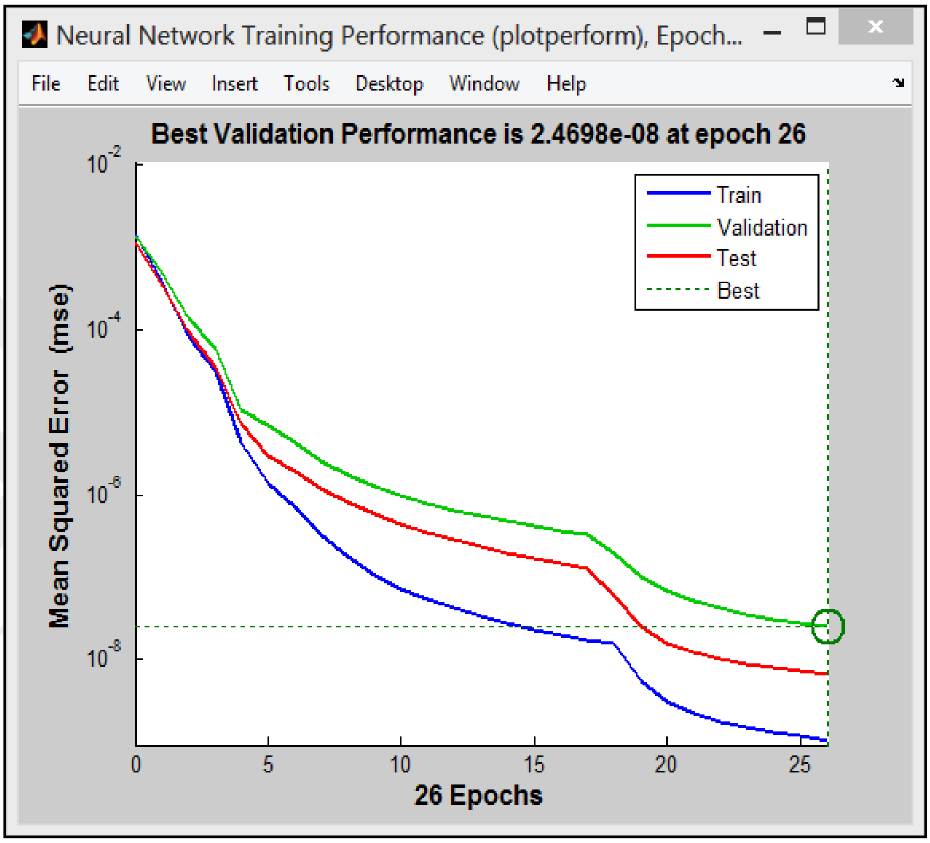
Minimum gradient reached.

When this command is performed, the window below will open in Matlab (Figure 4.3). This window can capture a lot of information and sections as summarized below:

1. Neural Network Section. This section provides details about the structure of the created network. Section 4.2.2 explains these details.
2. Under the section Algorithm, the information below is provided:
    a. Data Division explains that the input data set has been divided for training, validation, and random testing.
    b. Training shows that the (*feedforwardnet*) algorithm is used for training and the (*'trainlm'*) function is used for updating weights and biases.
    c. Performance measures the rate of accuracy of the proposed model. This work focuses on the Mean Square Error (mse) to check the network's performance.
    d. Derivative shows the type of gradient function that checks the optimality of the errors or performances.
3. Progress explains the following:
    a. Epochs; the number of iterations performed from the beginning of the training before reaching the goal. The code sets the number of epochs on 1000, however, the training only required 26 epochs.
    b. Time indicates the duration required until the training is complete. For this model, only two ms are needed. This factor shows that the time complexity of this model is very small.
    c. Performance shows the rate of the mse of the model. The best mse in the proposed model has been minimized to 8.78e-08.
    d. Gradient shows the rule by which the derivative of the solutions can be calculated to find minimum and maximum solutions.
4. Through Plots, results of the training can be illustrated and explained.
    a. Performance can show different explanations of the training progress. Figure 4.3 shows the performance of the training obtained by the proposed model. The figure shows the relation between the MSE rate and the epoch's number (at i^{th} iteration number the rate of the MSE). The relation is plotted for training, validation and testing. The ideal case

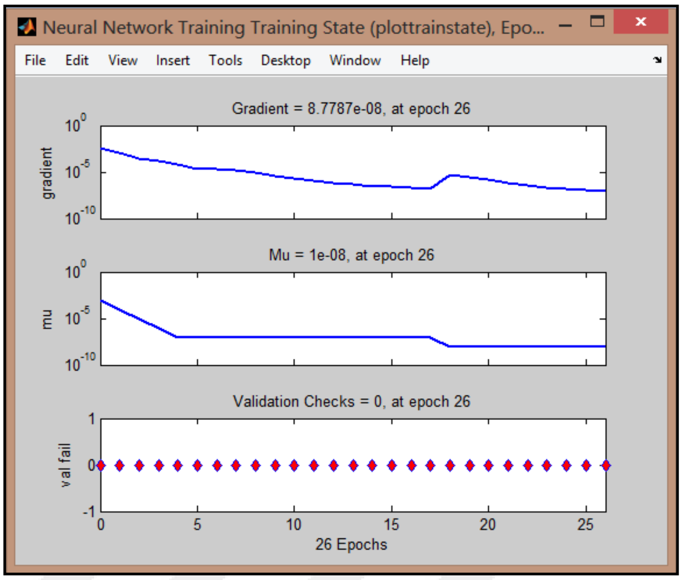
of the performance plot is where the three curves of the training, validation, and testing are as close as possible. The values of these three types of performance are placed between 1e-07 to 1e-10, which are very close.

Figure 4.4: Training, Validation, and Testing of the Proposed Model



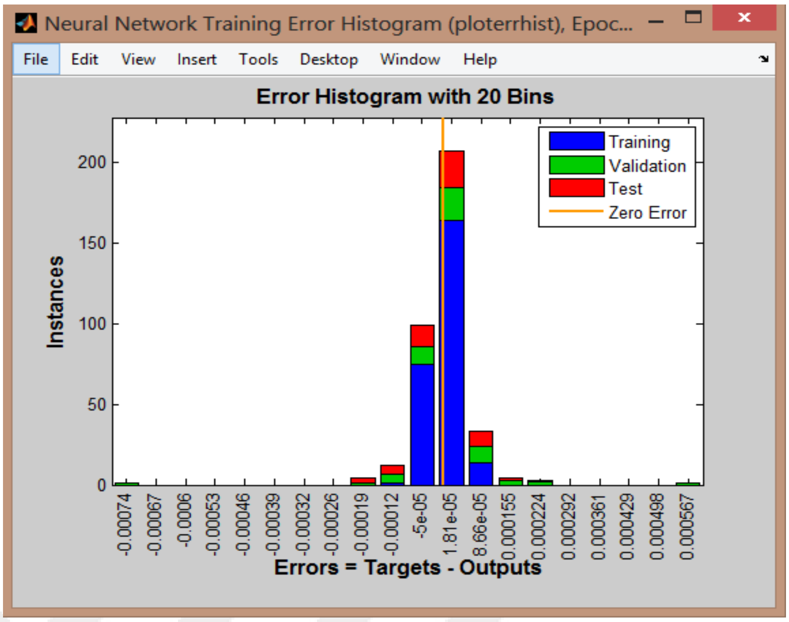
b. An important part of the training is the number of validation checks. The parameter shows the times in which the network is descending in the opposite of the learning direction. The validation check is a parameter by which the training will be stopped if the training process passes a predefined value for this parameter. For this model, the predefined number for the validation check is six. However, all 26 iterations show that number of validation checks is equal to zero which means there is no descent in the opposite direction.

Figure 4.5: Training state for validation check



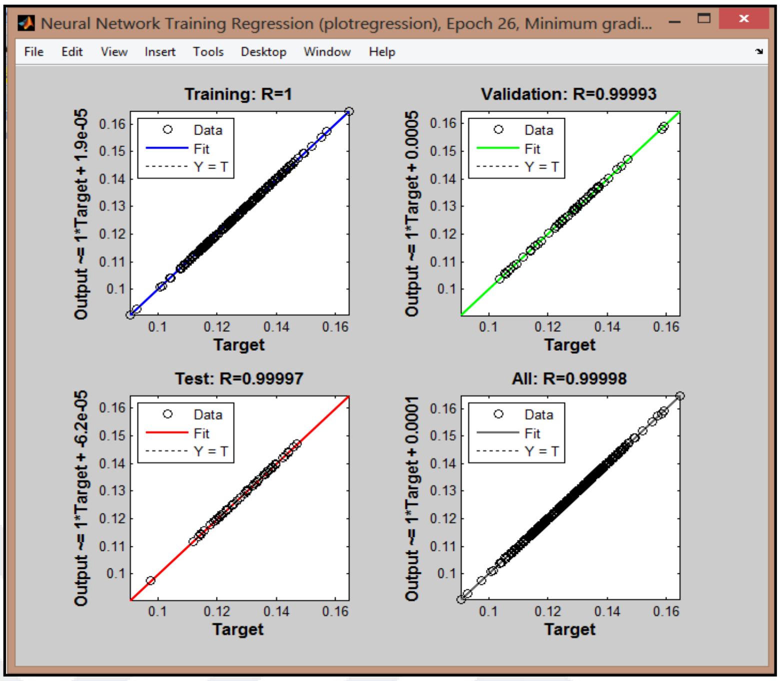
c. The error histogram shows the division of the errors over some ranges. It shows the number of instances that have the same value of errors. It is preferred that most cases should have as few errors as possible. The figure shows that out of 339 cases, 200 cases have fewer errors, i.e. 1.81e-05, 100 cases have a negative error rate with values between 5e-05, and the remaining cases have errors in the range from -0.00074 to 0.000567.

Figure 4.6: Histogram of the errors



d. The last parameter is called R-square. This parameter shows the closeness of the input data set to the regression line. It is preferred that the value of this R is as close as possible. For the proposed model, the value of the R is equal to 0.99. Moreover, the R value of the model has been obtained at each step of the training, validation, testing, and overall. The R values at each step are good enough to consider the performance of the model.

Figure 4.7: R-square value for the model



4.2.4 Training Validation

For any prediction model, the validation process is very essential. To achieve that, this work depends on the *k-fold* method. Through this method, the input data set has been divided into ten groups. Every time a group is considered for testing, the other nine groups will be used for training. The performance of each of the ten executions will collected. This process has been achieved for both data sets, and the results are shown in Table 4.1 and Table 4.2.

Based on these tables, it is easy to find the average performance and the mean. By comparing these two values, it is easy to see that two numbers are very close to each other. This process validates the learning received by the proposed network.

Table 4.1: Performance of 10 fold validation for TR data set

K^{th} Number	Performance (mse)
1.	7.25E-10
2.	3.86E-09
3.	6.08E-10
4.	1.17E-08
5.	7.46E-09
6.	2.83E-07
7.	1.69E-09
8.	1.57E-09
9.	3.97E-09
10.	3.14E-09
Average	9.53E-09
Mean	6.08E-10

Table 4.2: Performance of 10 fold validation for KR data set

K^{th} Number	Performance (mse)
1.	2.88E-10
2.	2.75E-08
3.	1.20E-07
4.	4.03E-09
5.	6.33E-10
6.	7.86E-08
7.	2.26E-08
8.	7.23E-09
9.	2.03E-08
10.	9.96E-08
Average	3.81E-08
Mean	2.88E-10

4.2.5 Model Testing

Usually ANN will be tested through unseen data. To achieve that, this work tests the model in four cases.

1. Testing the model with the KRD dataset after training with the TR dataset.
2. Testing the model with the TR dataset after training with the KRD dataset.
3. Testing the model with the KRD dataset after training with the KRD dataset.
4. Testing the model with the TR dataset after training with the TR dataset.

The results of these four types of tests are illustrated in Table-4.3.

Table 4.3: Testing the model in four situations

Trained- tested with	MSE	MAE
KRD – KRD	2.88E-10	7.76E-06
KRD – TR	2.0964e-07	1.5475e-04
TR – TR	6.08E-10	5.22E-06
TR – KRD	4.4256e-07	2.0978e-04

Results in all four situations show that the model can be used in different cultures. This generalization of the model is going back to the training process that depended on the analysis of OSN users from the perspective of threats and attacks.

4.3 MODEL VALIDATION

To test the performance of the BPNN model, this work checks the accuracy of an important type of supervised learning model that is more frequently utilized by researchers, the Support Vector Machine (SVM). The work preferred to utilize SVM as it is a supervised technique like the BPNN. Both techniques are tested in all four situations as mentioned in Table 4.4.

Table 4.4: Model validation with other techniques

Trained- Tested	BPNN		SVM	
	MSE	MAE	MSE	MAE
KRD – KRD	1.6275e-08	4.3112e-05	0.064	0.064
KRD – TR	2.0964e-07	1.5475e-04	0.1917	0.1911
TR – TR	1.5153e-08	4.6466e-05	0.0664	0.0688
TR – KRD	4.4256e-07	2.0978e-04	0.1912	0.1908

As stated in Section 4.2.5, the accuracy has been checked through two main performance indicators, which are root mean square error and absolute mean error. The indicator performance shows the outperformance of the BPNN over the SVM.

5. CONCLUSION AND FUTURE WORKS

5.1 CONCLUSION

This study started with finding gaps in the OSN field, questions that could be answered, and objectives that could be targeted. The relations between OSN user behavior and the policies of system intruders and/or attackers were investigated at an early stage. These relations have been analyzed from the point of OSN user vulnerabilities.

From Section 3.3.2 it becomes clear that in order to penetrate systems, today’s attackers are more often targeting user vulnerabilities than system vulnerabilities. Through various means of deceit, they attempt to abuse the users’ behavior in order to identify open channels or get access to the users’ systems for malicious activities, which include controlling and overriding systems, exploring accounts, and mining confidential and private information.

This work has concluded that the relations between OSN users’ behavior and attackers’ policies could be interpreted by some common and understandable questions. Each question comes in a scenario that reflects the policy by which an attacker misuses a behavior of OSN users. Through leveling or scaling the questions, users can point out their level with reference to each question, that is, with reference to each attacker's policy. It is not easy for users, especially for those who are less security aware, to understand or to interpret their situation. However, the 30 questions asked by this study can serve as a base for vulnerability identification against 18 common OSN attacks and threats. It will be more difficult for simple users to forecast their vulnerability level as questions interconnect with a scenario or more than one scenario through some obtained weights. To make all these above scenarios easy for OSN users, an intelligent- based model is proposed by this work as vulnerability level identifier of OSN users.

To build the proposed model, this work has utilized two AI based models, BPNN and SVM. The same dataset has been used to train and test the vulnerability level identifier for the models built with BPNN and with SVM. From the results the work concluded:

1. The BPNN based model gives better accuracy than other types of AI techniques.
2. The accuracy of the model is not affected by the culture from where the dataset has been collected.
3. The model interprets user behavior - attack policy relations into measurable indicators thorough which users can understand their level. These relations are common across the globe, although the vulnerability of OSN users differs.
4. Statistical figures can only show the percentage of OSN users with reference to one or several attacks, and only provide limited awareness that cannot efficiently interconnect with OSN users.

5.2 OBJECTIVE ACHIEVEMENTS

1. To study the attacks penetrating systems through behaviors and vulnerabilities of OSN users.

   There are different types of attacks that can penetrate a system. This work commenced by reviewing an overall study on most threats and attacks to OSNs that possibly have negative impacts on OSN users. Accordingly, many types of OSN attacks were found and classified into different groups. The groups comprise 18 threats that are able to penetrate systems through OSN users. Each of these threats and attacks has its own policy of penetrating the OSN users' systems by preying on their vulnerability.
2. To investigate the relation between different threats and attacks with OSN user vulnerabilities.

   To investigate the relations between OSN based attacks and users' vulnerability that can be interpreted from their behavior, the work prepared 30 understandable questions based on OSN behavior that leads users into becoming victims of an attacker. The important part of the questionnaire was drafting questions in such a way that they reflected the relations between OSN user behavior and the scenarios or policies pursued by OSN based attacks. The investigation even studied the impact of cultures on OSN user behavior through distributing questionnaires in two different cultures (countries).

3. To build an AI model that can detect the vulnerability level of OSN users.

   This objective has been addressed in several sections (in subchapters 3.3 to 3.6). Figure 3.1 showed the detailed steps of this model, and the implementation part of this model has been described in detail in Chapter 4 (in subchapters 4.2 and 4.3).

4. To test and validate the proposed model against some performance indicators.

   To test and validate the BPNN technique the study used two different performance indicators to measure the error rates and the accuracy of the model, namely MSE and MAE. These two methods indicated the accuracy of the BPNN based model in predicting the vulnerability level of OSN users against threat and attackers. As explained in Section 4.2.3, good results were obtained from the BPNN model test, such as minimizing the error rate to 8.78e-08 within 26 epochs.

   Another test was used to validate the BPNN based model. The work used the SVM, an important AI model for vulnerability level detection of OSNs users besides the BPNN. The SVM method was used to validate the result obtained from the BPNN. The results showed that BPNN is more powerful than SVM.

5.3 DISCUSSION

Through reviewing different research work, this work has performed a comprehensive study on OSN systems and the threats and the attacks that can penetrate these systems. In addition, the study has also focused on OSN user activities and behavior within the OSN systems, with reference to the policies used by attackers. This information has been analyzed to find out the exact activities that attackers may perform to penetrate systems, taking advantage of OSN users' vulnerability and behavior. Through that, the work found the most effective threats and attacks that lead to the loss of privacy for OSN users and cause their devices to malfunction. Previous work has only provided OSN users with some awareness in attempting to help them to prevent threats and attacks. However, most information has been presented in such ways that common users cannot understand it; furthermore, the methods are non-scalable.

Showing the scale and level of an OSN user's vulnerability can be used to analyze and identify the overall situation for the user. The work needs to build a predictor model to perform these analyses through determining the vulnerability scale of a user against most common threats and attacks. The work showed that BPNN is the most suitable AI technique for building this predictor model, as the error rate of the BPNN based model reaches (8.78e-08). The most important drawback in previous work is that users need special awareness of each culture, as behaviors of OSN users change between cultures. However, results showed that the proposed BPNN based model is culture independent, as its accuracy has not been affected by the change of the training dataset that trained the model and collected data in different cultures. Table (4.4) shows four cases to prove this point.

Finally, users can identify their own weak behavior through the questions used for collecting their answers for each behavior against an attack. As every question is written in an easy and understandable way, describing the attack-behavior scenario, users can get an idea about which behavior to avoid.

5.4 FUTURE WORKS

This work has tried hardly to find the best AI model and technique for predicting the users' vulnerability and security awareness level by using MATLAB and design a GUI Application for testing the OSN users, then testing the model and applying it on two different cultures. For the future stage, this work suggests an online web application that any OSN user can directly browse the page for realizing their vulnerability level by applying and subscribe the page. After registering in the web site, users will answer the questions to get their vulnerability level. Passing times, a data sheet could be collected involving different information such as the username, birthday, country, his/her education level, some public activities of the users, besides their vulnerability scales against each attack and the overall vulnerability. The purpose of storing these information is to collect real records on OSN user behavior in multi cultures, then publishing these data to allow researchers to use these data for further researching in this field.

The second future idea for this work is developing an application that could be installed on PCs. Users when operating of PCs can get their vulnerability level through monitoring the activities of the user for a specific duration. The application can work like internet security or malware detection systems by giving the user some awareness (popping messages) indicating the vulnerability level with solutions.

REFERENCES

(NASAA), N. A. S. A. A. 2011. *Informed Investor Advisory: Social Networking* [Online]. Washington, DC, USA,. Available: http://www.nasaa.org/5568/informed-investor-advisory-social-networking/
].

AHMADINEJAD, S. H. & FONG, P. W. 2014. Unintended disclosure of information: Inference attacks by third-party extensions to Social Network Systems. *Computers & Security,* 44**,** 75-91.

AL HASIB, A. 2009. Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security,* 9**,** 288-93.

AMIN, T., OKHIRIA, O., LU, J. & AN, J. 2010. Facebook: A Comprehensive Analysis of Phishing on a Social System. *Term project report*.

BALSAMO, S., DI MARCO, A., INVERARDI, P. & SIMEONI, M. 2004a. Model-based performance prediction in software development: A survey. *Software Engineering, IEEE Transactions on,* 30**,** 295-310.

BALSAMO, S., MARCO, A. D., INVERARDI, P. & SIMEONI, M. 2004b. Model-based performance prediction in software development: A survey. *Software Engineering, IEEE Transactions on,* 30**,** 295-310.

BALTAZAR, J., COSTOYA, J. & FLORES, R. 2009. The real face of koobface: The largest web 2.0 botnet explained. *Trend Micro Research,* 5**,** 10.

BATAINEH, M. H. 2012. Artificial neural network for studying human performance.

BEACH, A., GARTRELL, M. & HAN, R. Solutions to security and privacy issues in mobile social networking. Computational Science and Engineering, 2009. CSE'09. International Conference on, 2009. IEEE, 1036-1042.

BOSHMAF, Y., MUSLUKHOV, I., BEZNOSOV, K. & RIPEANU, M. The socialbot network: when bots socialize for fame and money. Proceedings of the 27th Annual Computer Security Applications Conference, 2011. ACM, 93-102.

BOSSLER, A. M. & HOLT, T. J. 2009a. On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology,* 3**,** 400-420.

BOSSLER, A. M. & HOLT, T. J. 2009b. On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology,* 3**,** 400.

BUCHEGGER, S. & DATTA, A. A case for P2P infrastructure for social networks-opportunities & challenges. Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on, 2009. IEEE, 161-168.

BUCHEGGER, S., SCHIÖBERG, D., VU, L.-H. & DATTA, A. PeerSoN: P2P social networking: early experiences and insights. Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, 2009. ACM, 46-52.

CREESE, S., GOLDSMITH, M., NURSE, J. R. & PHILLIPS, E. A data-reachability model for -elucidating privacy and security risks related to the use of online social networks. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012. IEEE, 1124-1131.

DAMEN, S. & ZANNONE, N. 2013. Privacy implications of privacy settings and tagging in facebook. *Secure Data Management.* Springer.

DANIEL, W., XU, X., BAI, M., CHEN, Z., MENG, X. & WANG, Y. PRIVACY ISSUES IN ONLINE SOCIAL NETWORKS: USER BEHAVIORS AND THIRD-PARTY APPLICATIONS.

DANIEL, W., XU, X., BAI, M., CHEN, Z., MENG, X. & WANG, Y. 2014. PRIVACY ISSUES IN ONLINE SOCIAL NETWORKS: USER BEHAVIORS AND THIRD-PARTY APPLICATIONS.

DAVE, D., MISHRA, N. & SHARMA, S. 2013. Detection Techniques of Clone Attack on Online Social Networks: Survey and Analysis.

DEAN, M. Oct. 2012. The Story of Amanda Todd Available from: Available: http://www.newyorker.com/online/blogs/culture/2012/10/amanda-todd-michael-brutsch-and-free-speechonline.html.

DUNCAN, S. 2008. MySpace is also their space: Ideas for keeping children safe from sexual predators on social-networking sites. *Kentucky Law Journal,* 96.

FACEBOOK 2014. Facebook Reports Fourth Quarter and Full Year 2014 Results. *Facebook Reports Fourth Quarter and Full Year 2014 Results.* Facebook.

FACEBOOK, I. 2015. Facebook Reports Third Quarter 2015 Results. *Facebook Reports Third Quarter 2015 Results.* Facebook, Inc.

FIRE, M., GOLDSCHMIDT, R. & ELOVICI, Y. 2013. Online Social Networks: Threats and Solutions.

FIRE, M., GOLDSCHMIDT, R. & ELOVICI, Y. 2014. Online Social Networks: Threats and Solutions. *Communications Surveys & Tutorials, IEEE,* 16**,** 2019-2036.

FIRE, M., KATZ, G. & ELOVICI, Y. 2012. Strangers intrusion detection-detecting spammers and fake proles in social networks based on topology anomalies. *HUMAN,* 1**,** pp. 26-39.

FONG, P. W., ANWAR, M. & ZHAO, Z. 2009. A privacy preservation model for facebook-style social network systems. *Computer Security–ESORICS 2009.* Springer.

GAO, H., HU, J., HUANG, T., WANG, J. & CHEN, Y. 2011. Security issues in online social networks. *Internet Computing, IEEE,* 15**,** 56-63.

GAYATHRI, K., THOMAS, T. & JAYASUDHA, J. 2012. Security issues of media sharing in social cloud. *Procedia Engineering,* 38**,** 3806-3815.

GUHA, S., TANG, K. & FRANCIS, P. NOYB: Privacy in online social networks. Proceedings of the first workshop on Online social networks, 2008. ACM, 49-54.

GUNATILAKA, D. A survey of privacy and security issues in social networks. Proceedings of the 27th IEEE International Conference on Computer Communications. Washington: IEEE Computer Society, 2011.

HE, B.-Z., CHEN, C.-M., SU, Y.-P. & SUN, H.-M. 2014. A defence scheme against identity theft attack based on multiple social networks. *Expert Systems with Applications,* 41**,** 2345-2352.

HEATHERLY, R., KANTARCIOGLU, M. & THURAISINGHAM, B. 2013. Preventing private information inference attacks on social networks. *Knowledge and Data Engineering, IEEE Transactions on,* 25**,** 1849-1862.

HO, K. 2015. 41 Up-to-Date Facebook Facts and Stats. *Social Media Marketing Report.* http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats.

HOGBEN, G. 2007. Security issues and recommendations for online social networks. *ENISA position paper,* 1**,** 1-36.

HUANG, T.-K. 2013. Understanding Online Malicious Behavior: Social Malware and Email Spam.

HUANG, T.-K., RAHMAN, M. S., MADHYASTHA, H. V., FALOUTSOS, M. & RIBEIRO, B. An analysis of socware cascades in online social networks. Proceedings of the 22nd international conference on World Wide Web, 2013. International World Wide Web Conferences Steering Committee, 619-630.

HUMPHREYS, L., GILL, P. & KRISHNAMURTHY, B. How much is too much? Privacy issues on Twitter. Conference of International Communication Association, Singapore, 2010.

IVANCEVIC, V. G. I. A. T. T. 2010. Brain and Classical Neural Network. *Quantam Neural Computation.* Netherlands: Springer Netherlands.

JIN, L., CHEN, Y., WANG, T., HUI, P. & VASILAKOS, A. V. 2013. Understanding user behavior in online social networks: A survey. *Communications Magazine, IEEE,* 51**,** 144-150.

JOE, M. M. & RAMAKRISHAN, B. 2014. Enhancing Security Module to Prevent Data Hacking in Online Social Networks. *Journal of Emerging Technologies in Web Intelligence,* 6**,** 184-191.

KAYES, I. & IAMNITCHI, A. 2015. A Survey on Privacy and Security in Online Social Networks. *arXiv preprint arXiv:1504.03342*.

KRISHNAMURTHY, B. & WILLS, C. E. Privacy leakage in mobile online social networks. Proceedings of the 3rd Conference on Online social networks, 2010. USENIX Association, 4-4.

LIVSHITS, V. B. & CUI, W. Spectator: Detection and Containment of JavaScript Worms. USENIX Annual Technical Conference, 2008. 335-348.

LUNDEEN, R., OU, J. & RHODES, T. 2011. New ways i'm going to hack your web app. *Blackhat AD***,** 1-11.

MAO, Z., LI, N. & MOLLOY, I. 2009. Defeating cross-site request forgery attacks with browser-enforced authenticity protection. *Financial Cryptography and Data Security.* Springer.

MARINOS, L., ACQUISTI, A., ANDERSON, P., CADZOW, S., CARR, J., DICKMAN, P., GRAY, C., LAING, C., PAPAKONSTANTINOU, V. & PASIC, A. 2011. Cyber-bullying and online grooming: Helping to protect against the risks.

MAXWELL CHI, M. C. S. N. March 16, 2011. Security Policy and Social Media Use. SANS Institute InfoSec Reading Room.

MCMILLAN, R. 2009. Researchers make wormy twitter attack. *PCWorld, San Francisco, CA, USA, Mar*.

MILLS, E. 2009. Facebook hit by phishing attacks for a second day. *CNET News***,** 8301-1009.

MISLOVE, A., MARCON, M., GUMMADI, K. P., DRUSCHEL, P. & BHATTACHARJEE, B. Measurement and analysis of online social networks. Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, 2007. ACM, 29-42.

MISLOVE, A., VISWANATH, B., GUMMADI, K. P. & DRUSCHEL, P. You are who you know: inferring user profiles in online social networks. Proceedings of the third ACM international conference on Web search and data mining, 2010. ACM, 251-260.

MOLOK, N. N. A., CHANG, S. & AHMAD, A. 2010. Information leakage through online social networking: Opening the doorway for advanced persistence threats.

MORENO, M. A., VANDERSTOEP, A., PARKS, M. R., ZIMMERMAN, F. J., KURTH, A. & CHRISTAKIS, D. A. 2009. Reducing at-risk adolescents' display of risk behavior on a social networking web site: a randomized controlled pilot intervention trial. *Archives of pediatrics & adolescent medicine,* 163**,** 35-41.

NEI, L. C., CHERNG, L. Y. & SINGH, M. M. 2014. A Case Study on Clickjacking Attack and Location Leakage.

PAUL, I. 2009. Twitter worm: A closer look at what happened. *PCWorld, San Francisco, CA, USA, Apr*.

PENG, W., LI, F., ZOU, X. & WU, J. 2014. A two-stage deanonymization attack against anonymized social networks. *Computers, IEEE Transactions on,* 63**,** 290-303.

RAHMAN, M. S., HUANG, T.-K., MADHYASTHA, H. V. & FALOUTSOS, M. Efficient and Scalable Socware Detection in Online Social Networks. USENIX Security Symposium, 2012. 663-678.

REDDY, E. K. Neural Networks for Intrusion Detection and Its Applications. Proceedings of the World Congress on Engineering, 2013. 3-5.

ROJAS., N. *The Faces of Facebook. [Online]* [Online]. Available: http://app.thefacesoffacebook.com/.

RUTKA, G. 2015. Neural network models for Internet traffic prediction. *Elektronika ir Elektrotechnika,* 68**,** 55-58.

SADEGHIAN, A., ZAMANI, M. & SHANMUGAM, B. Security threats in online social networks. Informatics and Creative Multimedia (ICICM), 2013 International Conference on, 2013. IEEE, 254-258.

SIMONITE, T. March 23, 2015. Fake accounts can inflate follower counts, suppress political messages, and run stealthy social marketing. *Fake Persuaders.*

SIVANANDAM, S. 2006. *Introduction to neural networks using MATLAB 6.0*, Tata McGraw-Hill.

STRUFE, T. 2009. Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine***,** 95.

SYMANTEC APRIL 2015. ISRT 20 INTERNET SECURITY THREAT REPORT.

UNICEF 2011. *Child safety online: Global challenges and strategies*, UNICEF Innocenti Research Centre.

VASTRAD, C. 2013. Performance Analysis Of Neural Network Models For Oxazolines And Oxazoles Derivatives Descriptor Dataset. *arXiv preprint arXiv:1312.2853*.

WEBSITE, T. August, 2014. *peer-to-peer (P2P)* [Online]. http://www.techtarget.com/: techtarget. Available: http://searchnetworking.techtarget.com/definition/peer-to-peer 2014].

WHITMAN, M. & MATTORD, H. 2011. *Principles of information security*, Cengage Learning.

WOLAK, J., FINKELHOR, D. & MITCHELL, K. 2008a. Is talking online to unknown people always risky? Distinguishing online interaction styles in a national sample of youth Internet users. *CyberPsychology & Behavior,* 11**,** 340-343.

WOLAK, J., FINKELHOR, D., MITCHELL, K. J. & YBARRA, M. L. 2008b. Online" predators" and their victims: myths, realities, and implications for prevention and treatment. *American Psychologist,* 63**,** 111.

YEGNANARAYANA1, B. 1994. Artificial neural networks for pattern recognition *Sadhana,* 19**,** 189-238.

ZHANG, C., SUN, J., ZHU, X. & FANG, Y. 2010. Privacy and security for online social networks: challenges and opportunities. *Network, IEEE,* 24**,** 13-18.

ZHANG, J. J. 2005. Introduction to artificial neural network. *Bellingham, WA: Bellingham AI Robotics Society*.

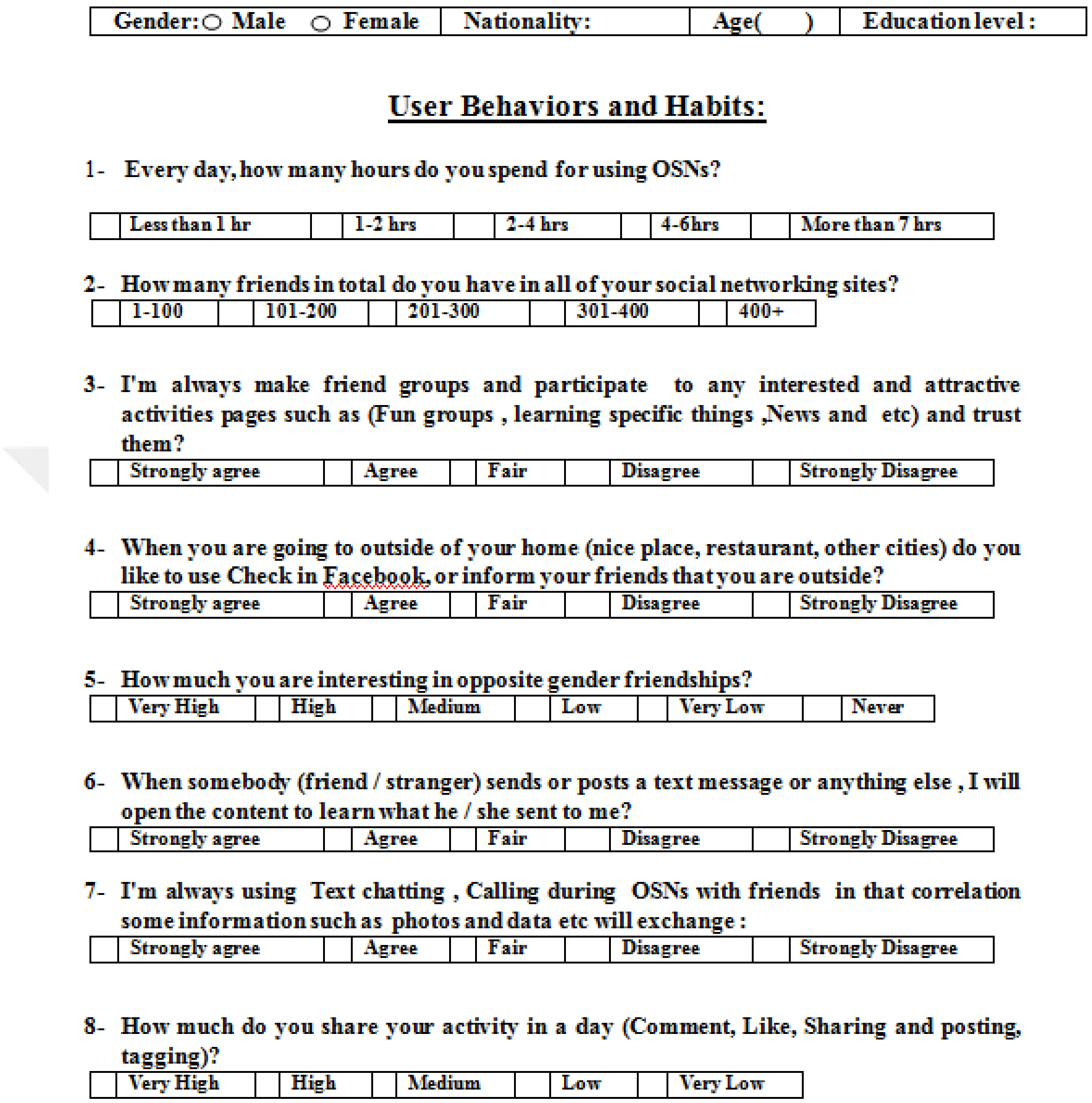
ZHANG, L. & ZHANG, W. An Information Extraction Attack against On-Line Social Networks. Social Informatics (SocialInformatics), 2012 International Conference on, 2012. IEEE, 49-55.

APPENDICES

Appendix A

#	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18
Q1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Q2	0	0	0	0	1	0	1	0	0	1	0	1	1	0	0	0	0	0
Q3	0	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	1	0
Q4	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
Q5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1
Q6	1	1	1	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0
Q7	0	0	1	0	0	1	0	1	0	0	0	1	1	0	0	1	1	1
Q8	0	0	1	0	0	1	1	0	0	1	1	1	1	0	1	0	1	0
Q9	0	0	0	0	1	0	0	0	0	1	1	1	1	0	1	1	1	1
Q10	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0
Q11	1	0	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0
Q12	1	0	1	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0
Q13	1	0	1	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
Q14	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	0	0	0
Q15	1	1	1	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0
Q16	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Q17	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0
Q18	1	1	1	1	0	1	0	0	1	0	1	1	0	1	0	0	0	0
Q19	0	0	0	0	1	0	1	0	1	1	0	1	1	0	0	0	1	0
Q20	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0
Q21	0	0	0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1
Q22	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	1	1
Q23	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0
Q24	0	0	0	0	1	0	0	1	0	0	0	1	1	0	0	0	0	0
Q25	0	0	0	0	1	0	0	1	0	0	0	1	1	0	0	0	0	0
Q26	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
Q27	0	0	0	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0
Q28	0	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0
Q29	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0
Q30	0	0	0	0	1	0	1	1	0	`	1	1	1	0	0	1	1	1

Appendix B



Gender:○ Male ○ Female	Nationality:	Age( )	Education level :

User Behaviors and Habits:

1- Every day, how many hours do you spend for using OSNs?

□ Less than 1 hr □ 1-2 hrs □ 2-4 hrs □ 4-6hrs □ More than 7 hrs

2- How many friends in total do you have in all of your social networking sites?

□ 1-100 □ 101-200 □ 201-300 □ 301-400 □ 400+

3- I'm always make friend groups and participate to any interested and attractive activities pages such as (Fun groups , learning specific things ,News and etc) and trust them?

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

4- When you are going to outside of your home (nice place, restaurant, other cities) do you like to use Check in Facebook, or inform your friends that you are outside?

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

5- How much you are interesting in opposite gender friendships?

□ Very High □ High □ Medium □ Low □ Very Low □ Never

6- When somebody (friend / stranger) sends or posts a text message or anything else , I will open the content to learn what he / she sent to me?

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

7- I'm always using Text chatting , Calling during OSNs with friends in that correlation some information such as photos and data etc will exchange :

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

8- How much do you share your activity in a day (Comment, Like, Sharing and posting, tagging)?

□ Very High □ High □ Medium □ Low □ Very Low

Security & Awareness

1. Parents should be aware about kid's activities on OSN.

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

2. It's normal to clicking an attractive and interesting link such as (New fashion, new Technology etc.), opening video or Image even if requested Double re-login on OSN.

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

3. For attractive and interesting applications, I will download; install and update whatever software I need.

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

4. I read policy of OSNs Applications (Apps).

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

5. Accepting privacy terms of Apps probably can gives permission to access privacy information (book address and photos).

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

6. It is normal to share your user name and password with best friends and I trust them?

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

7. I check Security and Privacy part in the browser setting.

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

8. I'm aware of the risks about behavioral advertising term:

	Strongly agree		Agree		Fair		Disagree		Strongly Disagree

9. How often do you delete cookie and internet files from your browser and PC?

	Never		Ones a week		2-3 times a week		Ones a month		2-3 times a month

10. Do you use any protector and security tools?

	Yes		No

Privacy:

1. Privacy policy should be considered when personal information disclosed to any website

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

2. Do you use the same email address and privacy information for all OSNs & internet accounts?

□ Always □ Often □ Sometimes □ Seldom □ Never

3. Do you modify or change your privacy setting (User name, password, and secure questions)?

□ Always □ Often □ Sometimes □ Seldom □ Never

4. To what degree you can control your sharing information with other OSN users?

□ Can't at all □ A little □ Moderate □ A lot □ Highly

5. It is normal to give your friend's information to other friends?

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

6. How much do you familiar with tagging process?

□ Very High □ High □ Medium □ Low □ Very Low

7. How much do you often use tagging with your friends or your friends tagging you?

□ Always □ Often □ Sometimes □ Seldom □ Never

8. When I'm Online , I'm aware that my browsing information may be collected by third party for advertising purpose

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

9. I'm comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information:

□ Strongly agree □ Agree □ Fair □ Disagree □ Strongly Disagree

10. Does your existing Follow Bottom is active for the strangers and friend of friends?

□ Yes □ No

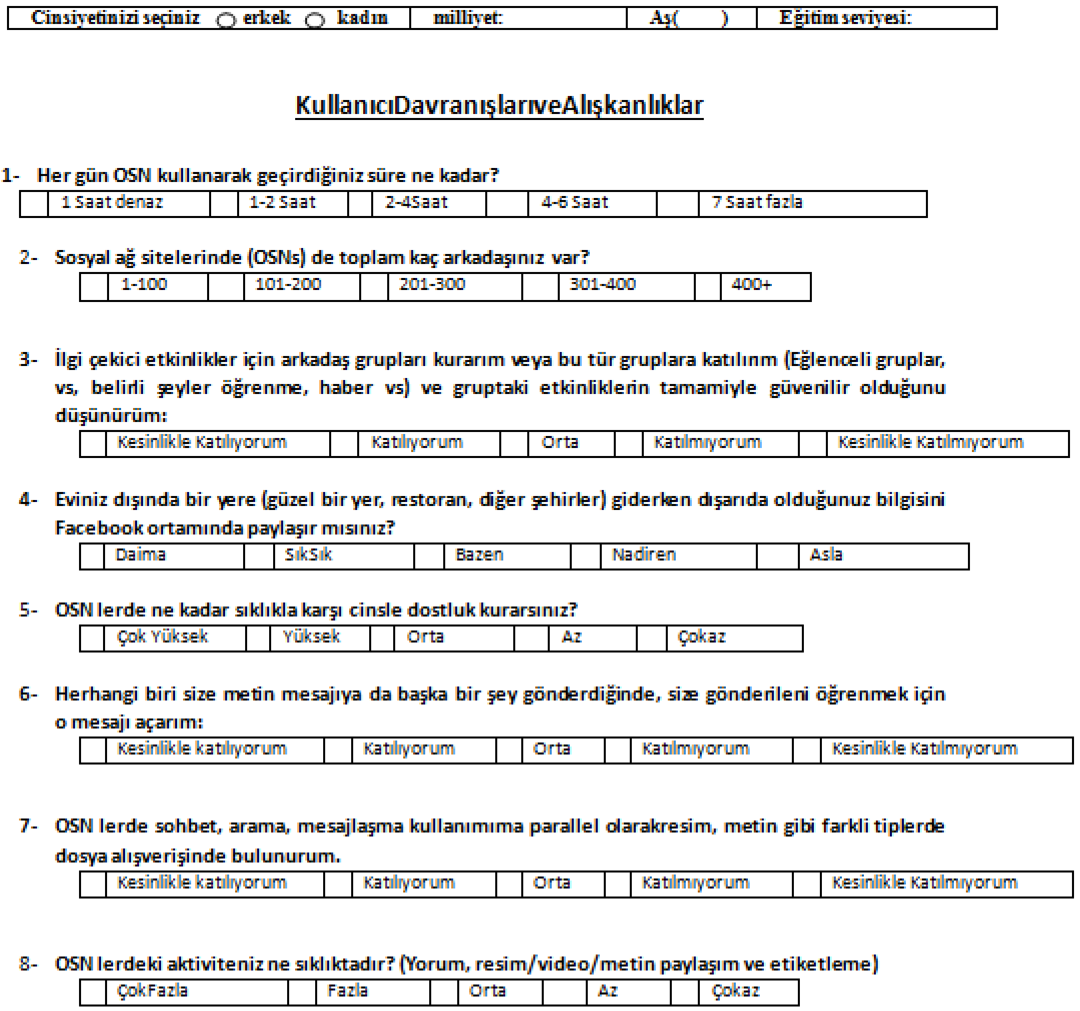
Content of user profile:

1. What do you use as your user name on your social network account?

Full Name	First Name Only	Last Name only	Nickname / Pseudonym	Fake / made-up name

2. Do you customize your profile contents including your photo or something else to avoid from watching all friends?

□ Always □ Often □ Sometimes □ Seldom □ Never



Cinsiyetinizi seçiniz ○ erkek ○ kadın	milliyet:	Aş( )	Eğitim seviyesi:

KullanıcıDavranışlarıveAlışkanlıklar

1- Her gün OSN kullanarak geçirdiğiniz süre ne kadar?

□	1 Saat denaz	□	1-2 Saat	□	2-4Saat	□	4-6 Saat	□	7 Saat fazla

2- Sosyal ağ sitelerinde (OSNs) de toplam kaç arkadaşınız var?

□	1-100	□	101-200	□	201-300	□	301-400	□	400+

3- İlgi çekici etkinlikler için arkadaş grupları kurarım veya bu tür gruplara katılırım (Eğlenceli gruplar, vs, belirli şeyler öğrenme, haber vs) ve gruptaki etkinliklerin tamamiyle güvenilir olduğunu düşünürüm:

□	Kesinlikle Katılıyorum	□	Katılıyorum	□	Orta	□	Katılmıyorum	□	Kesinlikle Katılmıyorum

4- Eviniz dışında bir yere (güzel bir yer, restoran, diğer şehirler) giderken dışarıda olduğunuz bilgisini Facebook ortamında paylaşır mısınız?

□	Daima	□	SıkSık	□	Bazen	□	Nadiren	□	Asla

5- OSN lerde ne kadar sıklıkla karşı cinsle dostluk kurarsınız?

□	Çok Yüksek	□	Yüksek	□	Orta	□	Az	□	Çokaz

6- Herhangi biri size metin mesajıya da başka bir şey gönderdiğinde, size gönderileni öğrenmek için o mesajı açarım:

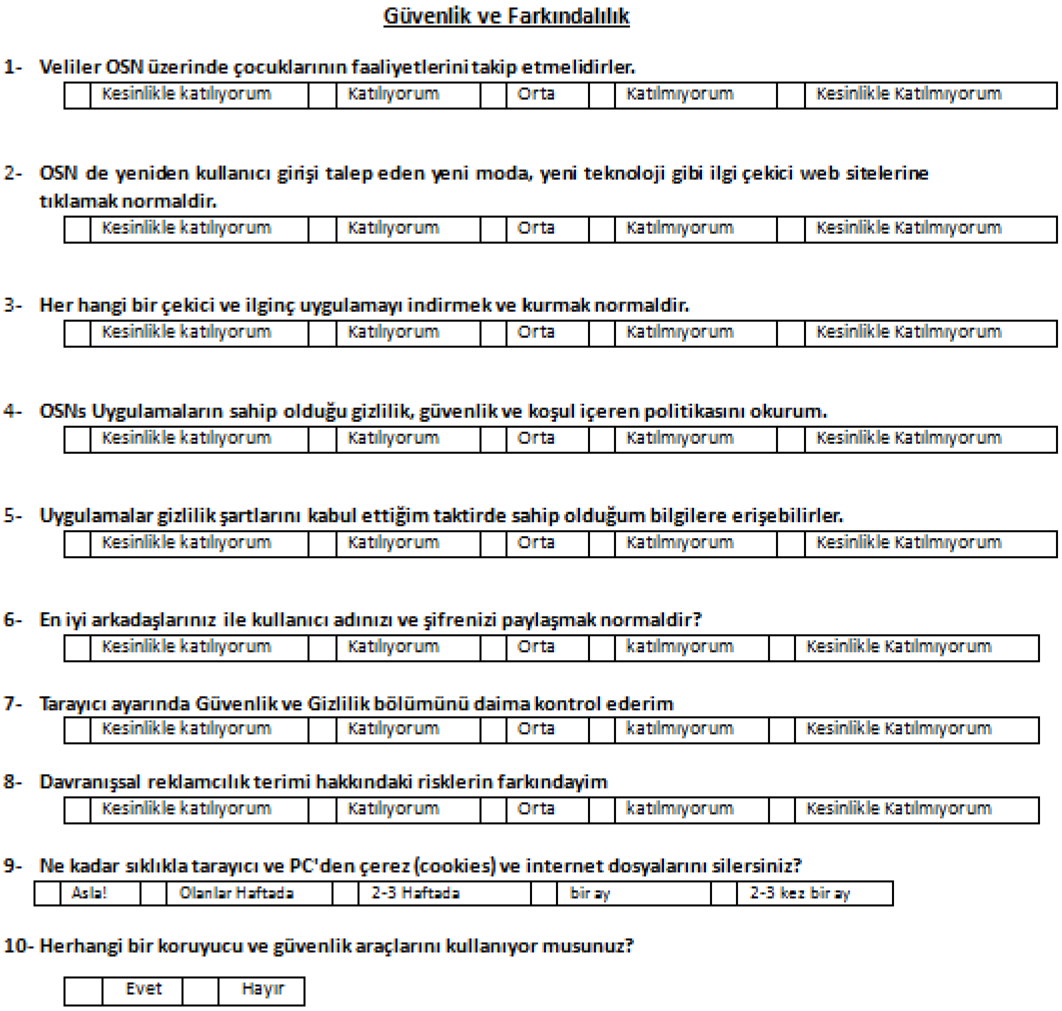
□	Kesinlikle katılıyorum	□	Katılıyorum	□	Orta	□	Katılmıyorum	□	Kesinlikle Katılmıyorum

7- OSN lerde sohbet, arama, mesajlaşma kullanımıma parallel olarakresim, metin gibi farkli tiplerde dosya alışverişinde bulunurum.

□	Kesinlikle katılıyorum	□	Katılıyorum	□	Orta	□	Katılmıyorum	□	Kesinlikle Katılmıyorum

8- OSN lerdeki aktiviteniz ne sıklıktadır? (Yorum, resim/video/metin paylaşım ve etiketleme)

□	ÇokFazla	□	Fazla	□	Orta	□	Az	□	Çokaz



Güvenlik ve Farkındalılık

1- Veliler OSN üzerinde çocuklarının faaliyetlerini takip etmelidirler.

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ Katılmıyorum □ Kesinlikle Katılmıyorum

2- OSN de yeniden kullanıcı girişi talep eden yeni moda, yeni teknoloji gibi ilgi çekici web sitelerine tıklamak normaldir.

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ Katılmıyorum □ Kesinlikle Katılmıyorum

3- Her hangi bir çekici ve ilginç uygulamayı indirmek ve kurmak normaldir.

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ Katılmıyorum □ Kesinlikle Katılmıyorum

4- OSNs Uygulamaların sahip olduğu gizlilik, güvenlik ve koşul içeren politikasını okurum.

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ Katılmıyorum □ Kesinlikle Katılmıyorum

5- Uygulamalar gizlilik şartlarını kabul ettiğim taktirde sahip olduğum bilgilere erişebilirler.

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ Katılmıyorum □ Kesinlikle Katılmıyorum

6- En iyi arkadaşlarınız ile kullanıcı adınızı ve şifrenizi paylaşmak normaldir?

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ katılmıyorum □ Kesinlikle Katılmıyorum

7- Tarayıcı ayarında Güvenlik ve Gizlilik bölümünü daima kontrol ederim

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ katılmıyorum □ Kesinlikle Katılmıyorum

8- Davranışsal reklamcılık terimi hakkındaki risklerin farkındayim

□ Kesinlikle katılıyorum □ Katılıyorum □ Orta □ katılmıyorum □ Kesinlikle Katılmıyorum

9- Ne kadar sıklıkla tarayıcı ve PC'den çerez (cookies) ve internet dosyalarını silersiniz?

□ Asla! □ Olanlar Haftada □ 2-3 Haftada □ bir ay □ 2-3 kez bir ay

10- Herhangi bir koruyucu ve güvenlik araçlarını kullanıyor musunuz?

□ Evet □ Hayır

Gizlilik:

1- Kişisel bilgilerimin herhangi bir web sitesinde kontrolüm dışında paylaşılmasını sağlayan Gizlilik Politikası gözden geçirilmelidir?

□ Kesinlikle katılıyorum □ Katılıyorum □ orta □ katılmıyorum □ Kesinlikle Katılmıyorum

2- Tüm OSNs ve internet hesapları için aynı e-posta adresini ve gizlilik bilgilerini mi kullanıyorsunuz?

□ Daima □ sıksık □ Bazen □ Nadiren □ Hiçbir zaman

3- Gizlilik ayarlarınızı ne sıklıkta değiştirirsiniz (Kullanıcı adı, şifre ve güvenli soruları)?

□ Daima □ SıkSık □ Bazen □ Nadiren □ Hiçbir zaman

4- Diğer OSN kullanıcıları ile paylaştığınız bilgileri ne derece kontrol edebiliyorsunuz? (Güvenli olmadığını düşünerek)?

□ Hiçbir şekilde □ Biraz □ Ortad erecede □ İyi □ Çok iyi

5- Bir arkadaşınızın bilgilerini diğer arkadaşlarınıza vermek normaldir.

□ Kesinlikle katılıyorum □ Katılıyorum □ orta □ katılmıyorum □ Kesinlikle Katılmıyorum

6- Etiketleme fonksiyonundan kadar haberdarsınız?

□ Çok Yüksek □ Yüksek □ Orta □ düşük □ Çok Düşük □ Asla!

7- Etiketleme fonksiyonunu ne kadar sıklıkta kullanırsınız (Başkasını etiketleme ya da diğerleri tarafından etiketlenme?)

□ Daima □ Sıksık □ Bazen □ Nadiren □ Hiçbir zaman

8- OSNlerde bazı uygulamaları kurduğum veya kabul ettiğimde üçüncü parti kişiler tarafından bilgilerime erişilip, reklam amaçlı olarak kullanılabileceğinin farkındayım:

□ Kesinlikle katılıyorum □ Katılıyorum □ orta □ katılmıyorum □ Kesinlikle Katılmıyorum

9- Kişisel bilgilerim kullanılmadığı sürece reklam sunmak için tarama geçmişimin kullanılması beni rahatsız etmez.

□ Kesinlikle katılıyorum □ Katılıyorum □ orta □ katılmıyorum □ Kesinlikle Katılmıyorum

10- Takip et (Follow) butonunuz arkadaşınız olmayanlar ve arkadaşlarınızın arkadaşları için aktif midir?

□ Evet □ Hayır

Kullanıcı Profilinin İçeriği:

1. Sosyal ağ hesabınızdaki kullanıcı adınız nedir?

Ad - Soyad	Sadece Ad	rumuz / takma ad	sahte / sahteisim	soyadı

2. Arkadaşlarınızın tamamının görmesini engellemek amacıyla fotoğraf ya da benzer şeyleri içeren profil içeriklerini özelleştiyor musunuz?

□ Daima □ Sık sık □ Bazen □ Nadiren □ Asla

ڕەگەزت چیە ؟ (نێر) - مێ	نەتەوایەتی ( )	تەمەن : ( ) ساڵ	ئاستی خوێندن ( )

(خوو و ڕەوشتی بەکارهێنەر)

1- هەموو ڕۆژێک , چەند کاتژێر بە سەر دەبەیت لە بەکارهێنانی تۆڕە کۆمەڵایەتیەکان (OSNs)؟

کەمتر لە (١) کاتژێر		(١ – ٣) کاتژێر		(٤ – ٧) کاتژێر		زیاتر لە (٧) کاتژێر	

2- کۆی گشتی برادەرەکانت (هاوڕێکانت) چەندە لە گشت تۆڕە کۆمەڵایەتیەکان؟

(١ - 100)		(101 - 200)		(201 - 300)		(301 - 400)		زیاتر لە (400)	

3- من هەمیشە گروپی برادەران دروست دەکەم و بەشداری هەر پەیجی(Page) و گروپی تر دەکەم کە خۆش و چالاکیە سەرنج ڕاکێشەکان وەک (گروپی گاڵتەو سەیروسەمەرە و ڤیدیۆی شتی نیارکراو و دەنگوباس و ... هتد) تیدایێت وە باوەڕیان پێ دەکەم

بەتوندی ڕازیم		ڕازیم		مامناوەندی		ڕازی نیم		بەتوندی ڕازی نیم	

4- کاتێ تۆ دەچیتە دەرەوەی ماڵەکەت (گەشت , چێشتخانە , شارێکی تر) ئایا حەز دەکەی چێک ئین (Check In)بکەی لە تۆڕە کۆمەڵایەتیەکان(Facebook) یان بە برادەرەکانت دەڵێی کە تۆ لە دەرەوەی ماڵەکەتی

هەمیشە		زۆر جار		جار بە جار		کەم جار		هەرگیز نەخێر	

5- تۆ چەند حەز دەکەیت لەگەڵ ڕەگەزی هاوتێ برادەریەتی بیەستیت؟

گەلێک زۆر		زۆر		مامناوەندی		کەم		زۆر کەم		هەرگیز نەخێر	

6- کاتێ کەسانێک (هاوڕێ / ناناسیار) نامەیەکی نووسراوم بۆ دەنێرن یا هەر شتێکی تر , یەکسەر نامەیەکە سە یر دەکەی و دەیکەمەوە و ناوەڕۆکەکەی دەخوێنیمەوە بۆ ئەوەی بزانم چی بۆ ناردووی؟

بەتوندی ڕازیم		ڕازیم		مامناوەندی		ڕازی نیم		بەتوندی ڕازی نیم	

7- من هەمیشە لەگەڵ برادەران قسە بە نامەی نووسراو دەکەم وە تەلەفۆنیش دەکەم لە ڕێگای (تۆڕە کۆمەڵایەتیەکان) دەکەم و بەم شێوەیەش هەندێک وێنە و زانیاری ... هتد دەگۆڕینەوە:

بەتوندی ڕازیم		ڕازیم		مامناوەندی		ڕازی نیم		بەتوندی ڕازی نیم	

8- لە ڕۆژێکدا چەند بەشداری چالاکیەکانت دەکەیت ؟ وەک (Comment, Like, Sharing and posting, tagging)

گەلێک زۆر		زۆر		مامناوەندی		کەم		زۆر کەم		هەرگیز نەخێر	

(Security & Awareness)

1 . دایک و باوکان پێویستە ئاگادار بن سەبارەت بە چالاکیەکان و هەلسوکەوتی منالەکانیان لە سەر تۆڕە کۆمەڵایەتیەکان .

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

2 . ئاساییە کلیک لە سەر شتێکی خۆش و لینک و (بابەتی) سەرنج ڕاکێش بکەی بۆ نمونە (شتی تازە و جوان وە تەکنەلۆژیا ..
هتد , یان کرنەوەی ڤیدۆ و وێنە) تەنانەت ئەگەر دووجار داوای چوونە داخیل بوون بکات لە سەر تۆڕەکۆمەڵایەتیەکان .

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

3. بۆ (Apps) و بەرنامەی خۆش و سەرنج ڕاکێش من هەر چیەکم پێ بوێت داون لۆدی دەکەم و دایدەبەزێنم بۆ نمونە
"یاری ".

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

4. من ڕێنماییەکانی بەرنامە و (Apps) لە سەر تۆڕە کۆمەڵایەتیەکان دەخوێنمەوە :

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

5. ڕازی بوون لە سەر ڕێنمایە تایبەتەکانی بەرنامە و (Apps) کە لەوانەیە ڕێگات پێ بدات بۆ چونە ناو زانیاری تایبەتەکن
وەک ناونیشانی و تۆماری ناوەکانت و وێنە .

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

6. ئاساییە کەوا Username و Password ئالوگۆر بکەیت لەگەڵ برادەراتی نزیک کەوا متمانەت پێیان هە یە .

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

7. من بەشی Privacy و Security بەسەر دەکەمەوە لە Browser Setting .

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

8. من ئاگادارم سەبارەت بە مەترسیەکانی تایبەت بە هەلسوکەوتی ڕێکلامدانەران و ڕیکلام و خەسلەتەکانیان .

بەتوندی ڕازیم		ڕازیم		مامناوەندی ڕازیم		ڕازی نیم		بەتوندی ڕازی نیم	

9. تۆ هەموو جار چۆن فایلی ئینتەرنێت و ڤایرۆس (Cookie) لە سەر (Browser) و لاپتۆپ و موبایل دەسڕیەوە .

٢ - ٣ جار لە مانگێک		یەک جار لە مانگێک		٢ – ٣ جار لە هەفتەیەک		هەفتەی یەک جار		هیچ جار	

10. ئایا قەت ڕێگایەکی پاراستن و شێوازێکی Security بەکار هێناوە ؟(Antivirus)

نەخێر		بەڵێ	

(تایبەتمەندی خصوصية Privacy)

1 . سیاسەتی و ڕێنماییەکانی خصوصیة پێویستە بە هەند (گرینگ) وەربگیرێت کاتێک زانیاری کەسی دەخرێتە ناو هەر Website ؟

بە توندی ڕازیم		ڕازیم		مام ناوەندی ڕازیم		ڕازی نیم		بە توندی ڕازی نیم	

2 . ئایا هەمان Email و Password زانیاری بەکار دەهێنی بۆ داخیل بونە ناو هەموو تۆڕەکۆمەڵایەتیەکان و ئینتەرنێت ؟

هەرگیز		کەم جار		جار بە جار		زۆر جار		هەموو جارێک	

3 . ئایا تۆ دەستکاری یاخودگۆڕانکاری لە خصوصیة (Privacy)خۆت دەکەی (User name, password, and secure questions)?

هیچ جار		کەم جار		جار بە جار		زۆر جار		هەموو جارێک	

4 . تا چ ڕادەیەک دەتوانی کۆنترۆڵی ئەو زانیاریانە بکەیت کە بڵاویان دەکەیەوە لەگەڵ کەسانی تر لە ناو تۆڕە کۆمەڵایەتیەکان

گەلێ زۆر		زۆر		مام ناوەندی		کەم		هیچ ناتوانم	

5 . ئاساییە زانیاری برادەرێکت بدەی بە برادەرانی ترت لە ناو تۆڕە کۆمەڵایەتیەکان :

بە توندی ڕازیم		ڕازیم		مام ناوەندی ڕازیم		ڕازی نیم		بە توندی ڕازی نیم	

6 . چەند شارەزاییت هەیە لەگەڵ (Tag) کردن بۆ نمونە وێنەی خۆت و هاوڕێیەکت Tagدەکەی لەگەڵ یەک

هیچ		زۆر کەم		کەم		مام ناوەندی		زۆر		گەلێک زۆر	

7 . تۆ چەند Tagging دەکەیت لەگەڵ برادەرەکانت یان ئەوان لەگەڵ تۆ ؟

هیچ جار		کەم جار		جار بە جار		زۆر جار		هەموو جارێک	

8 . کاتێ من لە سەر خەتم , من ئاگادارم کەوا زانیاریەکانم لەوانەیەبلاو بکرێتەوە لەلایەن کەسانی تر بۆ ئامانجی ڕاگەیاندن و ریکلامکردن کۆبکرێتەوە .

بە توندی ڕازیم		ڕازیم		مام ناوەندی ڕازیم		ڕازی نیم		بە توندی ڕازی نیم	

9 . من ئاسوودەم بەو ڕاگەیندنانە و ریکلامکردنانەی کەوا ناوەرۆکی زانیاریە کۆنەکانی من بەکار دەهێنن بۆ خزمەت و سوودی من مادام ئەو زانیاریانە نەبەستراوە بە ناوی من یا هەر زانیاریەکی پەیوەندار بە کەسایەتیم .

بە توندی ڕازیم		ڕازیم		مام ناوەندی ڕازیم		ڕازی نیم		بە توندی ڕازی نیم	

10 . ئایا (Follow Bottom)ی تۆ کراوەیە بۆ کەسانی نەناسیاو یان برادەری برادەران ؟

نەخێر		بەڵێ	

(ناوەرۆكی پرۆفایلی بەكارهێنەر)

1 . چی بەکار دەهێنیت وەک ناوی بەکارهێنەرت لە ناو تۆڕەکۆمەڵایەتیەکان ؟

ناوی کوتا	ناوێکی خوازراو	سەرناو (لەقەب)	تەنها ناوی یەکەم	ناوی تەواو

2 . ئایا ناوەرۆکەکانی پرۆفایلت بە وێنەت شتی تریشەوە وا ڕێک دەخەیت بە جۆرێک کە هەموو برادەرەکانت نەیبینن

هیچ جار		کەم جار		جار بە جار		زۆر جار		هەموو جارێک	