Counter Cyber terrorism using Online Radicalization detection and Unified Cyber Trust Model (UCTM) on surface and Dark Web

A THESIS

SUBMITTED TO THE COUNCIL OF

COMPUTER DEPARTMENT/ COLLEGE OF SCIENCE AT THE

UNIVERSITY OF SULAIMANI

IN PARTIL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

OF DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

(CYBER SECURITY)

By

Ala Omer Ahmed

Supervised by

Dr. Nzar A.Ali

Assistant Professor

September 2019 Xermanan 2719

To all who are closest to my soul…

Acknowledgments

I am wholeheartily thankful to my supervisor Dr. Nzar A. Ali whose support and help enabled me to undertake and successfully complete this thesis . His supervision has been truly valuable for me. I would also express my sincere gratitude to my both supervisors at Stockholm University Prof. Oliver Popov and Dr. Esmiralda Moradian, I learnt a great deal from them. I am extremely grateful to former president of Sulaimani Dr. Salahadin Saed Ali and current president of University of Sulaimani Dr. Raza Hussein as with their encouragement, help and support I was able to achieve this success.

I would express my thanks to head of Computer Science department Dr. Mustafa Khalil for his support. I would also express my thanks to all my friends, especially Dr. Ibtisam Ismael, the Dean of Collage of Social Sciences whose has always been there for me and Dr. Karzan Ghafur, director of International Academic Relations. I am grateful to Amira Muhammed for her help from the first day of my studies until the last day. Her support is highly appreciated. Certainly, I want to thank my parents and my family for all the support, love, encouragement and prayers for my success in life. They were always there to help me.

The last but certainly not the least, I would like to express my deepest love and gratitude to Frzand Sherko. Without his support, this project will not have been possible. He helped me with his love and all his valuable information to achieve this goal. I would like to thank my princess Aziz for understanding my circumstances and encouraging me with her love.

Ala

Abstract

Currently internet is used across the globe for social media, emailing, searching, researching, online shopping and other purposes. Whatever people do on the internet is only a small part, the other parts are deep web and dark web. Cyber is very important for the other fields. Information security, infrastructure and environment are all related to cybersecurity. Cyber terrorism is one of the activities on internet through which ideology of individuals or society can have impact on the political decision and can even lead to damage to the society and casualties. It is also a major threat on the data and information of people and the governments. To minimize the cybersecurity threats, most countries adopted specific laws and regulations and tries to find solution for it through researchers and research centres. However, threats remain on both surface web and dark web as working on counter cyber terrorism is new and not very much have been done yet. The aim of this research project is to counter cyber terrorism on the surface web and dark web through detecting those people involved in online radicalization; and also, those individuals working for the extremist groups. In the first part of this project, a special algorithm was proposed to find and geo-locate members of the Islamic State group within the online groups, uncover their roles and duties within the group according to their behaviour; and also detect those who recently influenced by the extremist jihadi ideology in order to prevent their recruitment in to the group. In the second part of this project, the Unified Cyber Trust Model was proposed to replace the current trust on the dark web to enable detection of those people who use dark web for the purpose of cyber terrorism. A Trust Management System is also suggested to assess the trust by itself and not through the assessment of the other nodes. The results of this research project can be used to counter cyber terrorism and thus minimize extremism, terrorist and radical activities.

Table of Contents

List of Abbreviations

Abbreviation	**Description**
UTM	Unified Trust Model
API	Application Programming Interface
B2C	Business to consumer
TOR	The Onion Router
UCTM	Unified Cyber Trust Model
TMS	Trust Management System
CCTV	Closed-circuit television
SHA	Secure Hash Algorithm
DES	Data Encryption Standard
RSA	Rivest-shamir-Adleman
SSL	Secure Sockets layer
IE	Information Extraction
IR	Information Retrieval
NLP	Natural Language Processing
IS	Islamic State
DOD	Department of Defense
URL	Uniform Resource Locator
IP	Internet Provider
OS	Operating System
XSS	Cross-site scripting
SQL	Structured Query Language
OWASP	Open Web Application Security Project
SIOT	Social Internet of Things
ICAO PKD	The International Civil Aviation Organization – Public Key Directory
CSCA	Country Signing Certification Authority
CRL	Certificate Revocation List
DS	Document Signer
CA	Certificate Authority

IC	Integrated Chip
eIDAS	Electronic Identification, Authentication and Trust Services
IDP	Identity Provider
eIDs	Electronic Identifications
FICAM	Federal Identity, Credential, and Access Management
G2G	Government to Government
G2B	Government to Business
G2C	Government to Citizens
MANET	Mobile Ad-hoc Networks
P2P	Peer to Peer

List of figures

List of Algorithms

Chapter 1

Genereal Introduction

1.1 Overview

People around the world use the Internet every day for social media, email, research, shopping, and many other things. Whatever people do on Internet is just a small piece and the rest is deep web. The furthest corner of the deep web, known as the dark web [1]. A lot of activities in different fields are done through the Internet. Cyber power is essential in every field and to support any other activities. Conversely, cyber superiority operations should be directed at neutralizing enemy cyber-attacks and reconnaissance capabilities, before repressing their cyber defences. Cyberspace superiority and cyber interdiction often result in powerful decision-making benefits during warfare that generally force an enemy to make fatal mistakes [2]. Security of information and minimizing dangers in digital environment depends on security of cyberspace.

Information Security is about confidentiality, integrity and availability of the data. It starts by determining assets and protecting them against the threats. Cyber security is the process of defending cyber space, which can be defined as a global network infrastructure linking uniquely identified physical and virtual objects, things and devices through the intelligent objects, communication and actuation capabilities digital environment from cybercriminal and cyberterrorism attacks and securing it [3][4].

As with any other new technology, while there are numerous positive and lasting affects on the society in general, there are also negative implications and consequences with usin the. This is usually manifested through unacceptable deeds, both socially and often legally such as propagating hate speech, child pornography, sale of controlled substances, advocating violence, inducing criminal behaviour, excitement, and recruitment for extremists and even terrorist actions and organization [5].

Cyberterrorism is the use of the internet to create widespread fear, loss of lives through significant body injury for political and ideological reasons. Internet terrorism involves activities such as deliberate acts that can cause considerable scale disruption of computer networks, in the case of personal computers through the use of malicious tools that include computer worms, computer viruses, phishing, and other malicious software and hardware methods [6].

Cyberterrorism has also psychological affects on humans through online radicalization and propaganda. On surface web, networked social media has become an omnipresent collection of various tools for social networking and content sharing. Initially, it has been used and still is for building and fostering social interactions, mixed with simple entertainment practices, generation of alerts in case of natural and human induced disasters, identifying ways for crowd funding innovative services and products (mainly in the non-kinetic world), and expressing and disseminating political ideas and agendas for societal change.

In order to reduce and eventually eliminate instances of radicalism and extremism, Law Enforcement Agencies need to continuously monitor the cyber space. As the number of security and forensic tools for monitoring and analysis of the activities have somewhat increased recently, many are still shortage in provision of counter measures to identify, remedy and eliminate cyberterrorism [7].

Terrorist organizations taking over the cyberspace are equipped with the most characterized modern warfare tools. Such organizations no longer only rely on military might and the use of bombs and weapons, but they are instead shifting focus to more savvier tactics and technological approaches. Their approaches tend towards activities that include propaganda, online radicalization, planning, fundraising and execution of physical attacks. Their online presence also extends to sabotaging online infrastructure and causing harm to their victims through the use of the dark web to mask their identities.

The users who have experience using the dark web know that keeping the privacy of users is essential Thus, trust is vital in dark web and digital trust to make users comfortable with using it is essentiall because authentication in the dark web does not exit. The communication among the users depend on trust. Trust in the dark web is selected based on the reputation of the group who has a good history of buying and selling goods, the group or the web pages who have a good reputation is more trusted [8]. In the dark web, the critical key for electing groups or service is based on the status of the group or the service provider.

It is not easy to see what trust exactly is, but we can learn what it is from different perspectives. The definition of trust is a combination of trust explanation in all the fields, where trust is the degree of belief that an entity will complete the expected tasks in the best, safest, less time, high quality and efficient way. Trust models can be employed to ensure trust in a digital environment and it is increasing trust in the cyberspace.

It is tough for an individual to identify the origin of the data or the location of the user. To increase reliability and trust, the scientists try to use Unified Trust Model (UTM), which is using more than one trust model to evaluate trustworthy of the service. However, the UTM is only used for assessing digital goods. Consequently, a unified trust model is a preferable way to evaluate function and measure trust. A UTM can be used to improve privacy, trust, security, speed, accuracy, anonymity and realability. This will help countering cyberterrorism on dark web.

1.2 The Related works

Increasing concerns on radicalization and recruitment to terrorist organizations through the internet is indicative of the growing presence of terrorist organizations in the cyberspace,for example, the increasing usage of social sites such as Twitter, Facebook, and YouTube by terrorist organizations to spread their ideologies and recruit new members. Social networks have become one of the most critical tools for violent extremist groups to spread their online radicalized ideologies. This increasing presence prompted the development of tools and algorithms that can identify key players, their connections, subgroups, involved nodes and flag them off as terror groups. The most advanced algorithms and tools at the moment on online radicalization are known to focus on static network structures while ignoring the origins of the extremist ideology.

Tayebi et al. 2011, [10] presented a systematic framework for detecting and analysing criminal systems as a concept idea to develop other advanced computational methods of identifying organized crime structures and networks involved. Most of the techniques suggest employing probabilities by analysing past behaviours of the users. The author designed algorithms for learning and testing the model parameters that can make predictions and as well predict the time by which the user is expected to act.

Brynielsson et al. 2012, [11] design an analysis method which can be used to analyse weak digital traces and footprints in extremist forums to trace possible lone wolf terrorists. In another research to counter online radicalization Jingxuan and colleagues 2013 [12] developed a dynamic information diffusion model based using Markov's Continuous time process concepts that can be used to predict dynamics of social network users using assumptions derived from the activation of a particular node.

In another research Cassel et al. 2014, [13], suggest that the classification of a group of users with similar patterns based on their node activities should be implemented. At one-point, researchers make a first attempt to develop an application that can automatically detect messages released by jihadists on Twitter and classify a tweet containing information supporting extremist views using machine learning techniques.

Wadhwa and Bhatia 2015, [9] suggest the mathematical modelling that involves the use of discrete time Markov Chains that discretized continuous time, is recommended for recording the proliferation of radicalization in online social networks. The model suggested in this report is modular and can be used for modelling the diffusion of radical ideas on social network platforms. During the research,the data was collected using Digg Application Programming Interface (API) and the network was treated as a static entity during the analysis.

Kaati et al. 2016, [14], develop systems that can capture psychological warning behaviours in written texts utilizing a machine learning approach in an attempt to identify lone terrorists using written communication.

When it comes to UTM, which is another part of this research, it is necessary to review digital trust models and UTM, in previous literature, a recommendation based trust model has proposed a mechanism to filter out unnecessary and misbehaving nodes while searching for a packet delivery route. However, building a trust model that adopts recommendations by other nodes in the network is a challenging problem due to the risk of dishonest recommendations like bad-mouthing, ballot-stuffing, and conspiracy.

According to Ruan et al. 2016, [15], the comparing based trust model depends on the reputation system of the nodes for predicting their future. Trust model of comparing peer-to-peer e-commerce (electronic commerce) communities commonly perceived as an environment offering both opportunities and threats. One way to minimize risks in such an open society is to use community-based reputations to help evaluating the trustworthiness and predicting the future behaviour of peers. In security trust, model each interaction between nodes and service and count on the number of malicious nodes. Wu et al. 2016, [16] mentioned that the accuracy of comparing based trust model is based on the interruption rate in the connection.

For the ranking based trust model, Ghavipor et al. 2016, [17] determined some boundary conditions for the ranking and interpret all links between nodes as affirmative votes for the web page. Again in 2016, [16] the authors mentioned that the trust model of ranking the idea of troll-trust is the idea of page ranking, which calculates the probability that a random surfer on the Web visits a given web page by traversing links outgoing from web pages in the random fashion.

Thrift et al. 2017, [18] proposed the priority-based trust model for selecting the best rating nodes. The third-party nodes will rate the quality and the performance of the nodes. Priority trust model used for service selection helps in the process of selecting the best rating and quality. The priority-based trust is robust and novel from several perspectives. (1) The reputation of a service provider is derived from referees who are third parties and had interactions with the provider in a rich context format, including attributes of the service, the priority distribution of attributes and a rating value for each attribute from a third party. (2) The concept of `Similarity' is introduced to measure the difference concerning distributions of priorities on attributes between requested service and a refereed service to precisely predict the performance of a potential provider of the requested service. (3) The concept of the general performance of a service provider on service in history is also introduced to improve the success rate on the requested service.

Tan et al. 2017, [19] confirmed that security based trust model will verify the nodes by analysis and investigation with logical evaluation including sampling and correlating measured data observed test result. Zhou et al. 2018, [20] said that trust model-based security is essential for verification software program. Verification by Analysis - The analysis verification method applies to confirmation by the investigation, mathematical calculations, logical evaluation, and calculations using classical textbook methods or accepted general use computational methods.

The analysis includes sampling and correlating measured data and observed test results with calculated expected values to establish conformance with requirements.

According to Vamsi et al. 2018, [21] the simplicity based trust model works on the probability of the positive outcomes of the nodes. Simplicity trust model certainty a possibility that the probability of a positive outcome lies in between the nodes. In the trust model based on the quality of the node, the simplicity, reputation, trustworthiness, and risk compose the vital computable factors supporting for trust decisions.

Shaikh et al. and Manuel et al. 2015, [22] [23] agree on that a trust model based on quality of service in cloud computing environment trust model between users and cloud providers establishing trust in three turns and when cloud users are satisfied at first two turns then at third turn they can rely on cloud provider.

In speed based trust model, Filali et al. 2015, [24] used time series model for speed flexibility to measure and gauge the improvement of the nodes and completeness of the tasks in specific time. Speed test when trust goes up, speed goes up, and cost goes down, a rate of the model is one of the critical parts should be aware of design it. According to the authors in this model, they could use a time-series model for speed flexibility to measure and gauge the improvement in a system.

Regarding the UTM, in previous literature working on the unified trust, the model is available on the side of the model that written to know about the ability of the model and the limitation of the model. In automated trust negotiation, which it is an approach to establishing trust between strangers through iterative disclosure of digital credentials and access control policies play a crucial role in protecting resources from unauthorized access. Kirrane et al. 2017, [25] in a study of Business to Consumer (B2C) e-commerce have used intention theory to understand the role of trust in Internet transactions, the limitation of this model did not contain critical relational concepts. The limitation of this model access control policy for a resource is usually unknown to the party requesting access to the support when trust negotiation starts.

Although, Fan et al. 2014, [26] demonstrated the security infrastructure uses integrated circuits (TEIs) that generate a unique set of output values in response to receiving a given set of input seed values. In pervasive systems, it is possible to collect user information invisible, unobtrusively by known and even unknown parties. A considerable number of interactions between users and ubiquitous devices necessitate a comprehensive trust model, which unifies different trust factors like context, recommendation, and history to calculate the trust level of each party precisely. Trusted computing enables effective solutions to verify the trustworthiness of computing platforms.

Moreover, unified trust model is like measurement, trust and trustworthiness are critical measurements of a distributed sensing system or a heterogeneous network comprised of sources of information, knowledge, hardware, and software. m-commerce has become one of the most evolutionary fields not only in the developed countries but also in the developing countries. UTM is used both on surface web and dark web in different fields. For example, on surface web online banking is one of the customers always face difficulty in finding the desired bank. Working with money and taking care of customer money is a sensitive case and the customer should be aware in selecting the trustworthiness of the bank. According to Laura Acevedo 2011, [27], productions rely on well-organized and rapid admission to banking evidence for cash flow appraisals, auditing, and daily financial business dispensation. Online banking bids accessible, secure transactions, and 24-hour banking preferences. The business transaction depends on the right and trusted bank. Therefore, customers always look for the bank that has a good reputation. However, the bank is still the place that the hackers want to access for their economic gain.

Unified trust model consists of different trust factors that are unified together and used to calculate precisely the trust level of each party and to know the accuracy of the trust computation that is a significant issue of the environment. Khiabani et al. 2013, [28] present the case study about a unified trust model to wireless sensor networks to increase the accuracy of trust computation mechanism, and design a trust evaluation method to improve the trustworthiness of the new nodes in the online banking systems. The vulnerability of the system should be identified to evaluate which key of the solution to use and control the weakness and find out which conditions affect the trust calculation mechanism and how much the model can deal with different scenarios.

In another study Nigudge et al. 2014, [29], they combine a set of outlines that inspect the associated security belongings in losses recompense, security observing, support, and consciousness, verification and encryption mechanisms; and Internet banking submission security features. They also comprise aspects that scrutinize the related usability possessions and registration, business technique; and multi-factor confirmation approaches.

In previous literature, Nithyanand et al. 2015, [30], applied trust models in the dark web to provide anonymity for the TOR browser, including a roving adversary that can attempt to compromise a positive number of nodes. Moreover, posits that the course collection, which is essential to be sure about it because it affects trust, security, and privacy; route assortment is modelled as a three-stages which the operator first preferences a circulation over paths, and then the adversary chooses a set of nodes to attempt to compromise.

Cheroff et al.2015, [31], consider different procedures for deciding first and last hubs in the system to limit the most extreme likelihood a corresponding enemy has for connecting source to goal. The principal takes a gander at the general case, in which there is a subjective number of trust levels. A clear calculation to compute an ideal conveyance keeps running in time exponential in the span of the foe. They consider a characteristic improvement of taking a gander at conveyances on singular hubs instead of sets of hubs and finding the item appropriation as an estimation of the joint dissemination on pairs. Therefore, UTM up to this point as per the examination and study it does not exist oblivious web or the TOR program.

1.3 Goal of thesis

The aim of this study is countering cyberterrorism on both surface and dark web. Social networks used for “programming” someone into radicalism, which eventually may result into linking people (individuals) to terrorist groups and organisations. On surface web the almost daily evidence of the terrible human cost has significantly increased the interest and the research on online radicalization. Developing algorithms, tools, methods, and applications to counter online radicalization will help in cutting terrorist threats.

The first part of this study is proposing an algorithm to find, detect and geo-locate the nodes (members) of terrorism organizations among online communities on the surface web. Based on what Richard Barret [32] explains about how such groups are generally structured, the behaviours of their members, the attitude of its leaders and military and financiers. As per the time this study was conducted there is no work that has been conducted on the Islamic State in regards to finding the numbers of connections each member of the community has, finding their location, collect data on members of online communities on Facebook and text mining the posts they write to identify their leaders. The result of this study can be used to tackle violence and terrorism electronically, classify the nodes based on Islamic States structure on social networks and track the radical nodes that we believe they become pre-terrorist nodes. It will also help to identify the nodes that are in the group, but not active yet and are not involved in jihadi contents.

The second part of this study is proposing a Unified Cyber Trust Model (UCTM) to calculate trustworthiness of entities based on history, context, and platform integrity measurement, and will be applied between the available services and the users. Use, and generally operates in the cyber security field. The UCTM provides information on the services and recommends the best ones for the users. The recommendations are not subjective and neither made based on the previous user's but on the Trust Management System (TMS). Evaluation of the trust relies on the previously done connections of the UCTM for its recommendations. The UCTM has been applied on two different case studies. Firstly, on online banking system just to test the system on the surface web and secondly on the dark web which it is the key purpose of the UCTM to provide trust for the users.

In the dark web electing service is based on reputation which is not trustable as the reputation may be based on the malicious nodes rank and recommendation. As result of trust problem in dark web, this UCTM is proposed to replaces the reputation and the part that monitors the transaction. The UCTM is precise because the malicious nodes would not participate in ranking, therefore, this is the way to increase trust, privacy, performance and accuracy.

The purpose of proposing this UCTM is to find the users of the dark web that are involved in the terrorist organizations dark web’s communities such as forums to donate for terrorist organizations, asking for creating bombs, and for software that hide them from governments or hack into the governments systems. To be able to use the UCTM in the dark web and benefit from it, the entities (both users and services) has to register in the forum. For collecting the user’s information including IP address, it has to use some hidden exploit built in into the registration form by using the UCTM, it will directly save the information of the user.

1.4 Thesis organization

This thesis is divided into six parts. Following this General introductory chapter is chapter 2, presents the theories of the thesis. Chapter 3 is presenting the algorithms and discussion simplicity and complexity of the algorithm used in this study. After this, chapter 4 is the discussion and result. Chapter 5 is the conclusion and suggesting ideas for future work.

Chapter 2

Theoretical Background

2.1 Introduction

Information privacy refers to the desire of individuals to control or have some influence over data about themselves. It is multilevel concepts and it is combining of data, technology, and political, legal and public expectation of privacy [33]. Information privacy is about protecting personal information; with the advancement of digital world the personal information - is more vulnerable than before. Security plays an important role to keep the personal data protected and protecting privacy will increase trust [34].

Information security covers three very important aspects, which are confidentiality- prevention of unauthorized disclosure of information, integrity- prevention of unauthorized modification of information and availability- prevention of unauthorized withholding of information or resources [35].

Security starts by knowing what you are protecting and against whom; what is your security goals, and then thinking like enemy to ensure security for your system. Nowadays, the term cybersecurity is used in place of information security, however cybersecurity is not only protection of information security, but of all other assets as well. According to Klimburg, cybersecurity has become a matter of global interest and very important internationally [36] [6].

2.1.1 Cyber security

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

The cyberspace and underlying infrastructure of any country are generally vulnerable to a wide range of risks such as cyber threats or even physical threats and hazards. Sophisticated hackers and nation-sponsored hackers at times exploit vulnerabilities to steal information, divert funds and in extremes disrupt or destroy the essential delivery of services. Security, when concerning computing, refers to both cybersecurity and physical security, which can both be applied when it comes to unauthorized access to critical data systems. Information security primarily refers to systems that are designed to maintain confidentiality, the integrity of data and information and is a subset of cybersecurity [37].

Cyber threats can either originate from state-sponsored hackers, global cyber syndicates, hackers for hire, and terrorists ‘cyberterrorism”. Most cyber threats are aimed at seeking state secrets, technology, trade secrets or even destroying critical infrastructure and causing harm to the economy, national and international security [38].

Cybersecurity involves the techniques and technologies aimed at protecting computer systems, networks, and programs from cyber-attacks and unauthorized access [39]. Due to the prevalence in cyber-attacks that have been increasing over the years, corporate and government institutions have invested much in cybersecurity to protect their computer systems and data. It entails protecting the hardware, software programs and networks from external intrusions and attacks. Cyber-attacks aimed at bringing the computer system down through denial of service, stealing important data and selling it to competitors or use it in identity theft (in case of personal data such as credit card details and passwords), finding ransom among others. Many data breaches have occurred in recent years where websites are hacked and data were stolen. Among the targeted data are the credit card numbers and personal information that help the hackers make identity theft.

Cybersecurity has become an integral part of investing in computer systems. The internet offered businesses and a new avenue to reach their customers. By setting up websites, customers can now purchase online, order products, communicate with businesses among others. With such opportunity, cyber attackers discovered that they can leverage such systems to either steal information, bring the systems down and frustrate businesses, inject viruses, trojans, and ransomware and ask for ransom among others [39]. Businesses are loosing billions of cash through cybercrime. To date, there are many ways at which cyber attackers use to attack computer systems. The following are some of the attacks that happen over the internet:

- DDoS, distributed denial-of-service, happens when an attacker floods a system with false requests [40]. The system, network or server becomes overloaded in a way that it fails to handle the normal traffic, making genuine users unable to access the service. As for the virus, it is a malicious code which gets way to a computer and does nasty activities. It can use the CPU and cause heavy loading, slowing the computer. A virus replicates and can attach to a program or file and move to another computer.

- Phishing is a popular technique used to lure people to send confidential information. The attackers send messages and emails which look official and genuine, which prompts people to send some data. An attacker may send an email to an employee, assuming to be the executive officer, and request some login details which he can use to access information.
- Malware is programs or files that when getting into a computer, they harm it by either deleting some files, alter some or steal information. Malware is wide as it encompasses trojans, virus, spyware among others.
- Ransomware, on the other hand, is a program created to encrypt user data in a computer. The user cannot access the files and if he or she tries to do so, the ransomware demand payments for the data to be unencrypted. Even after payment, the user may or may not access the files. Spyware programs tend to copy themselves in the computer and try to record using the camera or steal information with the aim of using such information to blackmail a person if he or she does not make some payment. It is for spying as the name suggests.
- An SQL injection happens when an attacker inserts malicious code to the database server. If the application has a vulnerability, the attacker will get into the database and steal or modify the data [40].
- Man-in-the-middle is another attack where a hacker gets in the middle of a communication network between two entities. In an insecure Wi-Fi, for instance, a hacker will tend to put himself between the user and a network and get all information the user tries to communicate to the server. The user unknowingly passes any information through the hacker who can get sensitive data such as logins and use them elsewhere.

2.1.2 Levels of cybersecurity

Application security is applied when building a website or application. Referred to as secure coding, it involves identifying vulnerabilities that a website might have and fix them at the coding level. These include having working login systems that require username and passwords, one-time passwords, session management, input validation, among others. When programmers work on applications and websites, they must test them using ethical hacking to try to identify any loophole that an external and malicious attacker might use to destroy the app or steal important data.

Network security is all about securing the corporate networks from outside intrusions. Activities involved include setting up intrusion detection systems that alert the security admins in case intrusion attempts take place, antivirus, firewalls that block attacks, virtual private networks that create secure tunnels when accessing or sending important data or communicating securely among others. Corporate organizations, learning, and government institutions are the ones who heavily invest in intranet networks where their computers and servers operate. They must secure these networks from illegal access to unauthorized persons who might later hack the systems and cause a breach.

Physical security involves protecting the physical location. The computer rooms, data center, and the premises must be protected. Closed-circuit television (CCTV) cameras are installed at strategic locations so that the person in the control room can observe what is going on. Doors to all the rooms are locked using biometric and card systems, or facial recognition system which only assigned to the legitimate users. Servers are stored in racks that are locked to prevent unauthorized users from accessing or carrying them away.

End-user security entails protecting computers or workstations that people work with every day. A computer must have antivirus software, data backup for data recovery in case it is erased or manipulated by attackers, data encryption, password-protected computers, and other ways [39]. Not everyone who owns and use a personal computer understands these security techniques, leaving them vulnerable to attackers.

Corporates have been employing personnel in the security docket to ensure that corporate information systems are protected. Security personnel are responsible for monitoring and maintaining the computer systems, updating software, purchasing and installing security programs, responding to security alerts among others. Moreover, they understand the computer systems that a corporation should invest in to ensure maximum security [41]. They also train workers on handling security issues, manage passwords and prevent social engineering cases. As such, apart from managing systems, they manage people who might be vulnerable to different forms of attacks.

2.1.2 Techniques used in cyber security today

Use one-time passwords – password and usernames are stored in the database. If an attacker has access to the database and steals these login details, he or she will use them in assessing different accounts and make changes or delete information. Moreover, the attacker can steal sensitive corporate information and sell it to the competitors. However, using one-time passwords, the password is sent to the genuine account user who keys it to log in to the system. Such passwords are used only once per login and rendered useless as the system will generate another one when the user tries to login nets time [42]. Therefore, even if the attacker has the password and username, he cannot still access the account.

Hashing all data in the database – hashing data changes it from clear text to unreadable text. There are several hashing standards such as Secure Hash Algorithm (SHA) 2 and 3 which are very hard to reverse the hashed data into a clear text. SHA 3 is the latest hashing standard that generates digital signatures when used [43]. Even the attacker gets access to the database, after bypassing all the other security levels, will find data that cannot help.

Update all software – old software versions have stayed much in the market. Hackers have tested them for a longer time and have identified their vulnerabilities. Developers usually release patches on a regular basis to fix all bugs that software might have. As such, living for the latest version or making regular updates keeps all software free from exploits.

Using updated antivirus software – cyberattacks have become sophisticated and create advanced malware and ransomware each day. Internet security firms tend to learn some of the vulnerabilities that systems have and update their antivirus. Therefore, corporates and individuals should invest in the latest software to keep many of the malware away because antivirus is among the major security measures for any computer system [44].

2.2 A brief history of Islamic groups on the Internet

Islamic groups have leveraged the internet to broadcast their plans as early as their birth. The popularity of the internet increased in the 90s, as more people began using it and more information was added [45]. Likewise, only a few Islamic terrorist groups used the internet at the time. Their presence has grown steadily and as the world wide web becomes complex, it has become complex to crack their movement down. Research indicates that all groups branded by the US as a foreign terrorist organization has a website [45]. It means that they use the website to publish content related to their views, perspectives and recruit new people to their group. However, as the internet becomes the widely known network connecting billions of people and devices, terrorists have become sophisticated. They no longer use the surface web of the internet to plan attacks. They understand that the internet is tracked all the time and would be easy for security agencies to track them down and thwart their plans. Instead, they use the surface web internet purely for communication. They now take advantage of applications that assure security and data encryption such as Telegram and TrueCrypt [46]. They mobilize the group members, spread messages and even raise funds to support their activities. Apart from instant messaging applications, they also use web forums to spread the message on their plans [45].

2.2.1 Challenges of the internet

When the internet was at its infant times, very few people who had access to it. Thus, there were few people to recruit even if the Islamic groups would like. It was expensive and there were few gadgets, owned by a few households, to access it. As stated above, very few of these groups had access to the internet [45]. Moreover, the internet has less capability in terms of communication, video uploads and other fantasies that are present today, as YouTube had not been developed. When social media was established and the internet expanded to more regions, Islamic groups found a niche. They discovered that instead of searching and recruiting people traditionally, there was a perfect medium where people can virtually meet and exchange ideas. YouTube came and they could now prepare and upload videos for their members and potential members to access them. Since then, the groups have established complex networks where they exchange plans and spread messages.

Looking at the instant messaging apps that encrypt communication to promote privacy, the idea becomes a double-edged sword. Though privacy is good and should be fostered, privacy that infringes on other people's right to live, worship or any other freedom is not good privacy. Privacy that would lead to terrorizing people is not commendable privacy [46]. Apart from video and the internet, Islamic groups have learned about the dark web, a place where it is hard to find them. They have grown sophisticated in the way they handle their strategies to optimize success. The dark web has offered them a new era or dawn to fundraise. Bitcoin, the most popular cryptocurrency, favors the dark web simply because it does not need a centralized system or institution to handle its transactions. There is no bank or accounts used, centrally hosted and managed, where one can trace money movements and launch investigations [47]. The anonymity of the dark web, the presence of Bitcoin, and the support that Tor and other programs offer gives the terrorists an upper hand over the security and anti-terrorist agencies. The dark web and the existing technologies and platforms that support it complicate the work that security agencies have to do before they trace any terrorist group that leverages the system.

Spreading terror videos by the Islamic groups has prompted countries to severely act against the actions. Moreover, using secure channels and the dark web are areas that governments try to crack down and discover what such groups are planning. Countries have also removed much content related to propaganda, recruitment, fundraising, and attacks, as well as accounts that these groups operate and use to spread their content [41]. As if that is not enough, governments have also created counter-terror units to address online activities that come against the legal usage of the network.

2.2.2 Islamic State presence on the Internet

In July 2004, Zarqawi, the leader of Al-Qaida in Iraq, published a video of beheaded an American national Nick Berg [48]. Video footage released showed the victim wearing orange jump suite similar to Guantanamo detainees. This was the first video of this type publishing by this group. Despite initial disputes between Osama Bin Laden and al Zarqawi for sharing the beheading, later on December of the same year Bin Laden called for union of Iraqi Jihadists and appointed Zarqawi as prince (Amir) of Al-Qaida in Iraq. Since then, the jihadi leaders started to show off on media and create pages to disseminate their ideology [49]. From 2006 till now Islamic States group using social network websites (especially Facebook and twitter) to attract local and international supporters and encourage them to join their group very extensively [50]. Social network also serves Islamic States by facilitating other websites of the group on the Internet to reach people [51].

Islamic States group is using Internet as a channel for threating people, attracting supporters and strengthening their armed activities [52]. They are leading terrorist groups in using technology and most of its members are regularly using computers and electronic devices. They use advanced technology for advertising and producing films on their activities. It is also number one organization for using social networks efficiently to attract as many supporters as possible. They through social network started a psychological war to encourage people toward extremism [53].

Communication and relations through the social networks become an important mechanism for them radicalization process, especially after joining Giuliano Delnevo (died in Syria fighting Assad's regime on 18th of June 2013, Giuliano announced his conversion to Islam in 2008 and changed his name to Ibrahim) to the group, he carried out major changes in communication strategy of the group [53].

2.3 Cyber terrorism

Cyberterrorism is a combination of the use of cyberspace and terrorism and is distinguishable from other forms of cybercrimes such as data theft and bank fraud. Cyberterrorism is mostly propagated by groups or organizations and even individuals who are influenced by terrorist movements and leaders in the name of passing forward a political message or ideology. It results in violence that has physical or psychological repercussions beyond the immediate intended target. Cyberterrorism often has a broad reach and can affect states and nations regardless of the terrorists' geographical location, terrorist attacks especially that involve the cyberspace can originate from anywhere in the world [53].

Cyberterrorism entails the process of attacking computer systems. These systems are essential in the management of economic and social domains such as air traffic, and other transport means, national security systems, banking systems, among others. Cyberterrorism alters or destroys information, mainly strategic value through secret, unpredictable actions. It is the premediated, openly driven attack on information, information systems, computer software packages, and data, which results into malicious attacks on non-combatant targets by either national or international malicious groups or secret agents. Reports have revealed increased attacks on systems containing national military secrets and security. This entails the theft of data or virus attacks intending to destroy the data or make it unusable. Cyberterrorism appears to have found the contemporary society unprepared. Few states have put in place necessary legislation to combat this emerging threat to global security [55].

Cyberterrorism attacks lead to violence against people or destroy property or generate substantial fear to individuals. Such attacks could lead to deaths, or injuries, explosions or significant implication to the economy. Based on their impact, serious attacks on basic infrastructures may constitute cyberterrorism. However, attacks which challenge non-essential services, or cause measurable expenses, are hardly perceived as cyberterrorism. Cyberterrorism happens for various reasons. Malicious groups can take control over various networks which manage critical infrastructure including water, air transport, energy supply, military operations, traffic management, telecommunication and financial management systems and other systems which support the social wellbeing. Cyberterrorism can also take control of key industrial and energy systems in a particular state or country. These groups also steal technology source codes, strategic business plans, private or secret commercial plans, and data [55].

As noted, most cyberterrorism activities are in most cases related to cybercrime acts. One can thus conclude that criminals could apply strategies used by terrorists in implementing attacks on systems. The attacks thus come in different forms some being targeted and others untargeted. Untargeted attacks take different forms. Phishing attacks typically involve fraudulent emails aimed at convincing a targeted user or organization to legitimize access to its private information such as password, financial data or identity theft. Watering Hole involve installing a fake website to compromise the original aimed at attacking the users such as downloading remote access tools. Ransomware is a form of untargeted attack which entails infecting a system through file encryption or barring the user from accessing the system. The user will require a ransom to get back normal access to the system. Scanning attacks test for vulnerabilities in targeted internet network or system which allows deploying of random attacks on a broader scale [56].

Targeted attacks also take different forms. Spear-phishing is similar to untargeted phishing although they are targeted at specific user or organization. Distributed Denial of Service entails deployment of large amounts of package requests, to a single website or system aimed at overloading the information system and denying normal access by an authorized user. Supply chain attacks hijack the organization’s elements before they arrive. Zero-day is personalized manipulation of a system with particular exposures [56].

2.3.1 Cyberterrorism Vs. cybercrime

Essentially, the line between cyber terrorism and cybercrime lies in the intention of the attacker. Cybercrime is mainly based on financial matters. An attacker will tend to get access to computer systems or network in a bid to access data or control the entire system. With the data, the attacker can ask for a ransom or sell it elsewhere [57]. If the attacker puts spyware and gathers some information about the victim, he will mainly ask for ransom and give the information back. If the data includes credit card numbers, the attacker may use them to do shopping or transfer funds between accounts. Although there are some attacks that have different reasons, to find system vulnerability (ethical hacking) or to prove prowess, many hacks will focus on the financial aspect.

On the other hand, cyberterrorism's motive is to cause harm to the masses. The attackers will find the critical infrastructures that serve millions of people and disrupt them. Interfering with the air traffic control in an airport means that the people at the airport cannot direct the aircraft when coming down. An aircraft might be descending while the other is taking off and cause collisions [57]. Although the case might be extreme if the hackers modify the signals and give wrong information to aircraft coming to the airport.

2.3.2 Examples of cyberterrorism

Global cyberterrorists accessing military technology and control it. They leave the country insecure to external attacks. They can disable such systems and immediately attack the country.

Terror attacks disrupting major and critical systems such as water treatment plans, power plants, traffic control in cities, oil among others. A terrorist just needs a computer to bring down a power grid and cause havoc [57]. This will cause a crisis or jeopardize the security of millions of people who depend on such resources to live or in their work.

Attacks that disrupt major websites and create content that bring havoc to many. If a website with major traffic being defaced or published, 'Terror in New York' yet there is no terror only that the attackers hacked the website and published the terrifying report. Many people will start worrying much about false information [58]. Though cyberterrorists may not physically kill people, they normally understand that when they hurt human psychology, they cause stronger effects than killing them [58].

2.3.3 Cyber terrorism Vs. traditional terrorism activities

Cyberterrorism contains a substantial tactical advantage for terrorist organizations comparing to the traditional terrorism. Traditional terrorism is at higher risks during their planning process, and this endangers their lives of them individuals. Much of the deadly attacks, including the attacks on security agencies and citizens leads to significant loss of lives. A cyberterrorism is safer given that all cyberterrorism activities are conducted over the internet. What is needed is just an Internet-connected computer to create massive attacks and harm. However, cyber-attacks on organizational financial systems would cause alarming and huge damage that suicide attacks. The life of the attacker, unlike in traditional terrorist attacks, is not at risk [60].

Even though the terrorist activities are local, propaganda from the terrorists' groups spread out across the globe. Traditional terrorism activities have in most cases targeted public buildings where people congregate aiming at blowing it up and killing almost everybody. However, the activity remains limited to the building and people inside. In centrally, cyberterrorism can expand the physical harm by just a click collapsing thousands of organizations' websites. This affects the lives of thousands of people who depend on such systems for the supply of basic services such as computer-controlled water and electric power distribution systems.

Whereas traditional terrorist groups generally use their members to execute their missions, the emergence of cyberterrorist comes to opportunities for using subcontractors. This emerged trend now challenges security forces which followed the traditional terrorist activities. There is thus a need to gather proactive intelligence to counter cyberterrorist activities since these attacks happen outside the terrorists' organizations. Traditional attacks stimulate significant emotional reactions to the public. In contrast, cyberterrorism is unlikely to arouse any emotional reactions as at the moment of action no cases of death or injuries are reported. Traditional terrorists usually send a message to the political class and the public in which violence and damage remain basic tools of communication. However, violence has become a goal rather than a tool in cyberterrorism [60].

The development of technology has made the world to shift from considering space and time as impediments. Terrorist groups can communicate with their militants via encrypted channels. Terrorist organizations can materialize their activities through encrypted messages which allows exploitation of the Internet experiences and also to spread the political and ideological propaganda. Due to its nature, it becomes easy to determine the source of the attack in traditional terrorism. This is quite difficult or nearly impossible cyberterrorism as the attacker may not have direct contact or association to any terrorist group. Equally, assessing the physical damage caused by traditional terrorism activities is somehow easier. Assessing the magnitude of the damage caused by cyberterrorism is impossible in most cases.

2.4 Surface, Deep and Dark web

The Internet is a combination of assets which has mixed the technology of infrastructures and calculating to provide prompt connectivity and worldwide information facilities to all its users at a little cost [61]. The Internet consists of three parts surface web, deep web, and dark web. The surface web is the most popular and heavily linked websites on the Internet, and the part of the Internet which is found by the search engine is the example of surface web pages including Google, Facebook, YouTube, the New York Times, and other websites [62]

The surface web consists of 4% of the Internet, and it is the visible web [63]. The surface web is the web that people use it for daily work. Some of the services on the surface web needs authentication to access, so through authentication people could communicate more comfortable because of guarantee that no one alters the data at either end of the communication. However, this point is the vulnerability in some cases because attackers and hackers could steal information.

The surface web is highly careful about the public use and filters the poor webpage and video. However, the privacy is the significant issue in the surface web, because anonymity is not available in the surface web that point makes surface web has weak privacy in some of the situations [62] [63]. Because of surface web weakness, people wish to find somewhere where it is more private and provide anonymity on the web.

The deep web and dark web are the place where people wish to access because it is anonymous. There, you can do if you have ever heard stories about illegal online activities such as drug buying and selling, killing the human, celebrities busted for child pornography, mad scientific experiments, and Illuminati rituals, it appears to be the unchartered web browsing experience. The mysterious and terrifying “dark side” of the Internet is the "dark web," or the deep web. The deep web is content concealed behind HTML forms sites and pages that we cannot find from any search engines indexing the material [64]. The deep web is invisible thus could not be detected by the search engine; the web pages and sites are usually not illegal or even dangerous.

The dark web offers are different from surface web, it offers greater privacy. They do not give a limit for providing information, and they are not filtered for public use, dark web for secretly political news [8]. Dark web is a place for those that just do not want to be searched and want to stay anonymous, the dark web market is used to discover hard-to-find books that you cannot find it in Amazon. To access the deep web and dark web, special browser such as The Onion Router (TOR) browser is required [65]

TOR is not a browser, but TOR is one of the encrypted networks that used for accessing deep web and dark web [8]. Furthermore, TOR gives people more privacy to surf because it does not track; this points makes TOR and dark net more trusted. The users of the dark web and deep web trust it, because it consists of anonyms group and information of the users who are invisible. The browser and the tools they use to anonyms them self is trustable. Furthermore, users of internets always need to protect their privacy; they found it in the dark web and deep web because their data are preserved [65].

2.4.1 Online Radicalization on surface web

Most of the digital infrastructure possesses important defence mechanism aided by modern technologies including firewall, password security system, key encryptions such as 3 Data Encryption Standard (DES) and Rivest-shamir-Adleman (RSA), stenography, intrusion detection systems, Secure Socket Layer (SSL), IPsec, access control lists, among others. However, the discussion of terrorism prevention responsibilities falls under the jurisdiction of governments and national bodies. Internet is known as a major contributor of cyberterrorism radicalization. Radicalization remains on the rise as internet, and social media continue to spread.

Online radicalization in both parts of the approach are applied by potentially powerful terrorists and as a consequence of the spread of social media among the supporters of these extremist groups. The official propaganda and the discussions initiated amongst the users becomes major drivers and accelerators of the radicalization process. There seems a new shift towards radicalization of children over the Internet, bringing major concerns and demands to look for ways to combat these activities. This calls the need to stop online propaganda for the radicalization of children from both the supply and demand side. The phenomenon should not be viewed as isolated through the security lens [66].

2.4.1.1 Communication theory

Social media is based on the communication theory. Communication is the process by which people interactively create, sustain, and manage meaning. The communication process is the flow of information from one person to another. The communication theory is any systematic summary about the nature of the communication process, which is a field of mathematical and information theory [67] which studies the technical process of information [68] and the communication theory model is a structure that represents the communication theory [69]. The model of communication tools and The Strength of Weak Ties are inventing and developing social media based on sociology, but also becomes a good framework for analysing and taking advantage from Internet and social networks by the terrorist organizations, as an effective communicating tool.

The network theory is a road map for detecting effectiveness of social media for terrorist organizations and how it facilitates their activities by enabling them to hide their identities [69] [51]. The tools based on communication theory are used by terrorist organizations to organizing activities of group of people and even nation can be explained theoretically. The Islamic States group nowadays use tactics for their communication different from the traditional ways previously used by Al-Qaida cells and it is based on communication theory [70].

2.4.1.2 Graph theory

Social networks which are a part of social media are naturally modelled using graphs where nodes represent actors and edges relations between them. A graph consists of a pair of nodes, and the set of edges that connect the nodes [71]. In the following, network means the graph modelling it. Edges might be undirected or directed depending on whether they reflect symmetrical or not symmetrical relations between actors. Most social network analysis techniques focus on undirected graphs since the considered relations are typically mutual and bi-directional. Unless otherwise specified, this research only considers the techniques for undirected graphs [70].

2.4.1.3 Text Mining

I. Different text mining techniques are available for analysing the text patterns and mining process. One of the techniques to extract meaningful information from large amount of text is (1) Information Extraction (IE), the task of this techniques is to identify a predefined set of concepts in a specific domain, ignoring other irrelevant information, where a domain consists of a corpus of texts together with a clearly specified information need. In other words, IE is about deriving structured factual information from unstructured text [72] [73].

II. Information Retrieval (IR), is another technique for processing of extracting associated and relevant patterns according to a given set of words or phrases. It is a set of approaches, drawing on the tools of computer science, information science, and corpus linguistics, for accurately locating small amounts of relevant information in large data sources [74] [75].

III. Natural Language Processing (NLP), is techniques for automatic processing and analysis of unstructured textual information [76]. It performs different types of analysis for abbreviation and their synonyms extraction in the text. It combines linguistics and artificial intelligence to enable computers to understand human or natural language input. Natural language interfaces permit computers to interact with humans using natural language, for example, to query databases [77] [78].

For the text mining part in this study, IE techniques, IR techniques and Natural Language Processing NLP is combined to extract meaningful information, find relevant patterns according to a given set of words and for abbreviation and their synonyms extractions.

2.4.2 Cyberterrorism in dark web

Dark web is used for both Illegal and legal activities. The illegal activities include purchasing weapons, human organs, and drugs, scam credit card, fake passport and ID. Stealing private and personal information, exploitation to upload malware, hiring killer and hackers, human trafficking, child pornography and for terrorist activity. The dark web uses for legal activities including access to additional information, military, everyday buying and selling, private message sending within the country and is used as well by the government for example in august 2013 to interrupt messages being sent amongst senior al Qaeda officials [79].

The military may use the dark web to study the environment in which it is operating as well as to discover activities that present an operational risk to troops. Islamic State (IS) and supporting groups seek to use the dark web's anonymity for activities beyond information sharing, recruitment, and propaganda dissemination, using Bitcoin to raise money for their operations [defense one]. In its battle against IS, the Department of Defense (DOD) can monitor these activities and employ a variety of tactics to foil terrorist plots [71].

The United States government has been trying to design certain programs that can take away some of the anonymity of the TOR and track users on the dark web. They are trying to find ways to fight these terrorist groups but still give terrorist organizations a certain level of privacy [80]. The users of the dark web they trust it, since the browser and the tools they use to anonyms them self is trustable. The previous users they have experience using the dark web and they know that keeping the privacy of the users is important in the dark web. Thus, trust is very important in dark web and digital trust to make users believe in the forums they visit and continue using it is very important.

The dark web is also affected by cyber terrorism. As the name 'dark' suggests, it means that there is no light. In a nutshell, it is hard to get to that web easily. Due to the immensity of the world wide web, as more websites are added each day as people and corporates tend to increase online visibility, the search engines are the ones mainly used to access it. Therefore, when someone tries to search for some information, they use Google, Bing or other search engines to reach there. Major websites such as Facebook, Amazon, Wikipedia, and others are easily accessible via search engines and hence, not part of the dark web. Many websites are accessible via search engines.

However, it is integral to note that there are even more websites that are not indexed by the search engines and thus, not accessible through search. These can mainly be accessed via typing the Uniform Resource Locator (URL) because their Internet Protocol (IP) addresses are hidden. Users mainly access them via encrypted networks which give them anonymity. There are special browsers that promote anonymity such as Tor, Freenet, and I2P. These are the browsers that people use when crawling the dark web, also known as dark net. The Onion Routing (Tor) started in 2002 by the Naval Research laboratory of the US to promote online anonymity and protect from online monitoring [81].

2.5 Exploits

Exploit is a wide term that describes computer exploits. It entails attacking a computer system, mainly taking advantage of a vulnerability. Attackers like identifying a vulnerability in any computer system because it gives them ease of assessing files and programs than a system with no vulnerability. The term means that the attacker has succeeded in getting into a system. To understand it better, a computer system is usually made up of computer hardware, software, operating system or plugins. If the vulnerability is an Operating system (OS) bug, the attacker can then hack many computers and introduce a malicious code that destroys files and data, copy files, spy or any other way. The user ends up losing data which is essential to every entity [82].

The malicious program would control the OS and execute many system tasks. Many exploits are done remotely over a network. The system owner will not know whether the computer is controlled remotely by someone else. When the software developers learn that there is a bug in the software, they work on a patch or fix to respond to the bug. The patch is usually downloaded online from the owner’s website or else automatically downloaded by the application or OS. Windows OS does not require the computer user to download the patch. It automatically does so when the computer is connected to the internet. For software, if the user does not download the patch, he or she may be left open to attacks.

2.5.1 Types of exploits

There are several ways that hackers leverage to exploit computers. With the presence of the internet and many devices being connected, hackers use web-based techniques to identify and exploit computer systems. The most common ones are Cross-site scripting (XSS) and Structured Query Language (SQL) injection. The three are among the top ten critical vulnerabilities according to the agency that analyses the data, Open Web Application Security Project (OWASP) [82]. Information is always considered as the most valuable asset an individual or corporate has. Computer hardware may be changed but it would be hard to get the actual data. Therefore, security officers must be diligent and proactive in handling securing systems.

XSS is a technique that happens when an attacker tricks a computer user into linking a malicious website. The user will assume as if the link takes him or her to a genuine website. When the user shifts the webpage, the attacker inserts untrusted data which has not been validated and either take the user to a malicious website or steals user session [82]. Alternatively, the link may lead to downloading malicious code or file that inserts itself in the computer and controls it.

SQL injection has been found to cause great harm to applications. In essence, the attacker takes advantage of the non-validated or non-sanitized inputs in the login forms and insert characters, a malicious SQL command, that is interpreted differently by the SQL query handler [82].

Security misconfiguration is a critical point of exploit. Computers come with security settings such as the firewalls. If a person, by mistake, misconfigures the firewall, he or she might open some ports that a hacker may use to find an opening to the system. Additionally, an application or software may have some with security misconfiguration whereby the attacker identifies that there is a way he or she can bypass the security configurations by fooling the application. He can access the software and steal personal information or alter it.

When exploiting a computer system, an attacker may have found a vulnerability that even the developers are now aware of. Known as '*zero-day exploit*,' the attacker exploits on the system and the patch will only be available when the developer has created it and uploaded it on the website for downloads [83]. For a zero-day-exploits, the intrusion detection systems may not helpdetect or prevent them. The worst would happen if the developer delays in releasing the patch as the system remain vulnerable until the patch is available to fix it. Computer exploits may also take shape of denial of the service, code injection or malware delivery among others. All these aims at identifying a vulnerability and taking advantage of one to access or bring down the computer.

2.6 Digital Trust

To provide an overview of digital trust, this chapter focuses on trust in the different fields of cyberspace. There are some UTM in the digital world for ensuring trust in digital trust environments. Digital changes occur quickly and to be prepared for those changes in the digital age, trust is highly important. Digital trust is a trust that is based on either past experience or evidence that an entity has behaved and/or will behave in accordance with the self-stated behavior [84].

Self-stated intent is provided by the entity, which may have been verified/attested to by a third party. The claim that the entity satisfies the self-stated behavior can either be substantiated through past interactions (experience) or based on (hard) evidence such as validatable/verifiable properties that have been certified by a reputable third party, e.g., Common Criteria evaluation for secure hardware.

2.6.1 Semantic Web

The notation of trust is one of the core components of the semantic web [85]. Agents and automated recourses must make judgments when alternative sources of information are available. Computers will encounter challenges in performing these judgments. Trust is calculated automatically for an individual in a network on the web; this trust metric uses group assertions to determine memberships within a group [86].

Architecture of digital trust in the semantic web consists of a reputation-based mechanism, context-based mechanisms. Such an architecture also provides confidence, which will lead to reputation-based mechanisms. Reputation-based mechanisms use rating mechanism by which users of other websites or information and customers will rank their confidence in an information source [87]. Booking, Expedia and eBay use this rating system, which requires information consumers to provide ratings.

In trust-based mechanisms, trust is based on meta-information, which is information about the information, such as how the information was obtained and who provided the information. For example, downloading and installing an application from the App Store for Apple products is more trusted than obtaining the application from another party. Content-based mechanisms rely on the content of the information and whether the same information has been provided by multiple reliable sources [88].

The semantic web is a large, multidimensional space. Trust in the semantic web is highly complex issue. According to the research in this area, parameters must be employed for proving trust in the semantic web.

2.6.2 Data Provenance

Knowledge of the origin, changes in the data and the processes that caused the changes in the data ensure the quality of the data. Provenance and trust cannot be separated. Trust is measured based on the history of the data. In data provenance, the reputation context and the content of the data source are the main focuses [89].

Uniquely identifying the original data according to the signature of the data modifier, including the date and the time, will increase trust in the provenance of the data. Many issues will be encountered in identifying all the artifacts. A model for tracking and recording the data provenance and assigning trust to the existing infrastructure will increase the likelihood of realizing the objective of trust in data provenance.

2.6.3 e-Government

Trust is the foundation of the relationship between the entities in e-services and will binds the entities together. Trust between online e-services is essential to the success of the relations. E-government trust model and showed that trust is a multidimensional problem and that digital trust in e-government must cover all the societal trusts [90].

Trust among the entities and trust in the Internet are essential to the success of an e-government. Trust can be ensured through a model that can measure the performances of the e-services that are provided to the citizens and the satisfaction of the citizens with the quality of the system, the accuracy of the information, the security of the channel and the speed of the process.

2.6.4 Operating Systems

The evaluation of trust in an operating system depends on the enforcement of a security policy and the sufficiency of its measurements. The design of a trusted operating system begins with security and must prevent the user from doing more than necessary. The “authentication, least privilege” verifies that the input is of the expected form and adheres to the “edit” rules of “complete mediation”; there are many other features that are necessary for designing a trust-based operating system, such as mandatory access control, discretionary access control, object reuse protection, audit log management, and intrusion detection [91]. Thus, trust is one of the most important aspects of a secure operating system. Providing multilevel security for an operating system will ensure that it is a trusted operating system.

2.6.5 Artificial Intelligence

Trust may depend on knowing whether anomalies exist in these systems, whether the anomalies that do exist can be managed, and whether these anomalies affect the limitations of the human supervisors. Nowadays a robot measures its own trustworthiness, and they assumed that the robot can be trusted to perform important tasks; if a human can trust the robot as a team member, then the robot may become helpful to human teams [92].

A developed life-cycle model framework that incorporates trust components and is based on the system for codifying how trust is incorporated into a new system. Testing and evaluation ensure that the trust components are functional and trust is explored in the context of human-robot collaboration on the factory floor. A time-series model of trust to relate speed to flexibility to measure and gauge the improvement in a system on the factory floor [93].

A human user's trust in a human robot interaction was measured by exploring the development of a unifying survey scale depending on the context and the culture of the perceiver and the bias that is introduced by a questioner, trust has an elusive, subjective meaning. Trust will develop through use over time, thereby ensuring that trust is built with all the technologies that preceded artificial intelligence [94].

2.6.6 Social Media

Trust is a significant component of many relations. Trust can be created online between actors, and it is not necessary to have live meetings online. Social media has been identified as a key vehicle for fostering social connections that maintain or expand existing social networks. Trust in social media is based on social trust among entities and the level of security of websites and applications; these interactions can facilitate digital trust. Social media includes interactive Web 2.0 Internet-based applications [95].

Web 2.0 has security issues from the attack and penetration perspectives; however, there are solutions that allow such issues to be overcome. Web 2.0 satisfies the security requirements for being a trustable party. It is not clear where Web 2.0 will lead, but the trends may positively influence the direction of Web 2.0. Apart from trusting individuals on social media, the security levels on Web 2.0. cause users of social media to trust the environment.

2.6.7 Internet of Things

A trust-, encounter-, and activity-based protocol for the Internet of Things was proposed. Based on this research, when interacting with each other, two nodes can directly rate each other and exchange trust. The social Internet of Things (SIoT) integrates social networking and the Internet of Things. A reputation-based trust mechanism for the SIoT can address some of the malicious behaviors that mislead other nodes. A trust model for protecting user security via location-awareness and identity-awareness was proposed [96].

In, a layered IoT architecture for a trust management control mechanism was proposed. Another trust system based on node behavior detection was proposed in, in which a well-defined trust negotiation language that supports semantic interoperability in the IoT context was introduced [97].

2.7 Trust in Cybersecurity

Trust problems that are related to security issues become apparent. Trust-based security solutions in open environments will require development to further increase security. In, trust was defined as the security expectation of an entity according to the available security evaluation of that entity. Trust computation models differ in terms of the information that they use to compute trust. Cybersecurity risk is a complex multicomponent and multilevel problem that involves hardware, software, environmental, and human factors [98].

The operating system, the semantic web, data provenance, online e-services, artificial intelligence agents, and interactive social media on Web 2.0 often have security requirements and are trustable; however, there remain cybersecurity threats such as cyberbullying, home automation, digital media, and cyberterrorism in cyberspace. Models that are secure in cyberspace are highly important for increasing the digital trust in this environment.

For obtaining security experiences from services for trust computations, the results of trust computations are used to make decisions in cyberspace. In addition, the concept of the similarity ratio for security systems of services was proposed, along with a formal model of the similarity ratio. The similarity ratio enabled the aggregation of experiences from many services regarding the security system of a specified service [99].

2.8 Trust for Digital Certainty

Certainty is the firm conviction that something is true or the quality of being reliably true, whereas uncertainty refers to the lack of sureness about someone or something and may range from a falling short of certainty to an almost complete lack of conviction or knowledge, especially about an outcome or result. Lawrence suggests that identifying the degree of certainty is underappreciated in various domains, including policymaking and the understanding of science [100].

Uncertainty can be identified in each domain and field. In the field of technology and especially on the Internet, when everything is connected the level of uncertainty will increase. Trust helps increase certainty. A framework will assist developers in including trust in Internet of Things scenarios. Traditional security mechanisms are insufficient, and the framework considers privacy, identity requirements, functional requirements and trust [101].

Trust will help people overcome perceptions of uncertainty [102]. A trust model of web services that uses the average ratings by end users to automatically determine the selection of web services. A novel metric for quantifying the consistency at the compliance level of a service contract [103].

2.9 Trust in the Dark Web

People worldwide use the Internet for engaging in social media, sending email, research, shopping, and other daily tasks. What people do on the Internet constitutes a small part of the Internet; the remainder of the Internet is known as the deep web. The visible surface of the Internet is indexed by search engines, while the deep web is not. Visitors of the deep web require specially configured software to access it. The furthest corner of the deep web is known as the dark web; thus, the dark web is a part of the deep web. It contains content that has been intentionally concealed and may be accessed for legitimate purposes or to conceal criminal or malicious activities. The dark web is a platform for Internet users for whom anonymity is essential; it can be accessed using a special web browser, known as the Tor browser. Tor relies on a network of volunteer computers to route users' web traffic through a series of other users' computers such that the traffic cannot be traced to the original user [104].

The United States government has focused on designing programs that can remove some of the anonymity of Tor browsers and track users on the dark web. The government is also developing methods for fighting these terrorist groups while still providing people with a certain level of privacy [80]. Users have trust in the dark web given the trustable nature of the browser and the tools that are used for anonymity. Previous users have experience using the dark web, and they know that maintaining the privacy of the users is important in the dark web. Thus, trust is highly important in the dark web, and digital trust enables users to believe in the forums and the websites that they visit and continue to use.

2.10 Digital Trust Models

There are many trust models in the digital world for ensuring trust in digital environments. Digital changes occur quickly, and trust is highly important in preparing for these changes in the digital age.

Digital trust models are employed in research. Some trust models are employed in dark web communications, transactions and exchanges; for example, one trust model pertains to the recommendation features of websites such as eBay to avoid the cold start problem. Other studies consider trust models in social networks. Trust models are further used in e-government services, while some works focus on evaluating trust models.

Models based on trust used to obtain metadata, and to discover a demonstration of whether or not the models are effective. This can be used to further study the connections between users and products and to focus on latent factors of users and products, such as time parameters and in product browsing [105]. This can improve upon this work by investigating security-based models for protecting composite and community-based architectures from potential attacks [106].

Cyberspace is significantly economical, completely secret, the type and size of the targets as well as the potential damages are enormous through the click of the mouse. An attacker in no required to cross any distance or seen as a perpetrator. These factors are common and reasons why terrorists would prefer cyberspace to accomplish their missions. The availability and distribution of Internet make recruitment and mobilization of new members easier. Terrorist groups find it easier to search for information and find the physical location of the facilities of interest. Finding and sourcing funds, building connections for implementing joint missions, exchanging information and educating new members also becomes easy via the Internet. Disinformation, threats and creating terrifying images of torture and executions affect psychological wellbeing of targeted individuals, and this could spread quickly causing more panic and fear. Understanding the impacts of cyberterrorism on the psychological welfare of people becomes extremely important [107].

There are many trust models on the internet to ensure trust in digital environments. Trust models are the exit in dark web communications, transactions, and exchanges". Moreover, when the customers buy goods in dark web there exist three parts one buys the products, another sell, and the other monitors the transaction if the person who buys do not like the goods or they do not get the goods. They do not pay the cryptocurrency, and the operation would not be done, and the buyer would not transact the money. However, this process is done without the people ever meeting.

Trust is multidiscipline, multidimensional and multifaceted. Societal trust means studying various forms of trust from economic, medicine, psychology, sociology, religion, political and information science. It is not easy to see what trust exactly is, but people can learn what trust is from different perspectives. In sociology trust is one of the constructs, and it is attributable to relationships in social systems. Trust is very important in society and [108] without trusts all contingent possibilities should be always considered, leading to a paralysis or inaction.

When an entity trust someone else or that someone is trustworthy, that implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to this entity is high enough to consider engaging in some form of cooperation with him. Correspondingly, when an entity say that someone is untrustworthy, that imply that the probability is low enough for the entity to refrain from doing so [109].

Mapping from societal trust to digital trust needs understanding the trust theory and with frameworks, modelling and managing in technology this aim can be reached. The digital trust designers have to find a way to express this trust in digital world, the results have to be evaluated and risk management is very important here. It needs to provide both security and privacy [110].

Trust is influenced by reputations (Public evidence of the trustee), recommendations (i.e. a group of entities' evidences on the trustee), the trustee's past experiences and context (e.g. situation, risk, time, etc.). Most of this work focused on a singular trust value or level calculation by taking into account the previous behaviour of the trustee [111]. The reputations, the recommendations and the trustor's own experiences are assessed based on the quality attributes of the trustee, the trust standards of the trustor and the local context for making a trust or distrust conclusion [112].

Automatic trust management is very important to design trust in digital world. The automatic trust management includes four aspects, which they are trust establishment, trust monitoring, trust assessments, trust control and re-establishment. That is the process of establishing trust between the actors, monitoring the performance of actor's behaviours, evaluating the trustworthiness and assessment of current relationship. When changing happening the truster can decide which measure should be taken and then if the trust relationship is broken can re-establish the trust relationship or control it [17].

The self-stated purpose of intent is provided by the entity and this may have been verified/attested by a third party. The claim that the entity satisfies the self-stated behaviour can either be gained through past interactions (experience) or based on some (hard) evidence like validable / verifiable properties certified by a reputable third party i.e. Common Criteria evaluation for secure hardware.

There is a great deal of work done in proposing digital trust models to ensure trust, security, efficiency, accuracy and simplicity [113]. Those models are employed in social media, peer-to-peer network, distributed network, e-services, robotics, and semantic web [114]. The UTM is like measurement [115], trust and trustworthiness are critical measurements of a distributed sensing system or a heterogeneous network comprised of sources of information, knowledge, hardware, and software [89] of different trust models. Thus, a unified trust model is to detect threats in different services in different layers of Internet. The trust model theories that are been applied are the probabilistic and gradual approach.

Trust models aim to capture computing, transmitting and perceiving of any types of trust in a computational setting. The concept of trust varies from a person to another without any unified definition. However, the most common types of trust defined in the literature are (1) reliability trust, subjective probability by which an entity expects that another entity perform a given action; and (2) decision trust, one entity is depending on another entity in a given condition with a feeling of relative security, even with the possibility of negative consequences [116].

Each trust model setting must have at least two entities which have to interact in some way. An entity can play several roles or at least one role, trustor, the entity which places trust, and trustee, the entity on which trust is placed [117]. The purpose of a trust model will determine the features of the model and the roles of the entities. In some subjective trust models depending on the type of the model, an entity can be a spectator that informs about its opinion of other entities based on its own experience and observations [118].

Trust models can be classified in several ways. According to the two common ways of classification that can cover most of the current trust models are (1) a probabilistic approach, and (2) a gradual approach. A probabilistic approach is about single trust value, the entity is either trusted or not trusted, while the gradual approach is concerned with the valuation of trust, the outcome can be positive or negative to some extent and a higher trust value corresponds to a higher confidence in an entity [119].

2.10.1 The International Civil Aviation Organization – Public Key Directory (ICAO PKD)

ICAO is an example of a trust model developed to support global interoperability of ePassport validation [116]. It is a centralized directory that facilitates an independent, secure, organized and cost-effective sharing of up-to-date information between States. Each electronic passport has IC chip embedded in carrying information such as personal details, finger-print, and photo. To ensure secure transfer of data a digital signature is attached to ePassport to ensure the data is not altered. Below are various components of the ICAO system. Figure 1 shows the structure of the ICAO PKD model.

Electronic passport issuance feature consists of Country Signing Certification Authority (CSCA) certificate and passport-issuing system. The CSCA certificate acts as a signature for Certificate Revocation List (CRL) and Document Signer (DS) certificate, where CRL is a list of digital certificate that have been revoked by issuing Certificate Authority (CA) used to store the information about the revocation of CSCA Certificate. While the DS certificate assigns the electronic data stored in the Integrated Chip (IC) of ePassport.

ICAO-PKD feature the ICAO-PKD comprises two components, common reference and registration directories. The standard registration directory store information after validation confirmed while a current reference directory copies validated data stored so that it is referred for inspection of entry into, and departure, the country [120].

Validation feature This is the system which validates an electronic passport. During the validation process system downloads CRL and DS Certificates from ICAO-PKD and compares against the registered CSCA Certificates to see if they match. The system then checks if the ePassport signed by the correct DS certificate registered in CRL.

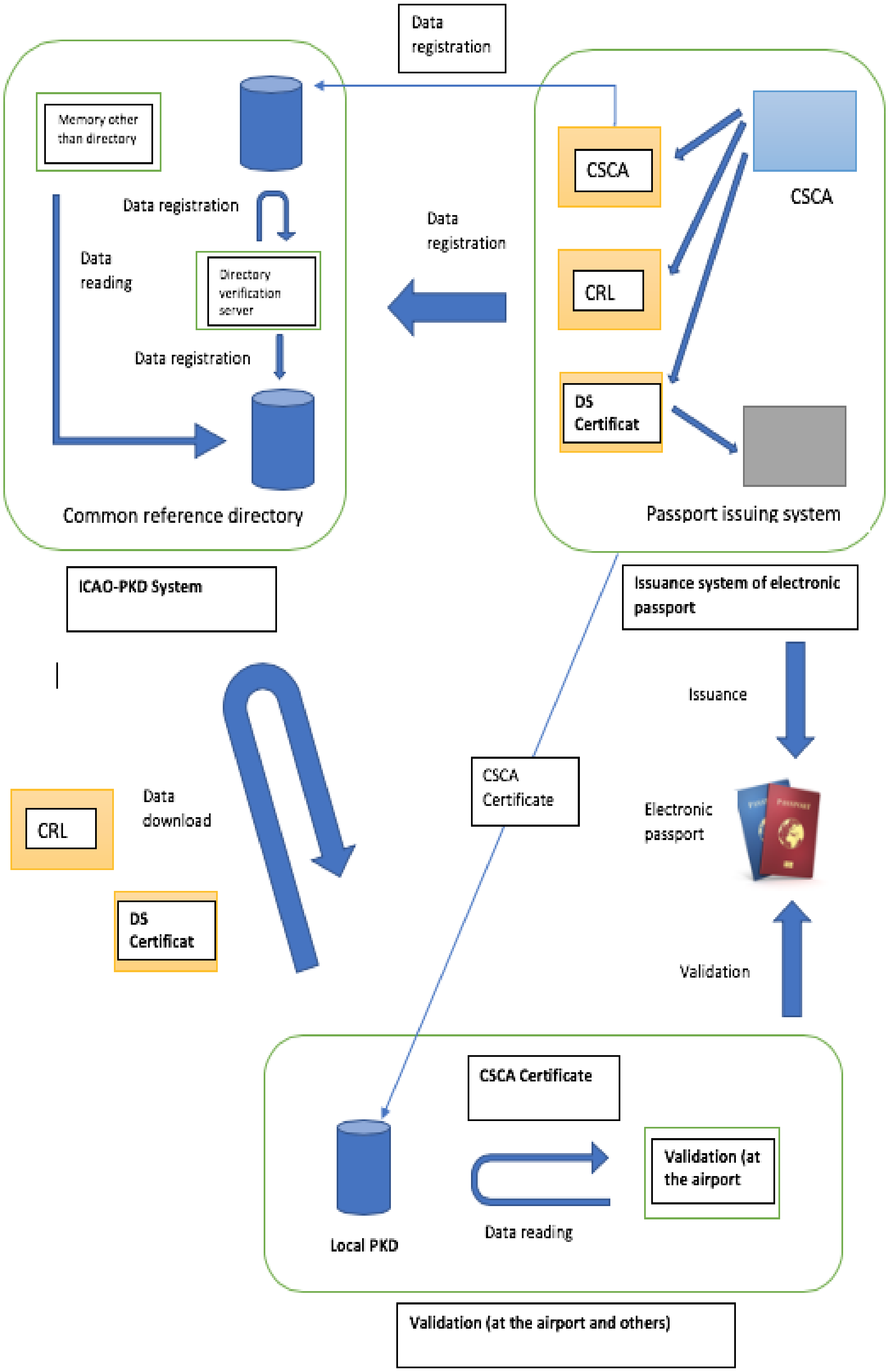


Figure 1: ICAO PKD, Adapted from [116].

2.10.2 Electronic Identification, Authentication and Trust Services (eIDAS)

eIDAS is a set of standards for trust services and electronic identification for the electronic transaction in the European single market. The primary aim of the eIDAS program is to provide a legal foundation for Secure Identity Across Borders Linked (STORK) which is proposes a solution to make it easy for citizens to access the concerned public service online wherever they are located and a legal effect for electronic trust service artifacts. eIDAS regulates electronic transactions, electronic signature, involved entities, embedded processes to ensure a safe way for people to conduct online business such as electronic funds transfer as shown in figure 2. The system allows citizens from the Member States to authenticate and verify their identification while transacting or accessing online services in the other Member States. Citizens use Electronic Identifications (eIDs) to validate themselves and connect with their Identity Provider (IdP) in their country. For instance, when a citizen needs an online service in a Member state, he/she is requested to authenticate himself or herself using eID. During the IdP for verification. If the result returned to the service provider is correct, the citizen is permitted to proceed with accessing the service [121].

The eIDAS Solution allows various eID national protocol interoperable with each other and translates national identification data into a standard format that can be used and understood by all Member States. This makes the eID of a citizen from a Member State to be interoperable and accepted in other counties. The eIDAS opens a window of new possibilities and opportunities to a citizen to use service across borders. With eIDAS, the European Union has managed to lay down a predictable legal framework and the right foundation for people, public administration and companies to safely access to online services and transact across the boarder in just ‘one click’. [122]

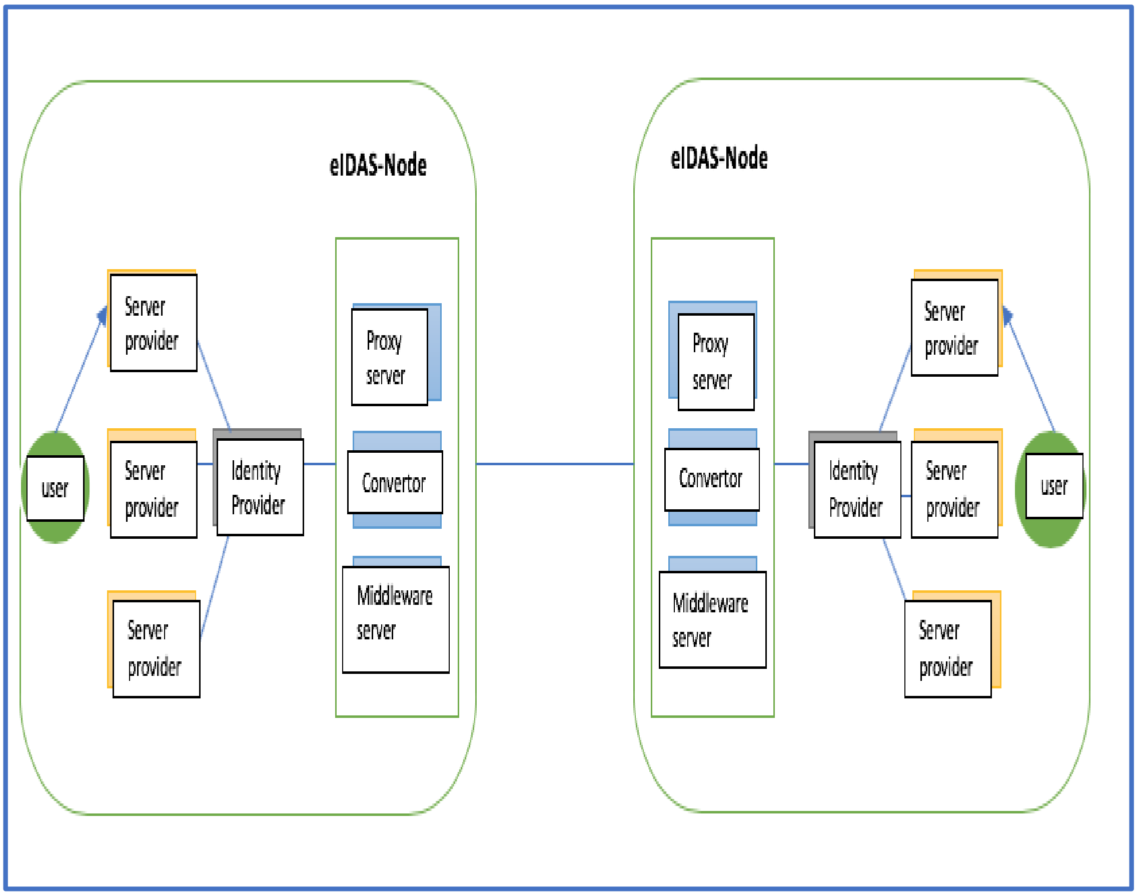


Figure 2: eIDAS structure, Adapted from [121].

2.10.3 Federal Identity, Credential, and Access Management (FICAM)

ICAM refers to Identity, Credential, and Access Management. It is a trust model developed by the United States Federal Government to provide guidance, processes, and supporting infrastructure that allows secure and streamlined online service delivery. Figure 3 shows the parts of FICAM. ICAM program was tasked to align the identity Management activities of the United States Government by ensuring the security and privacy of Government to Business (G2B), Government to Citizens (G2C), and Government to Government (G2G) digital interaction and services [122]. A well-structured ICAM program minimizes costs, secures access to information, simplifies user management, protects resources across organizations. Following are some of ICAM initiatives;

ICAM Access Management Services manages and controls how entities are granted access (both physical and logical access) to resources

ICAM Identity Management Services Guides agency activities to reduce redundancy in ICAM programs and to support smooth services delivery to external consumers by leveraging a government-wide federated identity framework. The program assigns attributes to a Digital Identity, which then connects it to a person, and manages the lifecycle of authoritative attribute sources.

ICAM Auditing and reporting Guides the agency on reporting and auditing to enhance continuous monitoring of service delivery to consumers [123].

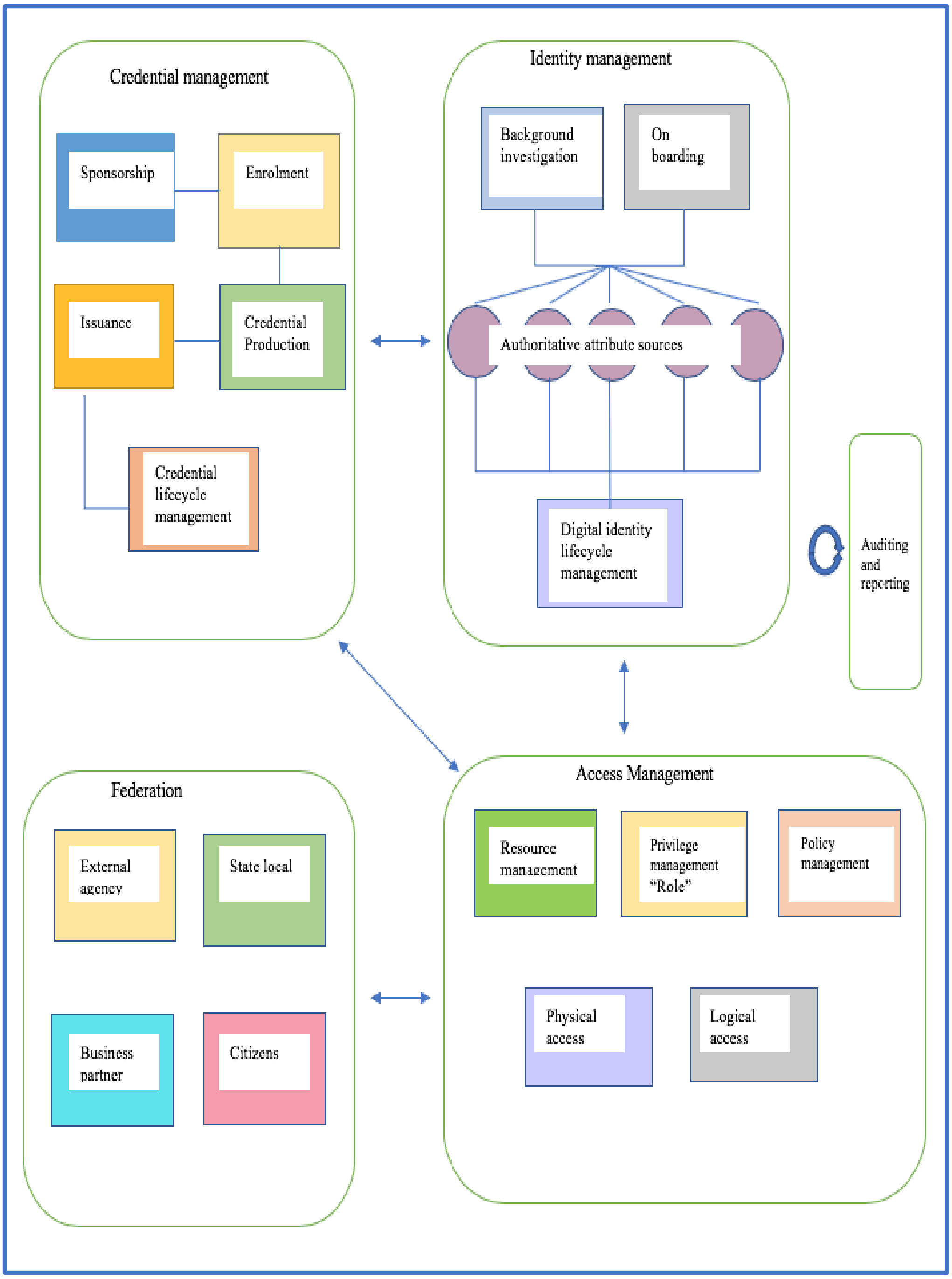


Figure 3: FICAM structure, Adapted from [122].

2.10.4 Blockchain

This is a trust model which provides an effective way to address the issues of traceability and anonymity in a distributed network with multiple entities, which wants to exchange information with each other securely [124]. The technology facilitates the formation of an efficient distribution system that allows products and services provided in a distributed manner. In blockchain technology showing in figure 4, two parties securely and anonymously exchange data, i.e., money, medical record, deems, customer details, contracts, or other assets that are in digital form.

The two main features of element of blockchain technology are (1) trust evoking, and (2) its decentralized nature [124]. Trust is facilitated through a high degree of transparency, where through the establishment of immutable architecture, two entities can publicly broadcast new transaction and information the network without involving a third party. Blockchain technology ensures high data integrity by securing interactions via public-key cryptography and engaging participants in the data verification process. On the other hand, decentralization of blockchain technology facilitates the realization of a private, reliable and versatile environment [125]. There is a higher level of privacy since the interaction in the peer-to-peer network relies on public-key cryptography, introducing pseudonym for each entity. Blockchain also provides a platform in which each object is permitted to enter and distribute their programs and code, therefore, providing an open and versatile setting [19][20].

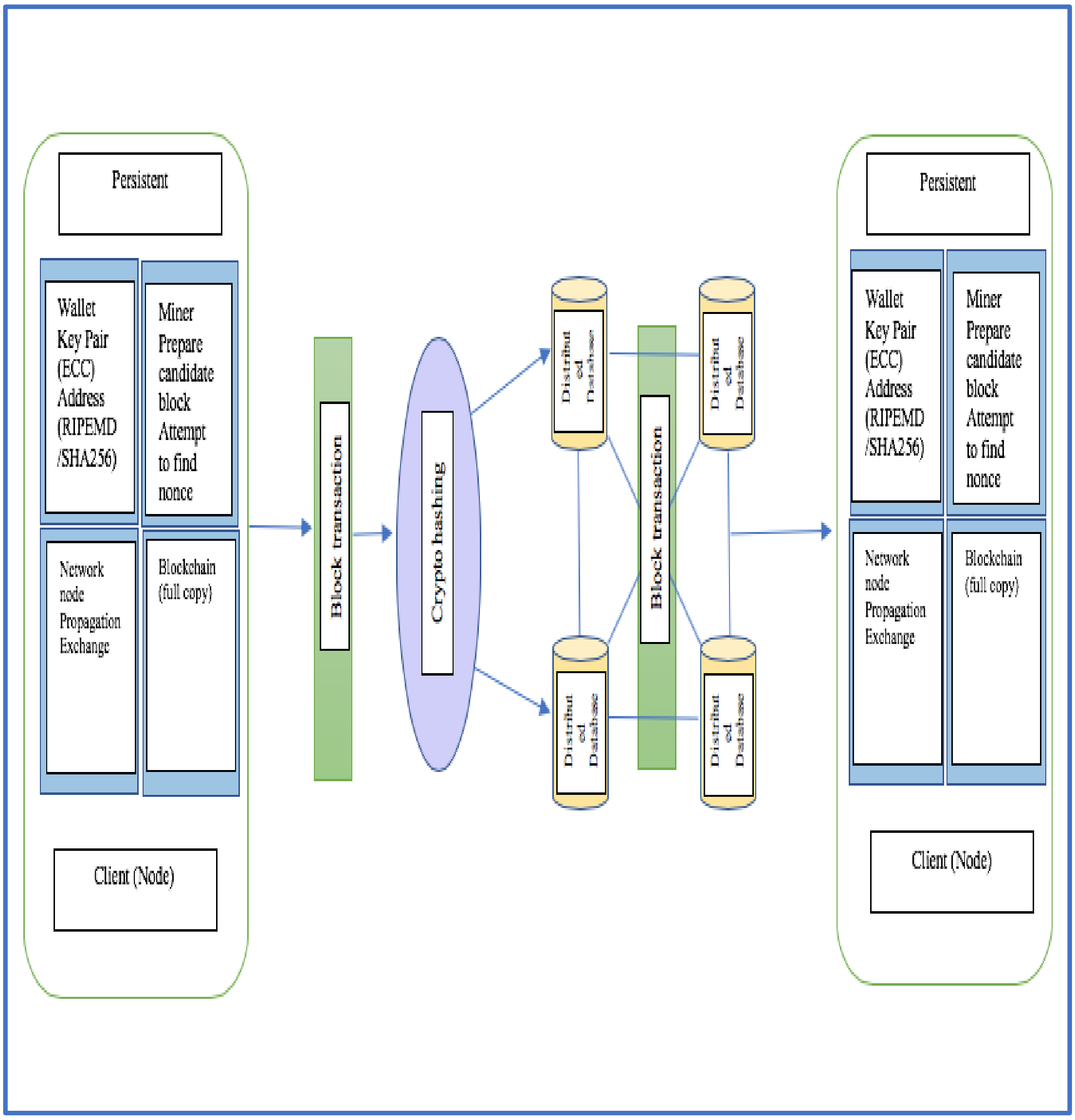


Figure 4: Blockchain security structure, Adapted from [124].

2.10.5 MANETs

The mobile ad hoc networks (MANETs) face significant challenges to deliver packets reliably through multi-hop intermediate node. MANET lack3~s the structure and central authority which can create and facilitate communication in the network comprised some independent entities which act as network objects which agree to rely on packets for each other. In MANETs, nodes have limited physical security information, dynamic topologies, resource constraints and significantly depends on the personal entity's collaboration in packet forwarding [126]. Previous literature has suggested a recommendation-based trust model help filter out the mischievous entities and locates cost-effective packet delivery route. The proposed trust model uses a defence scheme known as the clustering technique, which with the dynamism filter out threats linked to an untruthful entity based on node closeness, compatibility of information, and some interactions. It also makes recommendations based on the entity's past performance and views from other objects in the network (direct and indirect trust). The model enhances both the robustness and accuracy in a dynamic MANET environment [127].

The trust computation component in recommendation-based model, shown in figure 5 computes indirect and direct trust value using a bayesian statistical approach. The recommendation manager request, sends, and collect feedbacks for a network entity from a list of acclaiming entity cluster manager. The cluster manager runs the filtering procedure, i.e., receiving the sifted endorsement from various network nodes. The defence scheme send and receive a list from recommending using suggestion request and reply packets. And, Performance evaluation component evaluates the existence of bad-mouthing (the nodes are collude to give negative feedback on the victim in order to lower or destroy its reputation), selfish nodes (selfish nodes use the network and receive services from other nodes but they do not cooperate with other nodes of the network), and ballot stuffing (a number of nodes agree to give positive feedback on an node, often with adversarial intentions [128]) to determine the performance of the network

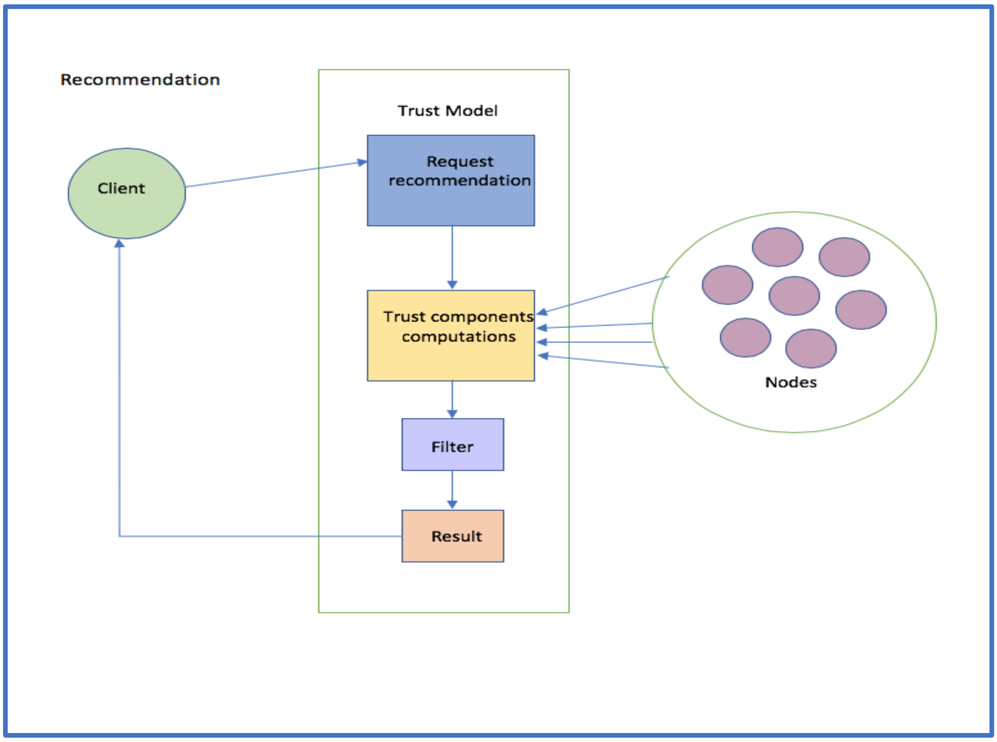


Figure 5: MANET Recommendations, Adapted from [126].

2.10.6 Claim-Based Authentication Trust Models

These are trust models which allow a subject, i.e., an application or a system to authenticate an entity without it disclosing more personal information such as the date of birth and security number. Claim-based authentication has a universal validation approach which enables objects to validate on exterior systems that provide the asking system with claims about the user. In a simple term, the trust model which allows a foreign object in one organization to access the network application or system resources of another firm using their own identities. The relying party or an external system is only required to trust the authentication authority that can validate those claims to enable the entity to be authenticated for specific functions [129].

A claim is a piece of information about an entity which can be a person, a computer, an application, or something else that uniquely identifies a specific user on the network that enables resources or validates request from an entity. The claims are packaged and signed into security tokens which are then sent by the issuer to a relying party. The token contains a set of bytes which expresses information (one or more claims) about an entity. All subjects transacting on the network are given token for identification. The user delivers claims to the application which trust those claims made by the issuer as it already trusts the issuer. Figure 6 shows the components of claimed based identity.

The authentication processes a person or an entity requests some system or application**.** The system or the application then redirects the object to an authentication page of an external system**.** After a successful authentication from the external network, the user is redirected back with some information. The system or the application request the external system to validate the entity**.** If the entity is valid, then it is allowed to get access to the system resources or an application [130].

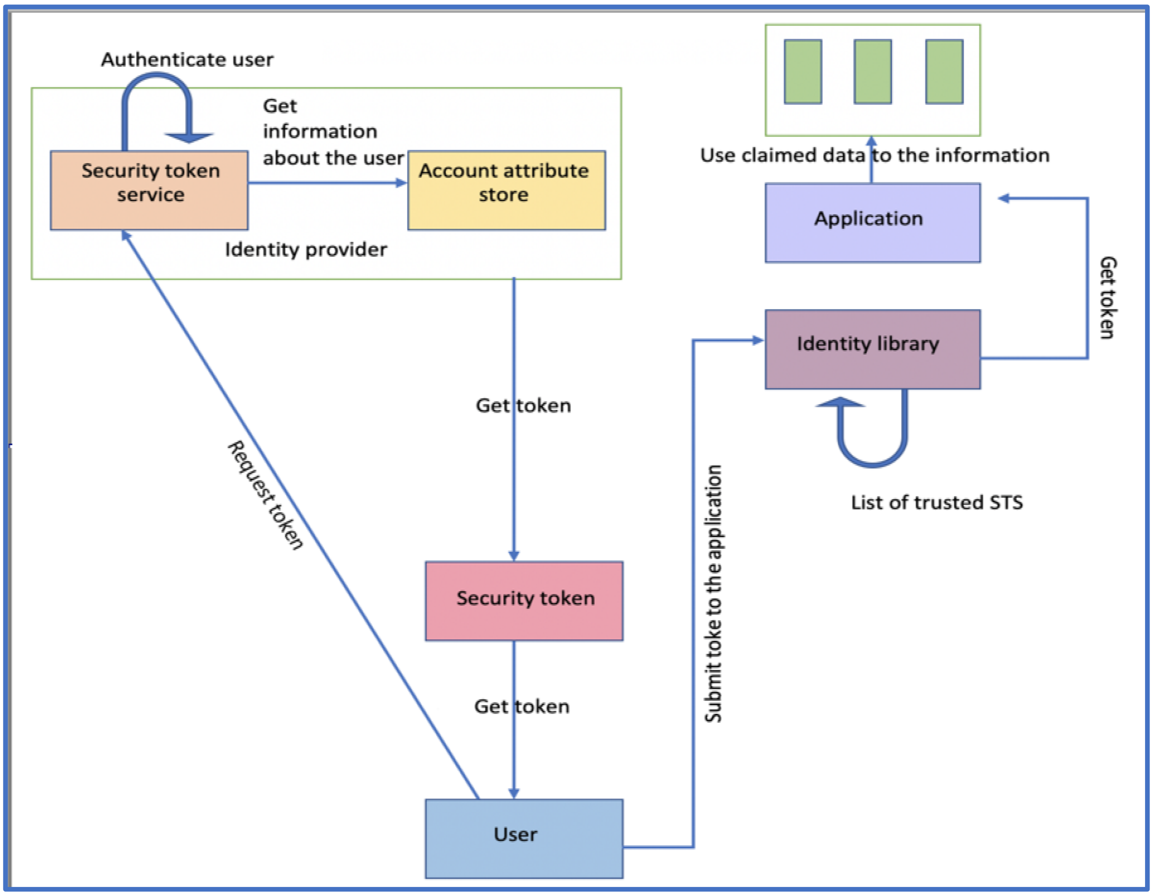


Figure 6: Claimed based Trust model, Adapted from [129].

2.11 Analysis of trust models

All trust models provide the building blocks which interconnects trust-solution used by the public administrator and the customers in various domain in an interoperable, secure, and trustworhty manner. Cryptographic mechanisms been used to authenticate entities and nodes involved in transaction and requests. There is mutual trust between nodes and services involved. Both the consumer and provider of these models can rely on and validate the trustworthiness and authenticity of each service and service-provider carrying out the electronic transaction. Every model has a specific objective; ICAO is to facilitate the worldwide authenticity of travel bearer and document. The ICAO Public Key Directory (PKD) is a central repository for exchanging the information required to authenticate and verification of ePassports between countries. It provides an organized, simple, secure and cost-effective system for sharing validated up-to-date information, the digital signatures, certificates and content of the chip [93].

eIDAS, enhance trust in an electronic transaction in the EU market. The eIDAS is a standard trust model for electronic transactions and identification in the European single market. This trust model regulates electronic signatures, electronic transactions, involved entities, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services [93]. ICAM, manage credential and access and US electronic identity. The FICAM trust model is aligning the Identity Management activities of the US Government. This trust model focuses on assuring the security and privacy of E-Government services, provides Information Sharing Environment ISE Need for Federal PKI [128]. Blockchain, global dematerialised money ("fiduciary" which is a person or a group of persons who holds a legal or ethical relationship of trust with one or more other parties), is a public ledger that makes bitcoin transaction anonymously and securely on the internet. This model is able to record transactions between two entities in an efficient and verifiable way, depending on the peer-to-peer electronic cash system [131].

Claim-based authentication relies on the suggestion made by a trusted entity to authorize an application to access system resources. It allows a subject to authenticate an entity and access to system resources without it disclosing more personal information [132]. All trust models have a different method of evaluating trust of an entity; The recommendation-based trust model, is to recommend the entities the best service and is different from other trust models since it is subjective and recommendation made by other nodes and filters out the mischievous entity as it searches packet delivery route. For instance, it checks the trustworthiness of a recommending entity by examining its closeness to the evaluating node, compatibility of information, and some interactions with the evaluated node. While claim-based authentication model, an entity trusts the claims of an application or system authenticated by a trusted user. The governance and assessment process differ in all models. Each trust model has specific criteria for assessing the service qualities, actual policy, and the trust status. And a different approach for registration, maintenance, and lookup services.

2.11.1 A probabilistic approach

A probabilistic approach deals with a single trust value in a black or white fashion — an agent or source can either be trusted or not — and computes a probability that the agent can be trusted. In such a setting, a higher suggested trust value corresponds to a higher probability that an agent can be trusted. It may add extension of an inference infrastructure that takes into account the trust between the users, and between provenance elements in the system and the users [133], or the focus can be on computing trust for applications containing semantic information such as a bibliography server [90], or a trust system is designed to make community blogs more attack-resistant [134].

2.11.2 A gradual approach

A gradual approach is concerned with the estimation of trust values when the outcome of an action can be positive to some extent, for example when provided information can be right or wrong to some degree, as opposed to being either right or wrong [135] [136]. In a gradual setting, trust values are not interpreted as probabilities: a higher trust value corresponds to a higher trust in an agent, which makes the ordering of trust values a very important factor in such scenarios. Note that in real life, too, trust is often interpreted as a gradual phenomenon: humans do not merely reason in terms of ‘trusting’ and ‘not trusting’, but rather trusting someone ‘very much’ or ‘more or less’. Fuzzy logic is very well-suited to represent such natural language labels which represent vague intervals rather than exact values. For instance, fuzzy linguistic terms are used to specify the trust in agents in a Peer to Peer (P2P) network, and in a social network, respectively. A classic example of trust as a gradual notion can be found in a four-value scale is used to determine the trustworthiness of agents, viz. very trustworthy – trustworthy – untrustworthy – very untrustworthy [17].

The last years have witnessed a rapid increase of gradual trust approaches, ranging from socio-cognitive models (for example implemented by fuzzy cognitive maps, over management mechanisms for selecting good interaction partners on the web or for open and dynamic environments [17]), to representations for use in mobile environments or recommender systems, and general models tailored to semantic web applications. The recommendation, quality, ranking, speed based trust models are all examples of gradual approach.

2.11.3 Direct vs Indirect trust evaluation:

Indirect trust modelling was usually known as (reputation trust modelling). Here humans evaluate trust values themselves through ranking, this kind of trust modelling is vulnerable against some attacks one of them when humans give their services high ranking so many times to rise their business, vice versa humans can give the others services low ranking to defeat the other's business.

Developing direct trust modeling which is a smart system that can evaluate comprehensive trust evaluation is difficult and needs more computing and internet bandwidth resources than indirect trust but it is the evaluation of trust through a system itself it means humans can not alter trust values. Using probabilistic approach and evaluation the trust with direct trust evaluation model will be accurate, secure and trustable [110].

2.12 TMS

The Trust Management System relies on the previously done connections on the UTM for its recommendations. When the evaluation of a UTM will be done by TMS then the recommendation is not subjective. The TMS will search in the database for the service, then recommends the service to the new nodes. It evaluates the trust level of a node by taking into account additional parameters concerning its current context and resource capabilities. Design a functional trust model that takes into account the specific demanding aspects of the assisted service when computing the trust level of a node having accomplished it. Consider all received reports and past interactions in making trust decisions by defining new methods to perform their combination and bypass the underlying attacks. The reports basing on the trustworthiness of nodes as reporting nodes [137].

2.13 Unified Trust Model (UTM)

The unified trust model is like measurement, trust and trustworthiness are critical measurements of a distributed sensing system or a heterogeneous network comprised of sources of information, knowledge, hardware, and software. There is a great deal of work done in proposing digital trust models to ensure trust, security, efficiency, accuracy and simplicity. Those models are employed in social media, peer-to-peer network, distributed network, e-services, robotics, and semantic web [112].

It works between some available services and the users. Each service has its unique properties, which are available for people’s use, and generally operates in the cyber security field. It provides information on the services and recommends the best ones for the users based on their needs depending on the trust models using in the UTM. Most of the times the recommendations are made based on the previous user's opinion “subjective”, and can also be not subjective but evaluated by a Trust Management system [111].

Chapter 3

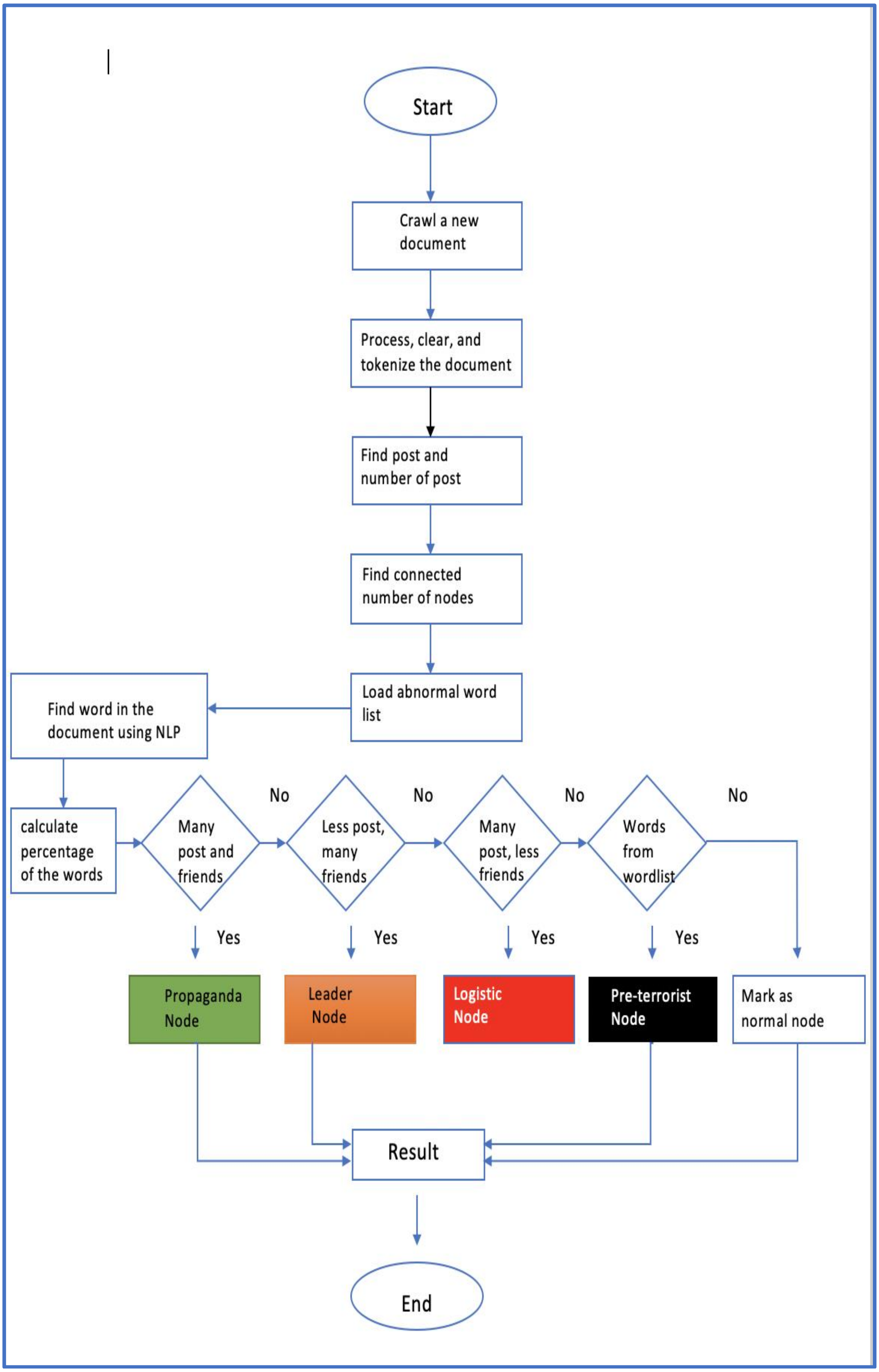
Research Design

3.1 Introduction

Online radicalization, mainly referred to as online youth radicalization because it is mainly directed to youths, is a process by which young people are introduced to extreme ideals of political and religious that contrasts with the contemporary ideals of a country. It can either be violent or non-violent but in recent years violent radicalization has been rising. Young people have been joined in terrorist ideologies using various ways and reasons. Some have been lured based on their experiences, their childhood, and upbringing, using false scriptures, wrong life interpretations, and twisted stories. Others promise youth jobs and better salaries. Social media and other online platforms have become the best places for youths to be trained on extremist issues. Apart from radicalizing young people, the internet has been used to publish radical content, create forums where youths can participate in radical topics among others. As such, the internet has become a hub for young people to become introduced to radical movements with the aim of achieving some missions.

3.2 The online radicalization algorithm

In the first part of this study an algorithm is proposed to monitor human activities on the various communities on the Web (Islamic States groups on Facebook) and analysing the corresponding (public) data.



Flowchart 1: Online Radicalization

1. Information retrieval (IR):

Information retrieval is responsible for searching, finding and collecting the page data first. Then clear data to retrieve the nodes and the posts in the page. Count the number of the posts, connection and location of each node in the network.

Algorithm 1: Information Retrieval

```
for each page in pages do:
raw_data = search (page)     #crawl and find all the data about that page
if (raw_data is not null):
page_text = clear_text (raw_data)   #removing unnecessary from the raw text
post = find_posts (page_text)
post_text = find_text(post)
number_of_posts = count(post)
connected_nodes = find_connected_nodes(post) = number_of_connected_nodes
end if
end for
```

2. Information Extraction (IE):

IE will find each word and sentence in the text. The retrieved data will be structured again into to prepare it for the language processing.

Algorithm 2: Information Extraction:

```
For each post in pages do:
#here we can structure the data we retrieved to tables or lists
        Sentences = find_sentence(post)
        tokens = word_tokenize(post)
        Nouns = find_nouns (tokens)
        Verbs = find_verb(tokens)
End for
```

3. Natural language processing (NLP):

Natural language processing is responsible of creating the world list and compare the structured text to the world list. It can process English, Arabic, Kurdish and Persian languages. It is also responsible to determine the location of the nodes. The location is retrieved in algorithm 1, but in this part the location name will be recognized.

Algorithm 3: Natural language processing (NLP)

```
Initial a list of word_dictionary for [English, Arabic, Kurdish, and Persian]
languages which consist of (words, verbs, locations and etc.)
for each page in pages:
for each word in page_text:
        for each language in word_dictionary:

        if(post_text.contains(word_dictionary[language][word])):
        abnormal_words.add (word)

        if(post_text.contains(word_dictionary[language] [verb])):
        abnormal_verbs(verb)

        if(post_text.contains(word_dictionary[language] [location])):
        abnormal_location(location)

                end for
        end for
  end for
```

4. **Counter Online Radicalization**

Data of the pages gathered through crawlers for collecting data of Facebook pages (how many people liked the page and who are they), as shown in algorithm 4, then all the public data of these people (friends, location, favorite groups) of each of the members of the group was collected via the same algorithm and saved in a database. These data are used to create connectivity graphs of individuals with their connections (friends), monitoring their activity rate in the pages then analysing their posts by text mining .

As first step this the crawler will collect the public data of those nodes (connections and location), after applying the algorithm on collected data, the nodes will be selected, then text-mining processing will be employed and after completing it the graphs will be plotted. It will classify each of those nodes types in the network. Each of those pages has a very wide number of members. Based on the number of activities of the nodes and number of connections of each of the pages the algorithm automatically will point out ten nodes and draw them in a graph. The text mining will work for English, Arabic, Kurdish and Persian texts. The text mining techniques that are merged in this algorithm are:

The algorithm will monitor the radical pages of Islamic States group. It will cluster the node based on them connections and activities rates in the groups. The analysis of the nodes in the algorithm is done according to Richard Barrett report about the structure of Islamic State.

- The green nodes are most active nodes with most activities and most direct links among the other nodes. The nodes with many direct connections and activities they are the ones that working in media for propaganda.

- Orange nodes are nodes that they have many direct connections and less activities, the nodes whom they have many connections but they are less active they are leaders.

- Red nodes are nodes with most activity in the pages and fewer connections, the ones with many activities but less connections they are logistics.

- Black nodes are nodes with most dangerous posts in the pages. They are actually the new affected ones (pre-terrorist).

From available information on cyberterrorism, it is evident that a lot of work has been done on identifying and tracking violent and extremist individuals and subgroups on social media, especially Twitter. Information gathered on the subject also show that a lot of work has been conducted on finding connections and activity rates, text mining as well as detecting key individuals through different methods. For example, the Islamic State is known to use Facebook to propagate propaganda and recruitment, Twitter for coordination with Islamic State members and YouTube to show its activities. The first part of this study is dedicated to the identification of nodes used by Islamic State groups on Facebook that are used for recruitment.

Algoithm 4: Counter Online Radicalization

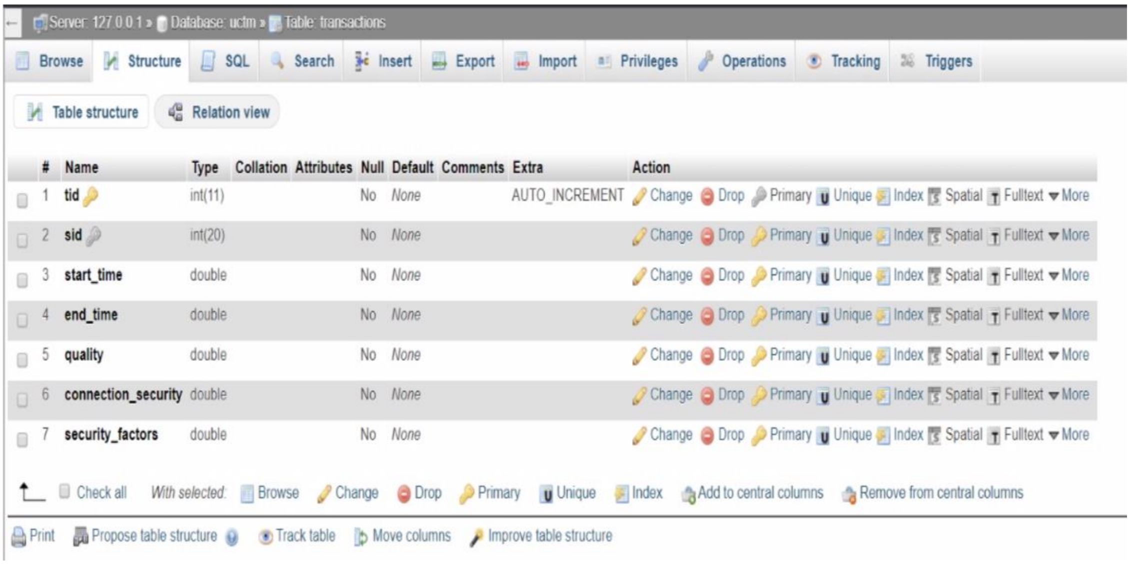
```
Inputs: pages [1-10], compare_words[n], compare_verbs[n]
Variables: public_info (all the public data in the page), post_number,
post_texts[n],
connected_nodes[n], connected_nodes_friend_number, sentences,
 words_list, verb_list, page_type, page_color, MAX_POST_VAL,
MIN_POST_VAL,
MAX_NODE_VAL, MIN_NODE_VAL, MAX_ABNORMAL_WORDS_VAL,
MAX_ABNORMAL_VERBS_VAL
For each page in pages do:
        Public_info = retrieve_info (page)        #by using a web crawler
        Post_texts = parse_document (public_info)
        Number_of_posts [page] = count_posts (public_info)
        Connected_nodes = search_document (public_info)
        Number_of_connected_nodes = count (connected_nodes)

        For each text in post_texts do:
                Sentences = parse (text)
                Words_list = tokenize (sentences)
                noun_list = noun_filter (sentences)
                Verb_list = verb_filter (sentences)

                For each word, verb in noun_list, verb_list:
                        If compare_words.contains(word)
                                Abnormal_words.append (word)
                        if compare_verbs.contains(word) :
                                abnormal_verbs.apend (verb)
                End for
        End for
        If(number_of_posts[page] > MAX_POST_VAL and connected_nodes >
MAX_NODE_VAL):
                Page_type [page] = ‘propaganda page’
                Color [page] = ‘green’
        if(number_of_posts[page] > MAX_POST_VAL and connected_nodes <
MIN_NODE_VAL):
                page_type [page] = ‘logistic page’
                page_color [page] = ‘red’
        If(number_of_posts[page] < MIN_POST_VAL and connected_nodes >
MAX_NODE_VAL):
                Page_type [page] = ‘leader page’
                Page_color [page] = ‘orange’
        If(abnormal_words > MAX_ABNORMAL_WORDS_VAL or
abnormal_verbs > MAX_ABNORMAL_VERBS_VAL ):
                Page_type [page] = ‘danger page’
                Page_color [page] = ‘black’
```

3.3 UCTM Algorithm

The UCTM algorithm consists of different trust models like speed, security, accuracy and recommendation. The user gets recommendations about trusted service list contains speed, accuracy and security value from the stored data in the TMS. The recommendation is done only if it is secure, quick and accurate service. If will prioritize and recommend the services based on the values of the trust models. The database schema of the UCTM is shown in figure 7.



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	tid	int(11)			No	None		AUTO_INCREMENT	Change Drop Primary Unique Index Spatial Fulltext More
□	2	sid	int(20)			No	None			Change Drop Primary Unique Index Spatial Fulltext More
□	3	start_time	double			No	None			Change Drop Primary Unique Index Spatial Fulltext More
□	4	end_time	double			No	None			Change Drop Primary Unique Index Spatial Fulltext More
□	5	quality	double			No	None			Change Drop Primary Unique Index Spatial Fulltext More
□	6	connection_security	double			No	None			Change Drop Primary Unique Index Spatial Fulltext More
□	7	security_factors	double			No	None			Change Drop Primary Unique Index Spatial Fulltext More

Figure 7: Database Schema

1. The Speed based trust model

The speed based trust model measure the time that service needs to complete a specific task. For each interaction between node and service, the TMS will calculate the speed.

$$Speed(s) = \left(\sum_{t=0}^{i} end\ time\ (t) - start\ time\ (t)\right)/i \qquad (1)$$

It will select transmitting time and response time. The speed will be calculated by start and end time of a transaction. (t) is time and (i) is the iteration. Figure 8 shows a sample of nodes and services (s) using the speed trust model.

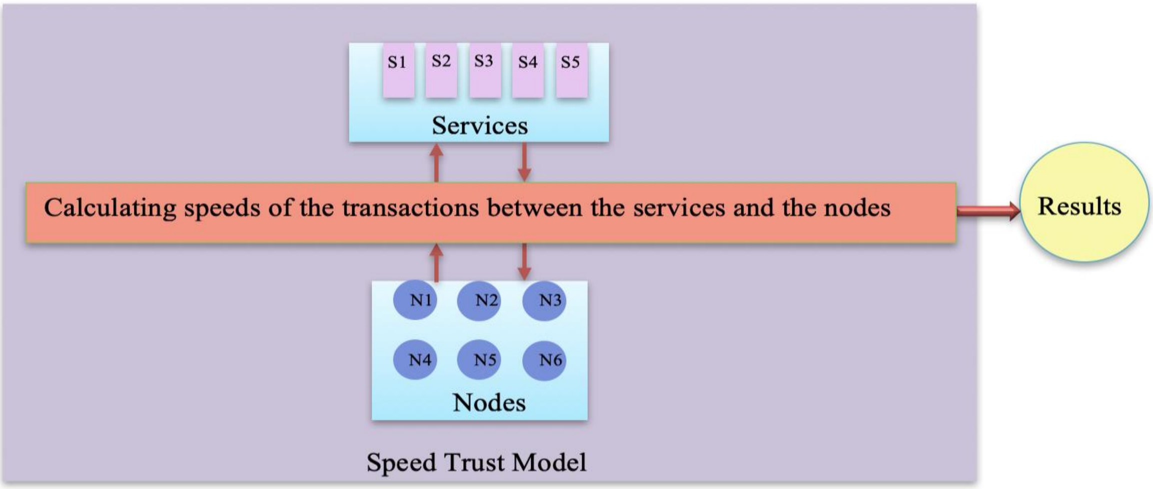

S1
S2
S3
S4
S5
Services
Calculating speeds of the transactions between the services and the nodes
Results
N1
N2
N3
N4
N5
N6
Nodes
Speed Trust Model

Figure 8: Speed measurement in the UCTM

```
Algorithm 5: The Speed
Inputs: services[n], transactions[n]
Variables: start_time, end_time, performance, speed
For each s, t in services, transactions do:
        Throughput = evaluate_transfering_rate(t)
        Performance = end_time(t) – start_time(t)
        Speed[s] = calculate (performance, throughput)
        Save_value(speed[s])
End for
```

2. The Accuracy based trust model

The accuracy is based on interruption rate in the connection.

$$Accuracy(s) = \sum_{t=0}^{i} accuracy\,\frac{ti}{i} \qquad (2)$$

It calculates the reputation, trust worthiest and risk as shown in figure 9. For each interaction (i) between the node and the service, it will calculate the interruption of transactions (t) and compare it to the actual number of transactions of the services (s) in the connection.

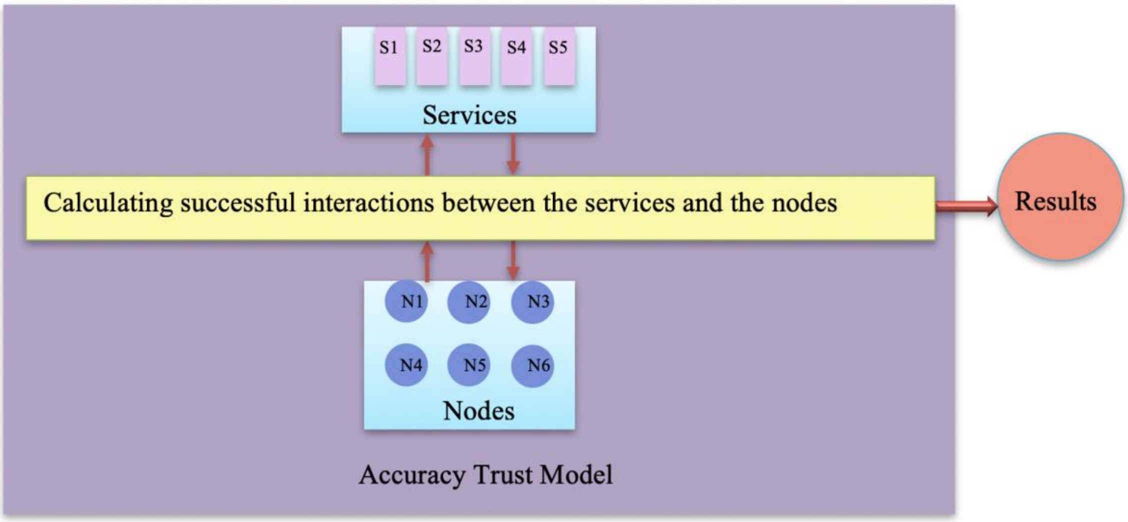

S1
S2
S3
S4
S5
Services
Calculating successful interactions between the services and the nodes
Results
N1
N2
N3
N4
N5
N6
Nodes
Accuracy Trust Model

Figure 9: Accuracy measurement in the UCTM

```
Algorithm 6: The Accuracy
Inputs: services[n], transactions[n]
Variables: accuracy, advertised x accuracy, evuated_accuracy(actual_accuracy)
For each s, t in services, transactions do:
        Advertised_accuracy[s] = get_provided_info(s)
        Actuall_accuracy [s] =evaluate_accuracy(t)
        Accuracy[s] = compare (advertised_accuracy, actual_accuracy)
        Save_value(accuracy[s])
End for
```

3. Security based trust model

For each interaction between nodes and service (s), a security trust model will count the iteration (i) number of malicious in the transaction (t) process.

$$Security(s) = \sum_{t=0}^{i}(connection\ security + security\ Factors\ (t))/i \tag{3}$$

Figure 10 shows a sample of nodes and services using the security trust model.

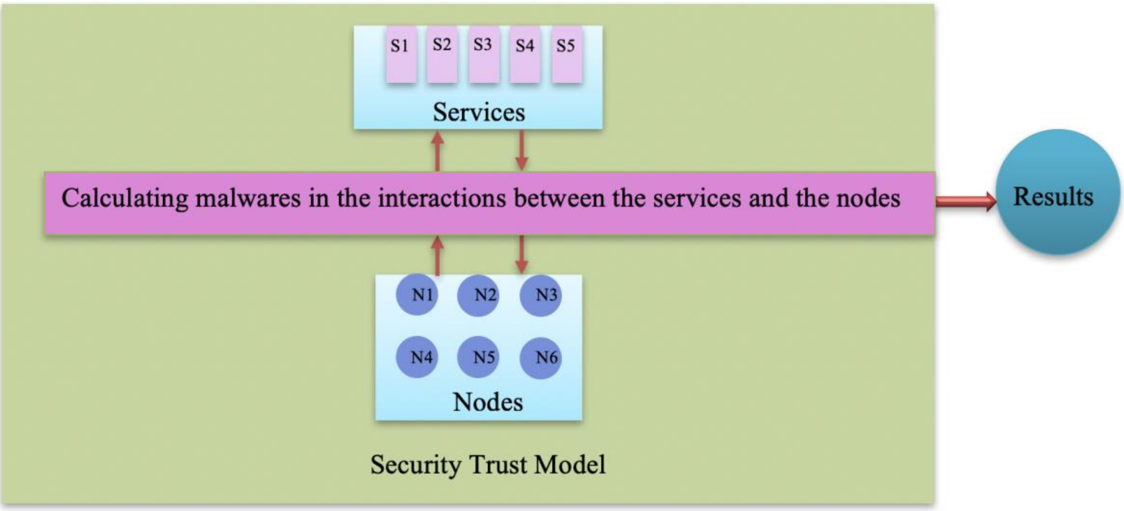

S1
S2
S3
S4
S5
Services
Calculating malwares in the interactions between the services and the nodes
Results
N1
N2
N3
N4
N5
N6
Nodes
Security Trust Model

Figure 10: Security measurement in the UCTM

```
Algorithm 7: The Security
Inputs: services[n], transactions[n]
For each s, t in services, transactions do:
        Security(s) = evaluate(transferred_data[t],
secueity_factors[t])
        Save_value(Security(s))
End for
```

4. The Recommendation based trust model

The recommendation based trust model help filter out the mischievous entities. It is based on the speed, security and accuracy trust models in the UCTM.

$$Recommendatin(s) = \sum_{t=i}^{i} accuracy\ (s) + speed\ (s) + Security\ (s) \qquad (4)$$

The recommendation is not done according to other nodes ranking of the models as it is in previous models. But the TMS will recommend the service (s) to the nodes based on the previous transactions (t) between services and nodes. For each request, the model selects the speed, accuracy and security values and recommend the high ranked models. Where (i) is iteration of the transactions. Figure 11 shows the recommendation trust model of the UCTM.

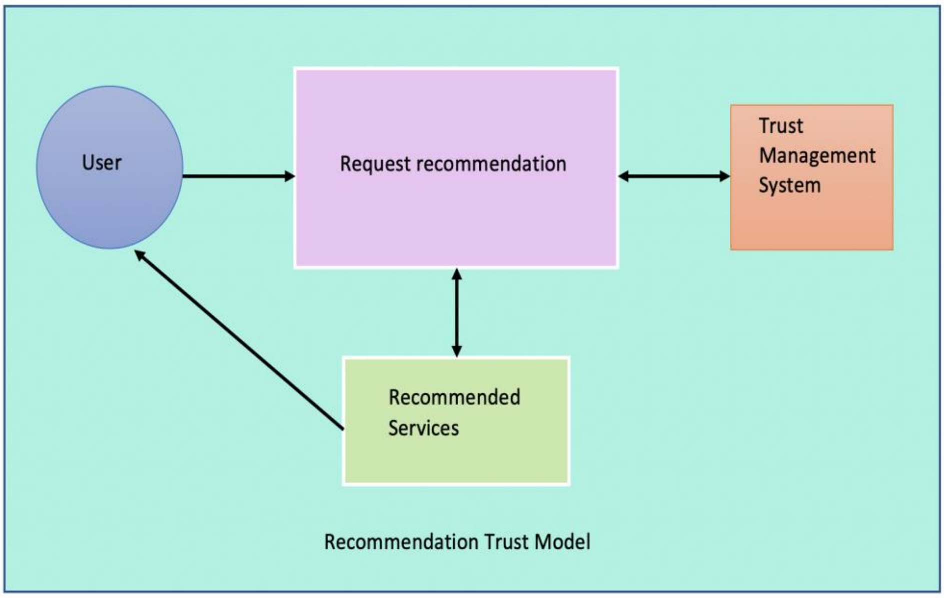


Figure 11: Recommendation measurement in the UCTM

Algorithm 8: The Rcommendation

```
For each s in services do:
        Trust_value[s] = quality[s] + speed[s] + security[s]
        Recommendation [s] = calculate(trust_value[s])
        Save_value(recommendtion[s])
End for
```

The UCTM algorithm starts with creating a service ID for the available services. Each of those services interacts in "interact function" and for each of that interaction that occurred the TMS calculates speed, accuracy, and security values. The TMS will determine which service is trusted based on the result and pass to the recommendation list as shown in figure 12.

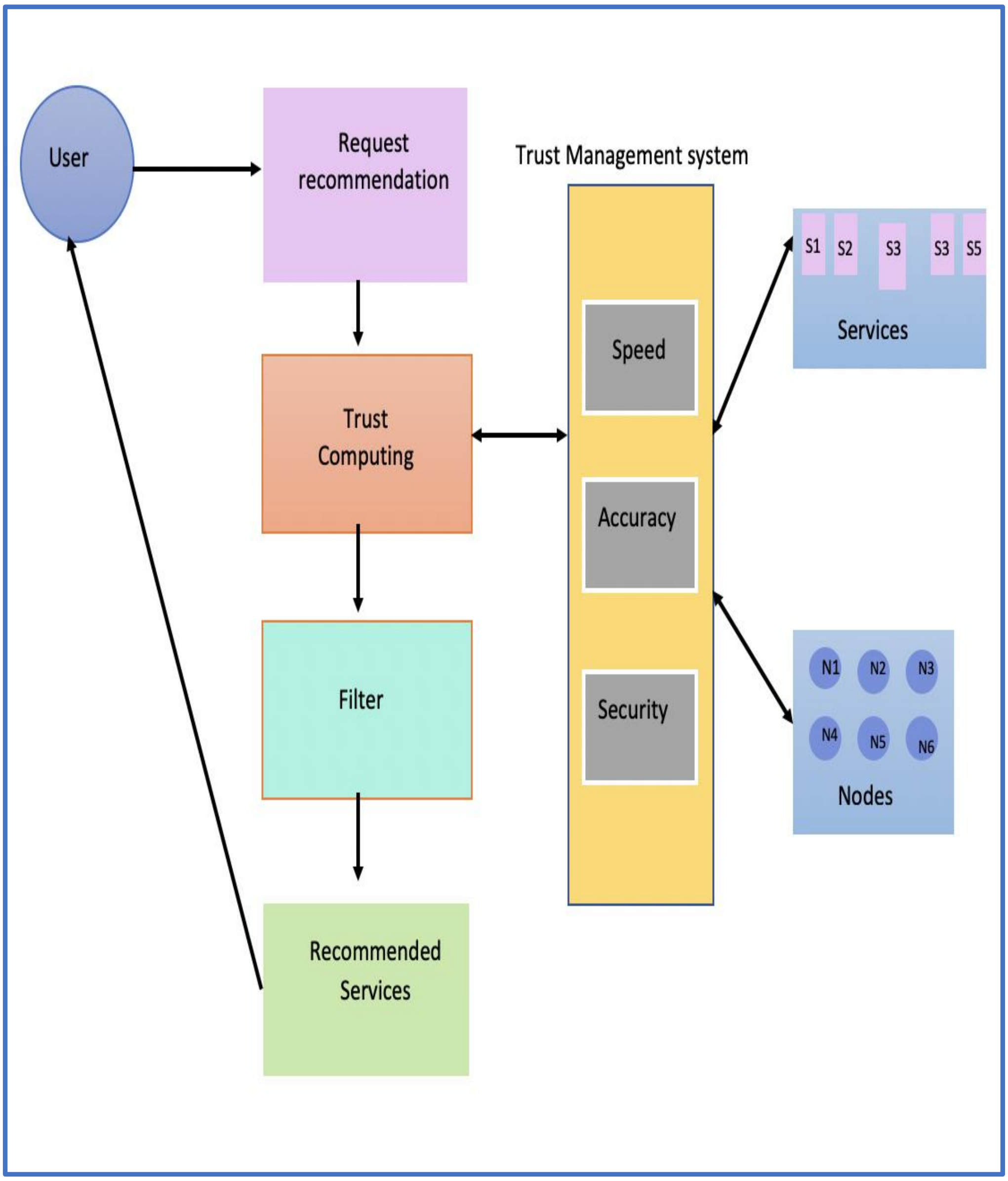


Figure 12: The UCTM structure

Algorithm 9: The UCTM Algorithms

General algorithm for TMS:

```
Inputs: Service[n], Transaction[n]
Variables: quality, speed, security, ranking, advertised_quality, actual_quality, trust_value
For each s, t in services, transactions do:
Advertised_quality = get_provided_info(s)
Actual_quality = evaluate_quality(t)
Quality[s] = compare(advertised_quality, actual_quality)
Save_value(Quality[s])
        Performance = end_time(t) – start_time(t)
        Speed(s) = calculate(performance)
        Save_value(speed(s))
        Security(s) = evaluate(transferred_data[t], secueity_factors)
        Save_value(Security(s))
        Trust_value = quality[s] + speed(s) + security(s)
        Ranking(s) = calculate(trust_value)
        Save_value(ranking(s))
End for
```

3.2.1 The complexity of the UCTM algorithm

Computational complexity is the study of the difficulty of solving computational problems, regarding the required computational resources, such as time and the capacity of the service. To develop a theory of the burden of computational issues, it is necessary to specify precisely what the problem is, what an algorithm is, and what a measure of difficulty is to measure complexity for the UCTM according to its algorithm. The complexity of the UCTM can be evaluated by measuring the complexity of each property or each factor that manage trust in the UCTM. The properties are speed, accuracy, security and recommendation. To evaluate the complexity, we need to assess the complexity of speed, accuracy and security trust models. Since classification, preference, and judgment are not complicated, they are not evaluating or calculate data, but they select and show data being assessed. To calculate the complecity of the

UCTM in this study the complexity (time, capacity) for speed, accuracy and security trust models are measured.

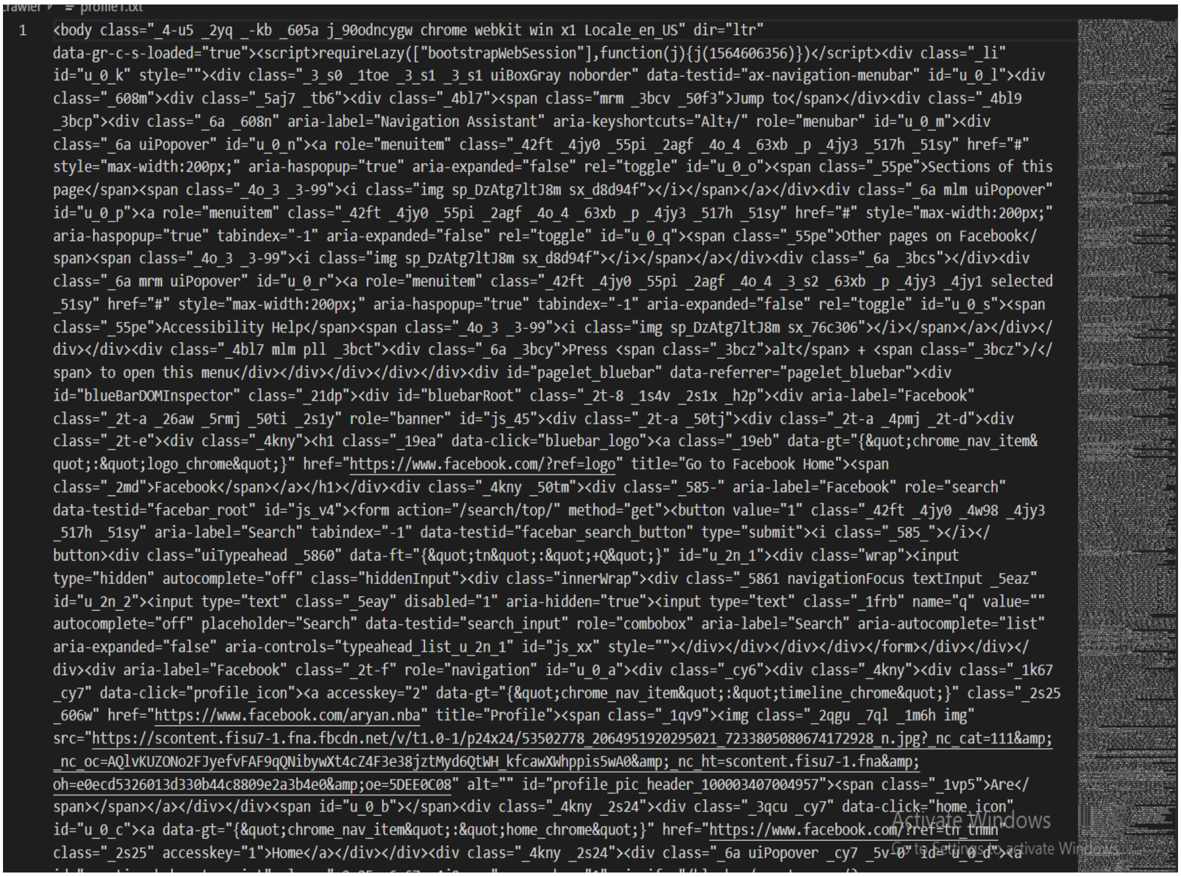
The complexity (time- capacity) for speed, accuracy and security is evaluated. The speed complexity is not affecting the evaluation of the services while working on big data because it just about time to complete the interaction between the node and the service. The security and accuracy complexity (time) will make different while working on big data. For example, having big data will increase the complexity of the security model because it needs to evaluate more packets for security issues. For the accuracy complexity, more data means more time to transfer the data, and it means more interrupt may occur in the transferring. The UCTM will be more complicated as the size of the data goes up, but as long as having a good computing power working on big data will be not a problem.

Chapter 4

Discussion and Result

4.1 Practical part of Online radicalization

In the first part of this study an algorithm is proposed and implemented to collect the data of radical pages of Islamic States group on Facebook and filter the text to target the requirements of the research. First four radical pages is identified and then the proposed algorithm will collect the data of those nodes that are members of the pages (connections, posts and locations) for three months, then ten most active nodes (Facebook profile) been selected between all the members of each page. Figure 13 shows the collected text of identified pages before any process.



```
<body class="_4-u5 _2yq _-kb _605a j_90odncygw chrome webkit win x1 Locale_en_US" dir="ltr"
data-gr-c-s-loaded="true"><script>requireLazy(["bootstrapWebSession"],function(j){j(1564606356)})</script><div class="_li"
id="u_0_k" style=""><div class="_3_s0 _1toe _3_s1 _3_s1 uiBoxGray noborder" data-testid="ax-navigation-menubar" id="u_0_l"><div
class="_608m"><div class="_5aj7 _tb6"><div class="_4bl7"><span class="mrm _3bcv _50f3">Jump to</span></div><div class="_4bl9
_3bcp"><div class="_6a _608n" aria-label="Navigation Assistant" aria-keyshortcuts="Alt+/" role="menubar" id="u_0_m"><div
class="_6a uiPopover" id="u_0_n"><a role="menuitem" class="_42ft _4jy0 _55pi _2agf _4o_4 _63xb _p _4jy3 _517h _51sy" href="#"
style="max-width:200px;" aria-haspopup="true" aria-expanded="false" rel="toggle" id="u_0_o"><span class="_55pe">Sections of this
page</span><span class="_4o_3 _3-99"><i class="img sp_DzAtg7ltJ8m sx_d8d94f"></i></span></a></div><div class="_6a mlm uiPopover"
id="u_0_p"><a role="menuitem" class="_42ft _4jy0 _55pi _2agf _4o_4 _63xb _p _4jy3 _517h _51sy" href="#" style="max-width:200px;"
aria-haspopup="true" tabindex="-1" aria-expanded="false" rel="toggle" id="u_0_q"><span class="_55pe">Other pages on Facebook</
span><span class="_4o_3 _3-99"><i class="img sp_DzAtg7ltJ8m sx_d8d94f"></i></span></a></div><div class="_6a _3bcs"></div><div
class="_6a mrm uiPopover" id="u_0_r"><a role="menuitem" class="_42ft _4jy0 _55pi _2agf _4o_4 _3_s2 _63xb _p _4jy3 _4jy1 selected
_51sy" href="#" style="max-width:200px;" aria-haspopup="true" tabindex="-1" aria-expanded="false" rel="toggle" id="u_0_s"><span
class="_55pe">Accessibility Help</span><span class="_4o_3 _3-99"><i class="img sp_DzAtg7ltJ8m sx_76c306"></i></span></a></div></
div></div><div class="_4bl7 mlm pll _3bct"><div class="_6a _3bcy">Press <span class="_3bcz">alt</span> + <span class="_3bcz">/</
span> to open this menu</div></div></div></div></div><div id="pagelet_bluebar" data-referrer="pagelet_bluebar"><div
id="blueBarDOMInspector" class="_21dp"><div id="bluebarRoot" class="_2t-8 _1s4v _2s1x _h2p"><div aria-label="Facebook"
class="_2t-a _26aw _5rmj _50ti _2s1y" role="banner" id="js_45"><div class="_2t-a _50tj"><div class="_2t-a _4pmj _2t-d"><div
class="_2t-e"><div class="_4kny"><h1 class="_19ea" data-click="bluebar_logo"><a class="_19eb" data-gt="{&quot;chrome_nav_item&
quot;:&quot;logo_chrome&quot;}" href="https://www.facebook.com/?ref=logo" title="Go to Facebook Home"><span
class="_2md">Facebook</span></a></h1></div><div class="_4kny _50tm"><div class="_585-" aria-label="Facebook" role="search"
data-testid="facebar_root" id="js_v4"><form action="/search/top/" method="get"><button value="1" class="_42ft _4jy0 _4w98 _4jy3
_517h _51sy" aria-label="Search" tabindex="-1" data-testid="facebar_search_button" type="submit"><i class="_585_"></i></
button><div class="uiTypeahead _5860" data-ft="{&quot;tn&quot;:&quot;+Q&quot;}" id="u_2n_1"><div class="wrap"><input
type="hidden" autocomplete="off" class="hiddenInput"><div class="innerWrap"><div class="_5861 navigationFocus textInput _5eaz"
id="u_2n_2"><input type="text" class="_5eay" disabled="1" aria-hidden="true"><input type="text" class="_1frb" name="q" value=""
autocomplete="off" placeholder="Search" data-testid="search_input" role="combobox" aria-label="Search" aria-autocomplete="list"
aria-expanded="false" aria-controls="typeahead_list_u_2n_1" id="js_xx" style=""></div></div></div></div></form></div></div></
div><div aria-label="Facebook" class="_2t-f" role="navigation" id="u_0_a"><div class="_cy6"><div class="_4kny"><div class="_1k67
_cy7" data-click="profile_icon"><a accesskey="2" data-gt="{&quot;chrome_nav_item&quot;:&quot;timeline_chrome&quot;}" class="_2s25
_606w" href="https://www.facebook.com/aryan.nba" title="Profile"><span class="_1qv9"><img class="_2qgu _7ql _1m6h img"
src="https://scontent.fisu7-1.fna.fbcdn.net/v/t1.0-1/p24x24/53502778_2064951920295021_7233805080674172928_n.jpg?_nc_cat=111&amp;
_nc_oc=AQlvKUZONo2FJyefvFAF9qQNibywXt4cZ4F3e38jztMyd6QtWH_kfcawXWhppis5wA0&amp;_nc_ht=scontent.fisu7-1.fna&amp;
oh=e0ecd5326013d330b44c8809e2a3b4e0&amp;oe=5DEE0C08" alt="" id="profile_pic_header_100003407004957"><span class="_1vp5">Are</
span></span></a></div></div><span id="u_0_b"></span><div class="_4kny _2s24"><div class="_3qcu _cy7" data-click="home_icon"
id="u_0_c"><a data-gt="{&quot;chrome_nav_item&quot;:&quot;home_chrome&quot;}" href="https://www.facebook.com/?ref=tn_tnmn"
class="_2s25" accesskey="1">Home</a></div></div><div class="_4kny _2s24"><div class="_6a uiPopover _cy7 _5v-0" id="u_0_d"><a
```

Figure 13: Data of the Facebook page before processing

Each of those pages has a very wide number of members on Facebook. Many of the nodes are members of all the radical pages at the same time, for example some of the media nodes are active in all the pages. Based on the number of activities of the members, number of connections of each of the nodes and content of them posts the algorithm will point out ten nodes and draw them in a graph. The script of the algorithm is working for English, Arabic, Kurdish and Persian texts. Fig 14, Shows the number of the members in each page.

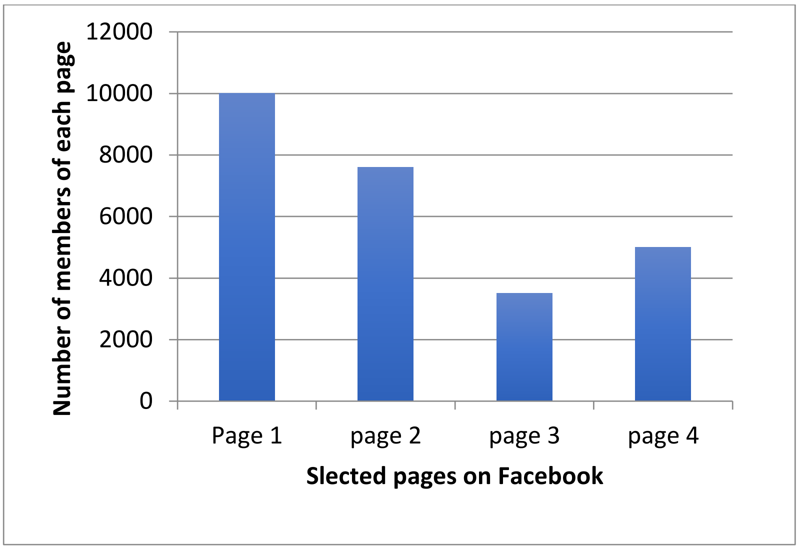


Figure 14: Number of members of four radical pages on Facebook

Fig 15, Shows the activities of each node in the pages. Each of those active nodes is recognized for them posts and activity rates in the pages. Fig 16 shows the connections of the nodes in the pages.

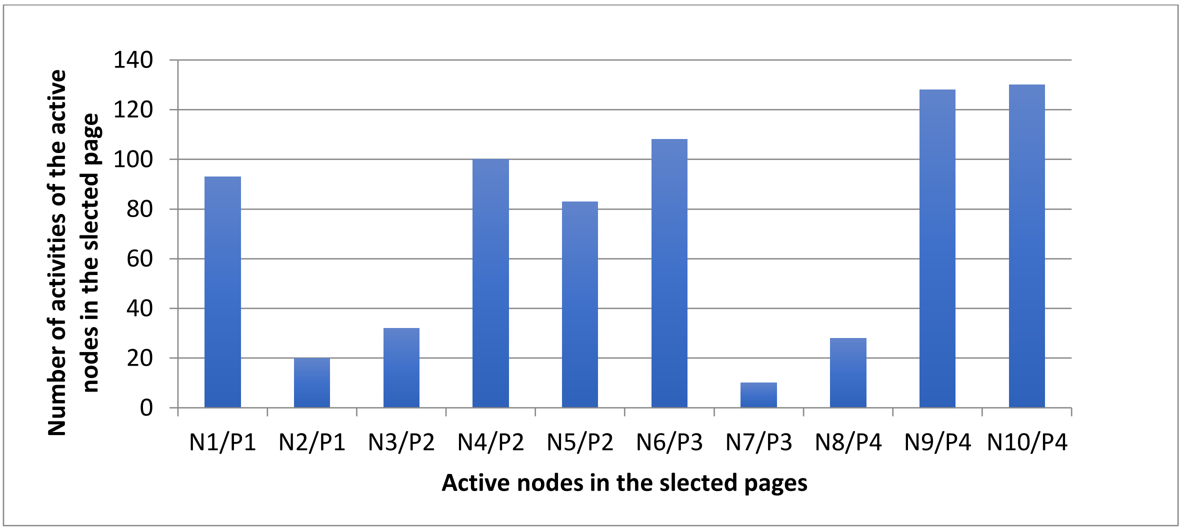


Figure 15: The number of activities of a Node in the Four Radical Pages

Table 1 shows the location of each node based on the collected data.

Table 1: Location of each node in the network.

Nodes	**Location**
Node 1	Europe
Node 2	Syria
Node 3	Syria
Node 4	Iraq
Node 5	Europe
Node 6	Iraq
Node 7	Pakistan
Node 8	Iraq
Node 9	Syria
Node 10	Turkey

Fig 16 shows the number of friends each of the nodes has. This is important to show each nodes impact on people connected to them directly.

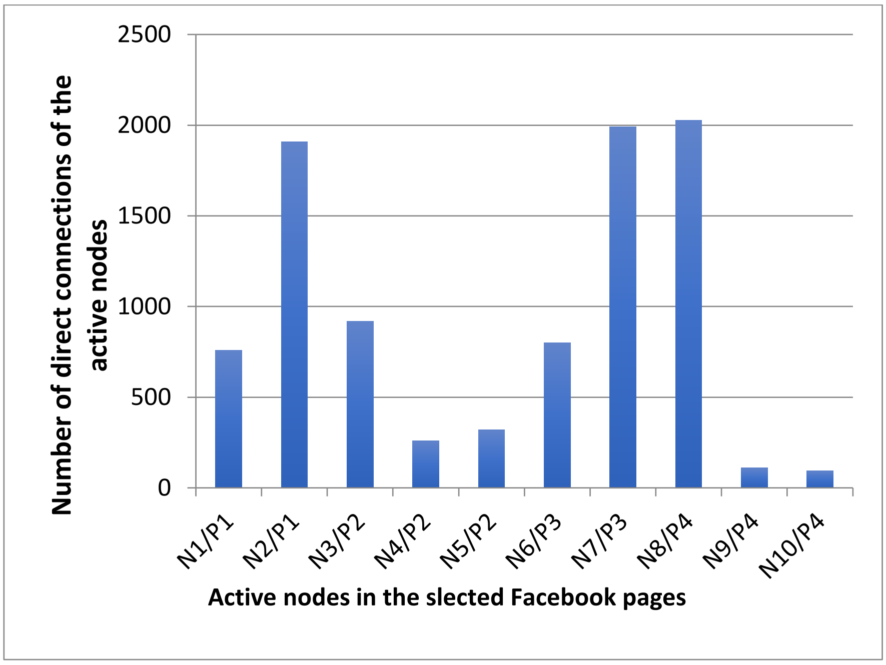
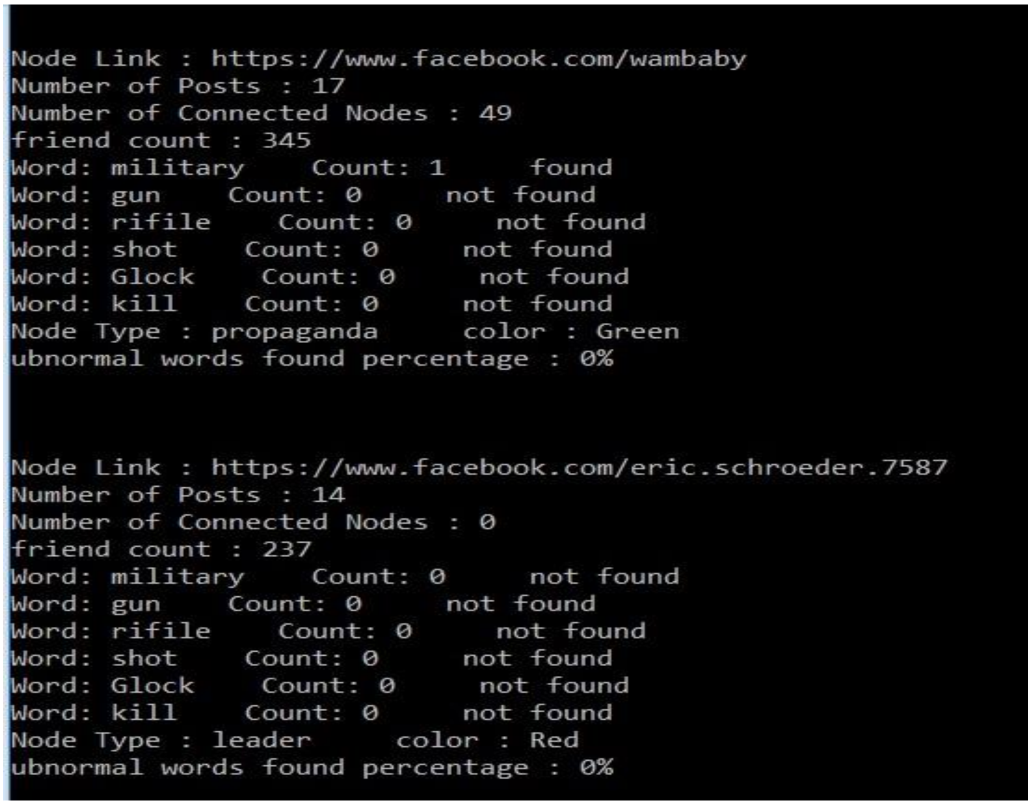


Figure 16: Number of direct connection of each node in the pages



```
Node Link : https://www.facebook.com/wambaby
Number of Posts : 17
Number of Connected Nodes : 49
friend count : 345
Word: military     Count: 1      found
Word: gun     Count: 0      not found
Word: rifile     Count: 0      not found
Word: shot     Count: 0      not found
Word: Glock     Count: 0      not found
Word: kill     Count: 0      not found
Node Type : propaganda      color : Green
ubnormal words found percentage : 0%


Node Link : https://www.facebook.com/eric.schroeder.7587
Number of Posts : 14
Number of Connected Nodes : 0
friend count : 237
Word: military     Count: 0      not found
Word: gun     Count: 0      not found
Word: rifile     Count: 0      not found
Word: shot     Count: 0      not found
Word: Glock     Count: 0      not found
Word: kill     Count: 0      not found
Node Type : leader      color : Red
ubnormal words found percentage : 0%
```

Figure 17: The node clustering with the proposed algorithm

As the result of the algorithm on this case study of monitoring four radical pages of Islamic States group. The result shows that one of the nodes is identified as pre-terrorist in the pages. Figures 17 and 18 show the clustered node based on them connections and activities rates in the groups.

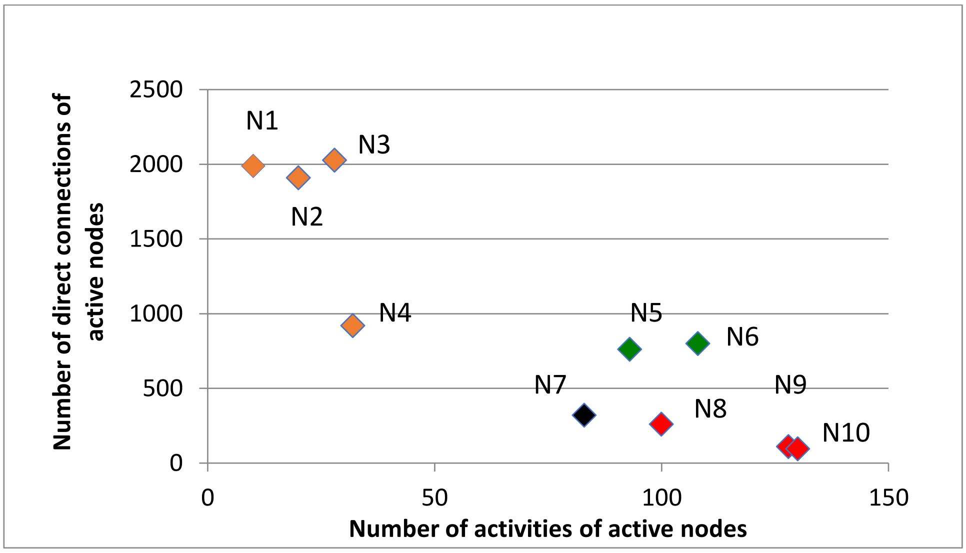


Figure 18: Nodes types

Figures 19 is a graph shows the analysis of the ten nodes in the group with their connections, activity rates and Locations. The nodes are analysed and clustered into media, leaders, logistics and pre-terrorist nodes. In the figure N5 and N7 are based in Europe, Node N1, N2 and N8 are in Syria, N9 is in Turkye, N3 is in Pakistan, N6, N10 and N4 are in Iraq.

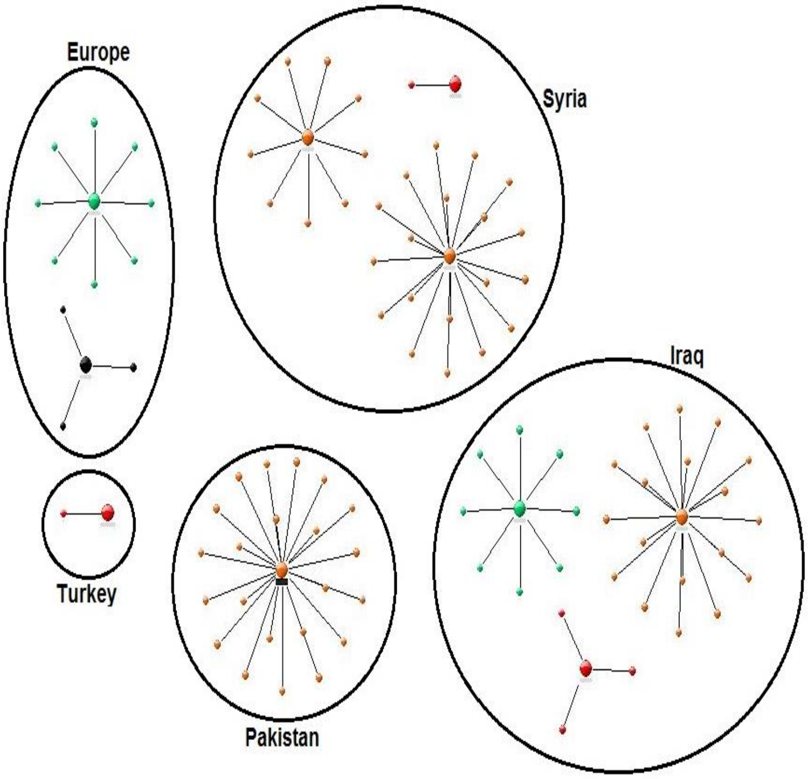


Figure 19: Node Analysis graph

4.2 practical UCTM

In the second part of this study an UCTM algorithm with TMS is proposed. Based on our exhausative review there is not any UCTM to calculate the trustworthy of the services and systems in the way this UCTM does it. The proposed UCTM is to calculate trustworthiness of entities based on history, context, and platform integrity measurement. It combines of different trust models and based on direct evaluating for the service using TMS. It evaluates the service based on the values of the trust models in order to increase trust in the process. Trust models, which are in the UCTM, are speed, security, accuracy and ranking, comparing, and recommendation models are all merged into recommendation model. Each trust model can also be used as a seperate model based on users requests. The UCTM is applied on two different

Cases on surface web and darkweb to prove the unification of the models on all the levels of the Internet.

4.2.1 Case Study 1: UCTM on Surface web – Online banking

In banking system, trust has significant role, trust means one side feels sure of the truth of other side and considers it they are honest and feel free to express feeling. Trust has role in being effective and reliable and feels comfortable to communicate with the other side. Consequently, trust is reason to continue using internet banking because when customers trust the bank and the online transaction they will widely use online banking.

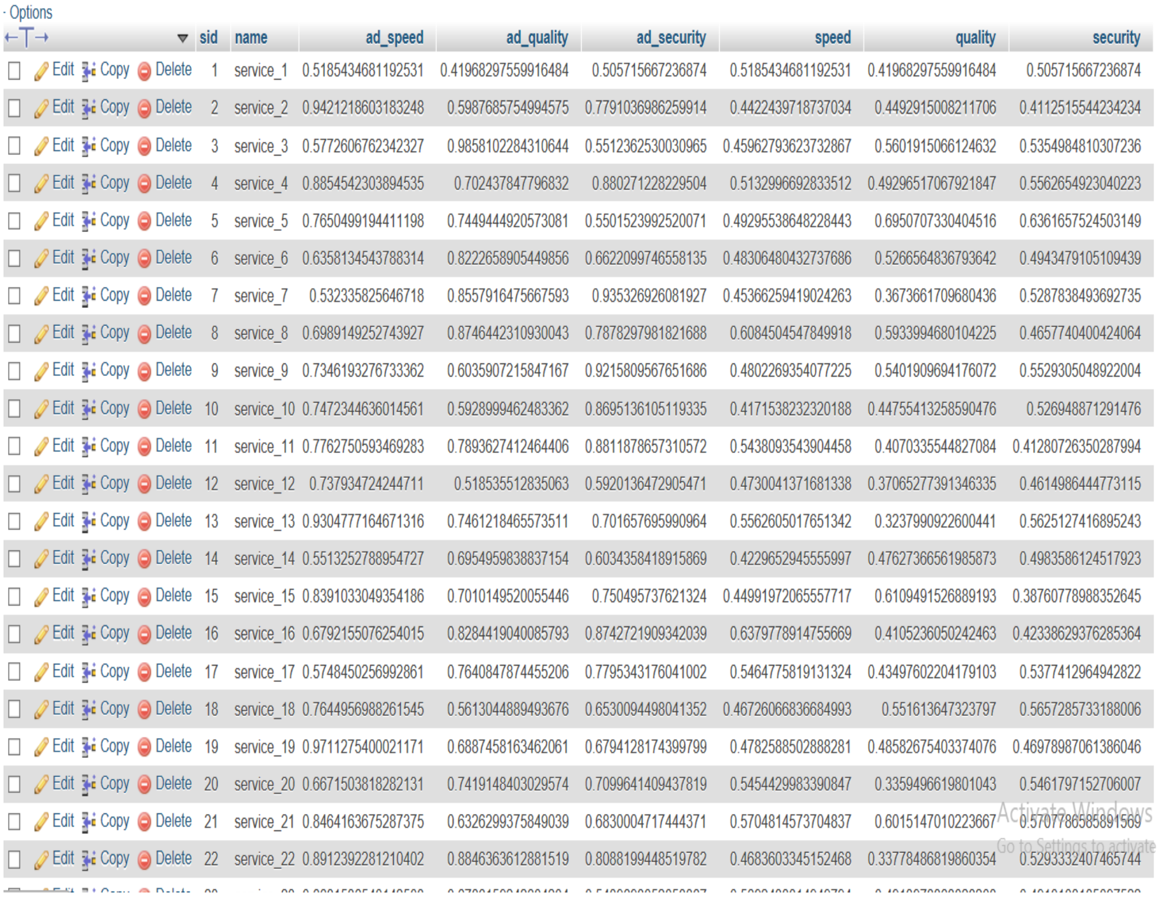
Unified trust model is different trust models that unified together would be used to calculate the trust level of each party and to know the accuracy of the trust computation that is a major issue of the environment. The vulnerability of the system should be identified in order to know which key of solution to use and control the vulnerability and find out which conditions affect the trust calculation mechanism and how much the model is able to deal with different scenarios.

In online banking system, the security is primary concern for the customer and security used to increase and monitor integrity of the system. The data security between the customer and the bank web page are handled through security protocol that called secure socket layer, that provides data encryption, server authentication, and message integrity for an Internet connection and security mechanism that called security “handshake” used to initiate the connection.

UCTM that proposed in the second part of this study, it is build on top of several trust models for the purpose of direct evaluating of speed, security and accuracy of the services using direct evaluation from the UCTM. It is comparatively evaluating some online banking systems and rate them to make users use the trusted services.

The UCTM is proposed to calculate trustworthiness of entities based on history, context, and platform integrity measurement. It combines of different trust models and based on direct evaluating for the service using TMS. It evaluates the service based on the values of the trust models in order to increase trust in the transaction and saving money in online banking system. Trust models, which are in the UCTM, are speed, security, accuracy and recommendation models. It recommends the bank for the customer based on the rates of trust models in the

UCTM. The banks are compared based on the ranking values which is contains the summation of the values of speed of the transactions, security of the transaction from unclear packets, and accuracy of the rate of interruption in the connection. The UCTM is precise because the malicious nodes would not participate in ranking. Moreover, UCTM in online banking system is essential because customer will select the bank that has recommended for them. This will increase trust of the users of the online banking systems.



Options

←T→			▼	sid	name	ad_speed	ad_quality	ad_security	speed	quality	security
□	Edit	Copy	Delete	1	service_1	0.5185434681192531	0.41968297559916484	0.505715667236874	0.5185434681192531	0.41968297559916484	0.505715667236874
□	Edit	Copy	Delete	2	service_2	0.9421218603183248	0.5987685754994575	0.7791036986259914	0.4422439718737034	0.4492915008211706	0.4112515544234234
□	Edit	Copy	Delete	3	service_3	0.5772606762342327	0.9858102284310644	0.5512362530030965	0.45962793623732867	0.5601915066124632	0.5354984810307236
□	Edit	Copy	Delete	4	service_4	0.8854542303894535	0.702437847796832	0.880271228229504	0.5132996692833512	0.49296517067921847	0.5562654923040223
□	Edit	Copy	Delete	5	service_5	0.7650499194411198	0.7449444920573081	0.5501523992520071	0.49295538648228443	0.6950707330404516	0.6361657524503149
□	Edit	Copy	Delete	6	service_6	0.6358134543788314	0.8222658905449856	0.6622099746558135	0.48306480432737686	0.5266564836793642	0.4943479105109439
□	Edit	Copy	Delete	7	service_7	0.532335825646718	0.8557916475667593	0.935326926081927	0.45366259419024263	0.3673661709680436	0.5287838493692735
□	Edit	Copy	Delete	8	service_8	0.6989149252743927	0.8746442310930043	0.7878297981821688	0.6084504547849918	0.5933994680104225	0.4657740400424064
□	Edit	Copy	Delete	9	service_9	0.7346193276733362	0.6035907215847167	0.9215809567651686	0.4802269354077225	0.5401909694176072	0.5529305048922004
□	Edit	Copy	Delete	10	service_10	0.7472344636014561	0.5928999462483362	0.8695136105119335	0.4171538232320188	0.44755413258590476	0.526948871291476
□	Edit	Copy	Delete	11	service_11	0.7762750593469283	0.7893627412464406	0.8811878657310572	0.5438093543904458	0.4070335544827084	0.41280726350287994
□	Edit	Copy	Delete	12	service_12	0.737934724244711	0.518535512835063	0.5920136472905471	0.4730041371681338	0.37065277391346335	0.4614986444773115
□	Edit	Copy	Delete	13	service_13	0.9304777164671316	0.7461218465573511	0.701657695990964	0.5562605017651342	0.3237990922600441	0.5625127416895243
□	Edit	Copy	Delete	14	service_14	0.5513252788954727	0.6954959838837154	0.6034358418915869	0.4229652945555997	0.47627366561985873	0.4983586124517923
□	Edit	Copy	Delete	15	service_15	0.8391033049354186	0.7010149520055446	0.750495737621324	0.44991972065557717	0.6109491526889193	0.38760778988352645
□	Edit	Copy	Delete	16	service_16	0.6792155076254015	0.8284419040085793	0.8742721909342039	0.6379778914755669	0.4105236050242463	0.42338629376285364
□	Edit	Copy	Delete	17	service_17	0.5748450256992861	0.7640847874455206	0.7795343176041002	0.5464775819131324	0.43497602204179103	0.5377412964942822
□	Edit	Copy	Delete	18	service_18	0.7644956988261545	0.5613044889493676	0.6530094498041352	0.46726066836684993	0.551613647323797	0.5657285733188006
□	Edit	Copy	Delete	19	service_19	0.9711275400021171	0.6887458163462061	0.6794128174399799	0.4782588502888281	0.48582675403374076	0.46978987061386046
□	Edit	Copy	Delete	20	service_20	0.6671503818282131	0.7419148403029574	0.7099641409437819	0.5454429983390847	0.3359496619801043	0.5461797152706007
□	Edit	Copy	Delete	21	service_21	0.8464163675287375	0.6326299375849039	0.6830004717444371	0.5704814573704837	0.6015147010223667	0.5707786585891569
□	Edit	Copy	Delete	22	service_22	0.8912392281210402	0.8846363612881519	0.8088199448519782	0.4683603345152468	0.33778486819860354	0.5293332407465744

Activate Windows
Go to Settings to activate W

Figure 20: The result of the UCTM algorithm on online banking systems in the database

Figure 20. Shows the results of evaluating ten different online banking systems using the UCTM. Each bank has number of transaction data, which it consists of at least 5000 transactions.

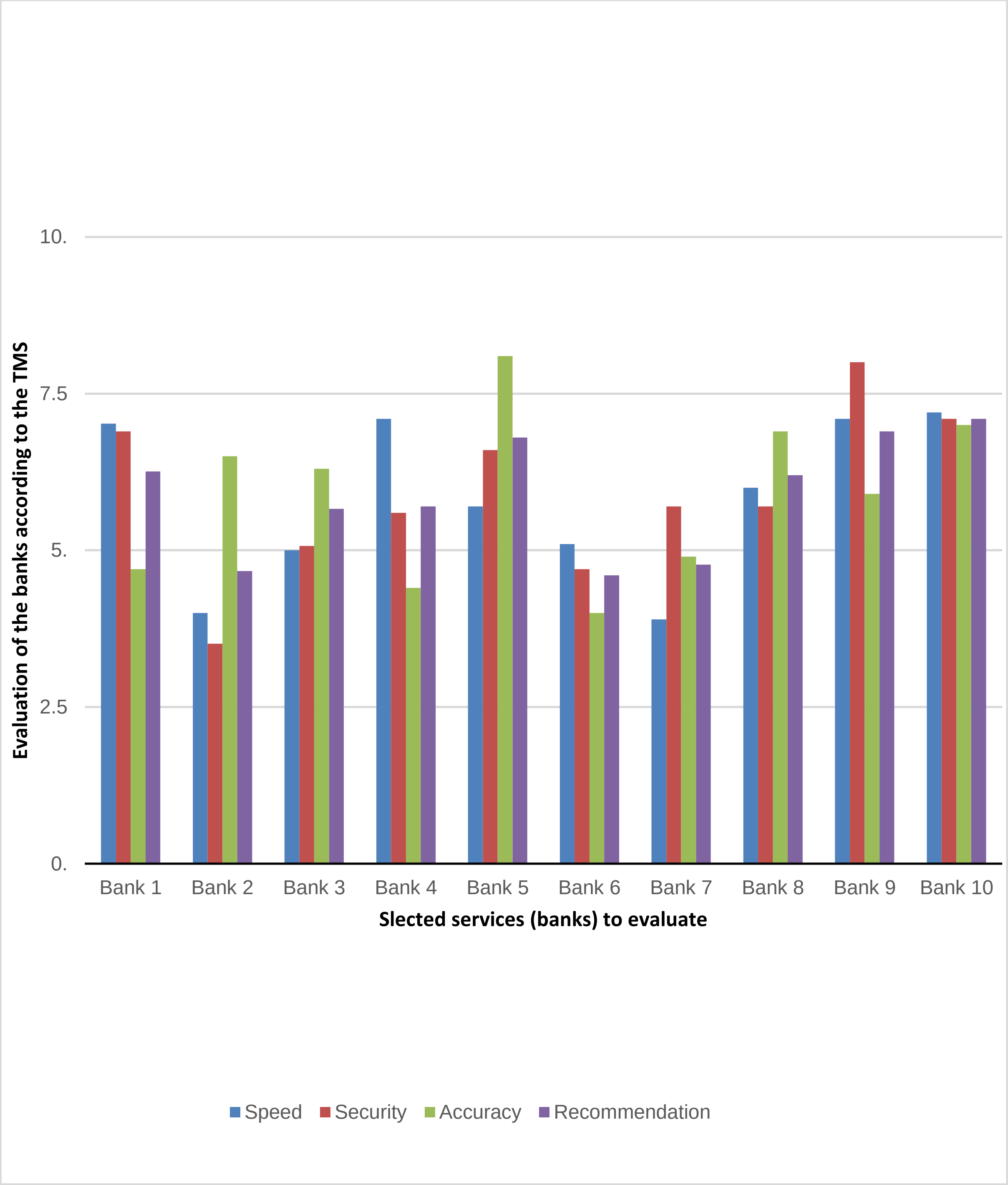


Figure 21: The trust values for each bank according to TMS

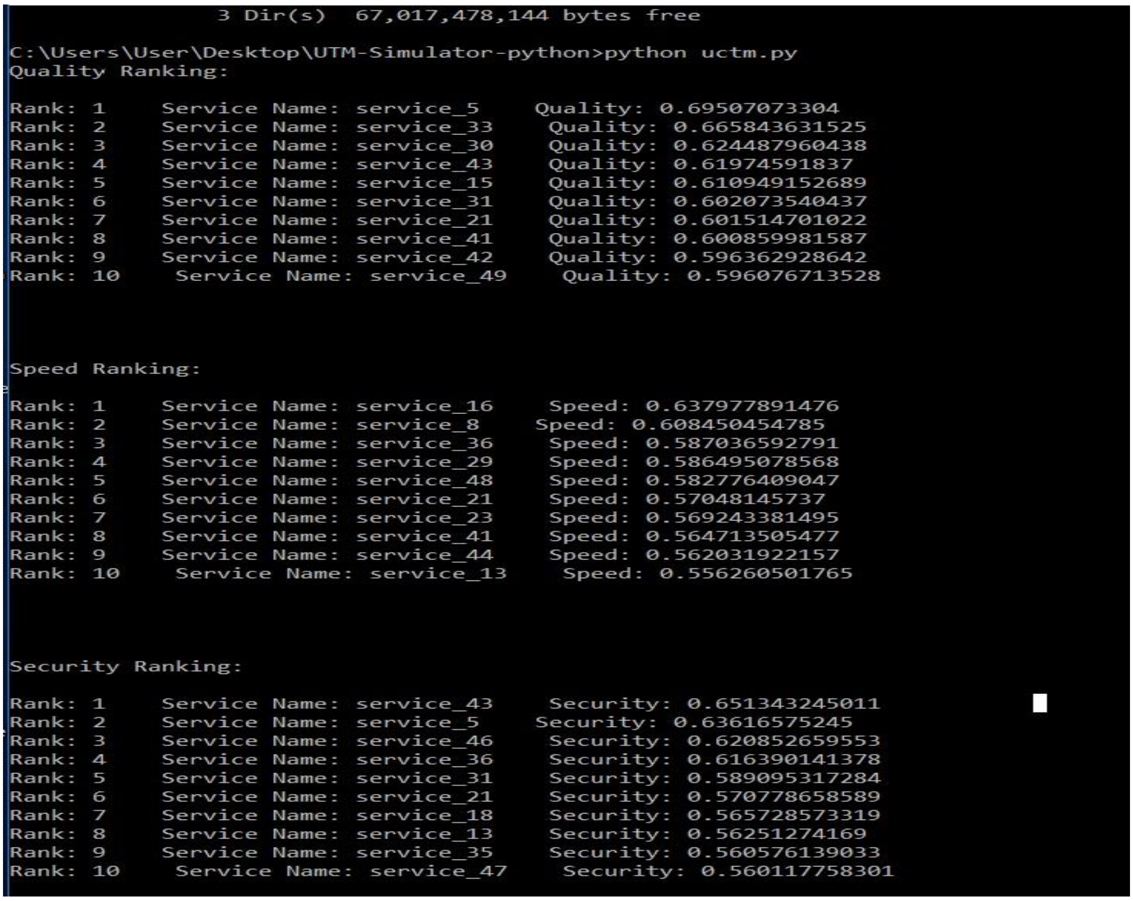
After getting values from transactions using TMS, the UCTM compare those values and select the ones that recommended by all the trust models, then recommend the online banking systems for the users as shown in Figure 20, Bank 10 is recommended based on the evaluations.

For each interaction between the user and the bank, the speed model will check sending time and response time and calculate those two values. The TMS will rank the bank based on the result. For the accuracy when nodes transacting with banks some of those transaction may fail, so the TMS must track them and use it to determine the accuracy of the banks in transactions they do. The TMS is a part of UCTM that responsible for logging transactions and quantifying trust values of banks continuously and store the values to evaluate banks against each other to provide best banks to the users.

4.2.2 Case Study 2: UCTM on Darkweb

The previous users they have experience using the dark web, and they know that keeping the privacy and trust of the users is important in the dark web. Trust is important in dark web and digital trust to make users comfortable with using it, because authentication in dark web is not exit. The communication occurs based on trust. Trust in the dark web is selected based on the reputation which is the forum has a good history of buying and selling goods, the individuals that have good reputation is more trusted. In the dark web, the important key for electing forums or service is based on the reputation of the group or the service provider. Furthermore, the base that uses increasing trust in digital world or Internet is trust models. There are many trust models on the internet to ensure trust in digital environments, but are still not been applied or used in dark web communications, transactions and exchanges .

When a customer buy digital goods in the dark web three parties are involved. One buys the goods, one sells, and the other monitors the process. If the person who buys do not like the goods or they do not get the goods, the transaction would not be done and the buyer would not transact the money to the seller, however, this process is done without any face to face meeting. Further, it is extremely hard for anyone to identify the source of the information or the location of the user. To increase reliability and trust, this in this study UCTM is applied to replace the third party and to evaluate trustworthy of the service. Consequently, is a preferable way to evaluate service and measure trust. It acts like measurement of trust, and the UCTM uses direct evaluating the service. The TMS is a part of the UCTM, is responsible for logging transactions and quantifying trust values of services continuously and stores the values to evaluate services and recommend the best service for the users. The UCTM replace both the reputation, and trust in the dark web. Increase privacy and performance in the environment for the users. And it will help in rating the service in a trusted way because the malicious nodes would not participate in evaluating the services.



```
               3 Dir(s)  67,017,478,144 bytes free

C:\Users\User\Desktop\UTM-Simulator-python>python uctm.py
Quality Ranking:

Rank: 1     Service Name: service_5     Quality: 0.69507073304
Rank: 2     Service Name: service_33     Quality: 0.665843631525
Rank: 3     Service Name: service_30     Quality: 0.624487960438
Rank: 4     Service Name: service_43     Quality: 0.61974591837
Rank: 5     Service Name: service_15     Quality: 0.610949152689
Rank: 6     Service Name: service_31     Quality: 0.602073540437
Rank: 7     Service Name: service_21     Quality: 0.601514701022
Rank: 8     Service Name: service_41     Quality: 0.600859981587
Rank: 9     Service Name: service_42     Quality: 0.596362928642
Rank: 10     Service Name: service_49     Quality: 0.596076713528



Speed Ranking:

Rank: 1     Service Name: service_16     Speed: 0.637977891476
Rank: 2     Service Name: service_8     Speed: 0.608450454785
Rank: 3     Service Name: service_36     Speed: 0.587036592791
Rank: 4     Service Name: service_29     Speed: 0.586495078568
Rank: 5     Service Name: service_48     Speed: 0.582776409047
Rank: 6     Service Name: service_21     Speed: 0.57048145737
Rank: 7     Service Name: service_23     Speed: 0.569243381495
Rank: 8     Service Name: service_41     Speed: 0.564713505477
Rank: 9     Service Name: service_44     Speed: 0.562031922157
Rank: 10     Service Name: service_13     Speed: 0.556260501765



Security Ranking:

Rank: 1     Service Name: service_43     Security: 0.651343245011
Rank: 2     Service Name: service_5     Security: 0.63616575245
Rank: 3     Service Name: service_46     Security: 0.620852659553
Rank: 4     Service Name: service_36     Security: 0.616390141378
Rank: 5     Service Name: service_31     Security: 0.589095317284
Rank: 6     Service Name: service_21     Security: 0.570778658589
Rank: 7     Service Name: service_18     Security: 0.565728573319
Rank: 8     Service Name: service_13     Security: 0.56251274169
Rank: 9     Service Name: service_35     Security: 0.560576139033
Rank: 10     Service Name: service_47     Security: 0.560117758301
```

Figure 22: The result of UCTM algorithm on Dark web services

In this case study, the implemented UCTM applied to evaluating digital trust for digital goods services through TMS to evaluate and manage trust values for those digital goods services that identified. It consists of an algorithm to recommend the services and a database to store trust values of the services. This implemented algorithm evaluates trust values for the transaction between users and providers then save the collected trust values in the database, trust values are security, speed, accuracy, and ranking. After evaluating those trust values and saving them in a database, then compare and select which service is better than the other services and recommend it to the users.

The current techniques used for evaluating service in the dark web is not trustable. Instead of that, applying the UCTM is a preferable solution; the evaluation of service with UCTM is more accurate. Thus, the result that people get based on reputation is not trustable too, a lot of malicious nodes can vote for them rank and it is subjective. The result that they get with the UCTM is more reliable and accurate. It will increase performance, privacy of the user, trust and reliability in the system.

Chapter 5

Conclusion and Future work

5.1 Conclusions

This study aims to counter cyberterrorism on both levels of surface and dark web. The significant horrific human cost through online radicalization and cyberterrorism activities has increased interest in research on countering cyberterrorism. The first part of this dissertation proposes an algorithm to find and geo-locate the online members of the Islamic State terrorist organization and identify their roles in the organization through online behaviour analysis. The result of the implemented algorithm can be used to track violence and terrorist activities electronically, classify the nodes based on Islamic States structure on social network and track the radical nodes that we believe they have become pre-terrorist nodes. It will also identify the nodes that are in the group, but not active yet and not involved in jihadi contents.

The previous security systems have always used the community and societal based trust to maintain cybersecurity. Gathering information on what people say about the system so that they can improve the confidence in their products was the only way of existence. The cybersecurity needs digital trust to increase certainty by both the users of the systems and the services. Digital trust is one of the most critical human requirements in the digital globalization era and is related to all fields of cybersecurity. Digital trust can be realized by combining information privacy and security and by maintaining a balance between them, especially when the world is at war with cyberterrorism. Privacy must be provided without putting the security of others at risk, and security should be provided without putting the privacy of those who are not dealing with cybercrimes at risk. Changing from societal to digital trust is very important to improve certainty in cyberspace. Digital trust models can facilitate improvements in the certainty of the entities of the digital environment.

UCTM will provide a satisfactory solution in this field. A great deal of work has been done on presenting trust models for different purposes. To best of our knowledge, there is a lack of a unified trust model that merge the trust models and simplify the installing for the users and the services. A

UCTM is like a measurement, trust and trustworthiness are critical measurements of a distributed sensing system or a heterogeneous network comprised of sources of information, knowledge, hardware, and software that can be applied on different purposes.

The second part of this dissertation proposes a UCTM with security, accuracy, speed, and recommendation trust model that merged comparing and priority trust models in it and TMS that can evaluate trust in this UCTM. The user of the UCTM can use all or some of the trust models together based on the requirements. It supports incognito mode to beware of the information and values that get from the interaction of the nodes and services. The UCTM based on direct trust; it will not depend on other nodes evaluation of trust. Most of the trust models that are being used in cyberspace and everyday commercial transaction are subjective and gradual, and it is based on the rating of people. The mood and fairness of people are never secured. A UCTM that objectively measures the trust by the trust management system that can replace the current subjective trust models is very much needed. This made the UCTM result in trust very accurate.

The UCTM is proposed to apply on dark web digital goods, as first step it will provide trust, privacy and security and it is a step to track the users and services of the forums in future. But since it is UCTM, it has to work on surface web too. The UCTM is applied to two different case studies on the surface web and dark web; it is accurately working on both platforms. In the case of the surface web is applied to different online banking systems. The UCTM is significant for the economy and is very important for bank users. A lot of people around the world use the online banking system. Evaluating the services with a direct TMS in this study increased trust and assurance. It evaluated each session and transactions between the users and the service in different dimensions and recommended the best online banking service according to the values of the transactions to the user and identify the malicious users for the bank systems. It improved the trustworthiness of the old and the new banking system based on the trust model values. Moreover, it helps in choosing the trusted bank in less time consuming, and in a better-trusted manner.

In the case of the dark web, the UCTM is applied on different forums for digital goods. As mentioned before it calculates entities trustworthiness based on speed, security, accuracy, ranking, priority, comparing, recommendation, and formally uses these factors in trustworthiness calculation and measurement. The simulation accomplished and examination of the projected model in different scenarios of the dark web and demonstrated its accuracy and performance. From the investigation of the examinations, the TMS empowered the whole system. The proposed display has seen expanding the proficiency and unwavering quality of trust assessment oblivious web conditions and adequately enhanced the reaction of the models to malevolent hub assaults. This has been exhibited to be genuine regardless of whether the quantity of exchanges is low and if the hubs habitually join and leave. Considering everything, the UCTM assessed by re-enacting in various investigations and demonstrated that the model offers responsive conduct and can be utilized adequately in the low association conditions.

Table 2: Trust in dark web with and without unified cyber trust model.

Trust with UCTM	Trust without UCTM
1. Trust-based trust models value 2. Ranking based on the value of (speed, accuracy and security) trust models 3. Recommendation based on (comparing, priority) trust models. 4. The UTM replace the third party	1. Trust-based on reputation 2. Reputation is based on people vote 3. Ranking based people vote 4. Recommendation based on ranking 5. Three-parties required for each transaction 6. The third party must be trusted and payed.

5.2 Suggestions for future work

Concerning our future work, proposing an exploit implanting into the proposed UCTM in this study to identify and geo-locate the users and services owners on dark web will make the process of countering cyber terrorism extremely easier; and even the members of terrorist organizations that run from surface web to dark web to avoid tracking from governments can be found.

References

[1] Brett Hawkins, “Under the Ocean of the Internet – The Deep Web”, SANS Institute InfoSec Reading Room, 2016.
[2] Bonner III, E.L., “Cyber power in 21st -century joint warfare”, Joint Forces Quaterly, vol. 74, no. 3, pp.102-9. 2014
[3] Martti Lehto, Pekka Neittaanmaki, "Cyber Security: Power and Technology”, Springer, 2018.
[4] Pavan Duggal, “ Cyber Security Law”, Independently published (January 17, 2019).
[5] Neumann, Peter R. 2013. "Options and Strategies for Countering Online Radicalization in the United States." Studies in Conflict & Terrorism (January): 431-459.
[6] Department of Defense, U. S. Army, U. S. Government, “ Cyberterrorism After Student- Terrorist Cyberattacks, Distributed Denial of Service (DDoS), Motives, Critical U. S. Infrastructure Vulnerabilities, Al-Qaeda Computer Capability, PC Attacks, Independently Published, 2017.
[7] Global Justice Information Sharing Initiative, “Developing a policy on the Use of Social Media. In Intelligence and Investigative Activities, Guidance and recommendations”, 2013.
[8] Schneier, B. , “Attacking Tor: how the NSA targets users’ online anonymity”. The Guardian, 1. Retrieved from, 2013.
[9] M. A. Tayebi, U. Glasser, P. L. Brantingham, “Organized crime structures in co-offending networks”. Ninth International Conference on Dependable, Autonomic and Secure Computing, New South Wales, Australia, 2011.
[10] J. Brynielsson, A. Horndahl, F. Johansson, L. Kaati, C. Mårtenson, P. Svenson, "Analysis of weak signals for detecting lone wolf terrorists." Intelligence and Security Informatics Conference (EISIC), 2012 European. IEEE, 2012.
[11] L. Jingxuan, P. Wei, L. Tao, S. Tong, “Network user influence dynamics prediction”. In Y. Ishikaw, J. Li, W. Wang, R. Zhang, W. Zhang (Eds.), Proceedings of the 15th Asia-Pacific Web Conference, APWeb , Sydney, Australia, 2013.
[12] M.F., S. Cassel, L. Kaati, A. Shrestha, “Activity profiles in online social media”, In: IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014), pp. 850–855, 2014.
[13] P. Wadhwa, M.P.S. Bhatia, “Measuring Radicalization in Online Social Networks Using Markov Chains”. Journal of Applied security Research, 10:1, 23-47, 2015.
[14] L. Kaati, A. Shrestha, T. Sardella, “Identifying Warning Behaviors of Violent Lone Offenders in Written Communication”, ICDM Workshop on Social Media and Risk, SOMERIS, Barcelona, Spain, 2016.
[15] Ruan, Y., & Durresi, A. A survey of trust management systems for online social communities–Trust modeling, trust inference and attacks. Knowledge-Based Systems, 106, 150-163, 2016.
[16] Wu, Z., Aggarwal, C. C., & Sun, J., “The troll-trust model for ranking in signed networks”. In Proceedings of the Ninth ACM International Conference on Web Search and Data Mining (pp. 447-456). ACM, 2016.
[17] Ghavipour, M., & Meybodi, M. R., “An adaptive fuzzy recommender system based on learning automata”. Electronic Commerce Research and Applications, 20, 105115, 2016.
[18] Thrift, N., & Amin, A., “Neo-Marshallian nodes in global networks”. In Economy, 2017.
[19] Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K., “ Survey of security advances in smart grid: A data driven approach”. IEEE Communications Surveys & Tutorials, 19(1), 397-422, 2017.
[20] Zhou, Q., & Luo, J.,” The study on evaluation method of urban network security in the big data era” . Intelligent Automation & Soft Computing, 1-6, 2017.
[21] Vamsi, P. R., & Kant, K., “Trust and reputation aware geographic routing method for wireless ad hoc networks”. International Journal of Ad Hoc and Ubiquitous Computing, 27(2), 121-137, 2018.
[22] Shaikh, R., & Sasikumar, M., “Trust model for measuring security strength of cloud computing service”. Procedia Computer Science, 45, 380-389, 2018.
[23] Manuel, P., “ A trust model of cloud computing based on Quality of Service”. Annals of Operations Research, 233(1), 281-292, 2018.
[24] Filali, F. Z., & Yagoubi, B., “Global trust: a trust model for cloud service selection”. International Journal of Computer Network and Information Security, 7(5), 41, 2018.
[25] Kirrane, S., Mileo, A., & Decker, S.,” Access control and the resource description framework: A

survey". Semantic Web, 8(2), 311-352, 2017.
[26] Fan, W., & Perros, H., " A novel trust management framework for multi-cloud environments based on trust service providers". Knowledge-Based Systems, 70, 392-406, 2014.
[27] Dangolani, S. K., "The impact of information technology in banking system (a case study in Bank Keshavarzi IRAN)". Procedia - Social and Behavioral Sciences, 30, 13–16, 2011.
[28] Khiabani, H., Bashah Idris, N., & Ab Manan, J. L., "A unified trust model for pervasive environments - Simulation and analysis. KSII Transactions on Internet and Information Systems", 7(7),1569–1584, 2013.
[29] Nigudge, S., & Pathan, M. K. A.," E-banking : Services , Importance in Business , Advantages , Challenges and Adoption in India" .,190–192. 91, 2014.
[30] Nithyanand, R., Starov, O., Zair, A., Gill, P., & Schapira, M., "Measuring and mitigating AS-level adversaries against Tor". Nithyanand, Starov, Zair, Gill, & Schapira, 2015.
[31] Chertoff, M., & Simon, T., "The Impact of the DarkWeb on Internet Governance and Cyber Security". Global Commission on Internet Governance, (6). Chertoff & Simon, 2015.
[32] R. Barrett, "The Islamic State", Senior vice president the Soufan Group, 2014.
[33] France Belanger, Robert E. Crossler, "Privacy in Digital Age: A Review of Information Privacy Research in Information Systems", Belanger & Crossler/Privacy in the Digital Age, 2011.
[34] Steven M. Bellovin, "Thinking Security- Stopping Next year's Hackers", Addison Wesley, 2019.
[35] Dieter Gollmann, "Computer Security", Third Edition, John Wiley and Sons, 2011.
[36] Alexander Klimburg (Ed.), "National Cyber Security Framework Manual", NATO CCD COE Publication, Tallinn 2012 .
[37] Robert Anderson, Jr. Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland, Executive Assistant Director, Criminal, Cyber, Response, and Services Branch, Federal Bureau of Investigation, 2014.
[38] Mayssa Zerzri, "The Threat of cyberterrorism and Recommendations for Countermeasures", C.A.Perspectives on Tunisia, 2017.
[39] Buczak, Anna, L., and Guven, Erhan. "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." IEEE Communications Surveys & Tutorials, 18.2, 2016.
[40] Bhattacharyya, Dhruba, and Das, Debasish. "Defeating Cyber Attacks Due to Script Injection." International Journal of Network Security, 20.2, 2018.
[41] Fielder, Andrew et al. "Decision support approaches for cyber security investment." Decision Support Systems, 86, 2016.
[42] Varadarajan, Rammohan, and Malpani, Ambarish. "One-Time Use Password Systems And Methods." US20170249633A1, United States, 2019.
[43] Dworkin, Morris, J. "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions." Federal Inf. Process. Stds. (NIST FIPS), 2015.
[44] Zare H., Olsen P., Zare M.J., Azadi M., Operating System Security Management and Ease of Implementation (Passwords, Firewalls, and Antivirus). In: Latifi S. (eds) Information Technology – New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham 92, 2018.
[45] Tom Holt, Joshua D. Freilich, Steven Chermak, and Clark McCauley. "Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos." Dynamics of Asymmetric Conflict, 8:2, 2015.
[46] Weimann, Gabriel. "Terrorist Migration to the Dark Web." Perspectives on Terrorism, 10.3, 2019.
[47] Spalevic, Zaklina and Ilic Belgrade. "The use of dark web for the purpose of illegal activity spreading." ЕКОНОМИКА, 63.1, 2017.
[48] K. Welch, "The Beheading of Nicholas Berg", Houston, 2004.
[49] UNODC , "The Use of the Internet for terrorist purposes". In collaboration with the United Nations Counter-Terrorism implementation on Task Force. United Nations office on drugs and crime Vienna, New York, 2012.
[50] Brendan I. Koerner, "Why IS is winning the Social Media", WIRED, 2016.
[51] Telegraph reporter, "How terrorists are using social media", 2014.
[52] A. Hoffman, Y. Schweitzer. "Cyber Jihad in the Service of the Islamic State (IS)", Strategic Assessment, Volume 18. No.1, 2015.
[53] F. Marone, "Italian Jihadists in Syria and Iraq", Journal of Terrorism Research, 2016.
[53] N. Grigoriev; E. Rodyukov, " Modern Cybernetic terrorism and his social consequences", house of the state university of Mangement, 2019.
[55] Halim ajraktari, Agon Kokaj, " Cyber war and Terrorism in Kosovo", Academic Journal of Business, 2019.

[56] Srinivas, Jangirala; Das, Ashok Kumar; Kumar Neeraj." Government regulations in cyber security: Framework, standards and recommendations", Future Generation Computer Systems.2018.
[57] Kenny, Michael. "Cyber-Terrorism in a Post-Stuxnet World." Elsevier, 2015.
[58] Gross, Michael, L., Canetti, Daphna, and Vashdi, Dana, R. "Cyberterrorism: its effects on psychological well-being, public confidence, and political attitudes." Journal of Cybersecurity, 3(1), 2017.
[60] Y. Veilleux, "Paradigmatics in Jihadism in Cyberspace: The Emerging Role of Unaffiliated Sympathizers in Islamic State's Social Media Strategy", Lepage, The Centre for the Study of Terrorism and Political Violence, Journal of Terrorism Research, 2016.
[61] Chertoff, M., & Simon, T., " The Impact of the DarkWeb on Internet Governance and Cyber Security", Global commission on Internet Governance, 2015.
[62] Jared Norton, " Learn to avoid NSA spying and become anonymous online", Create Space Independent Publishing Platform, 2016.
[63] Zhou Li, Alrwais, S., Yinglian Xie, Fang Yu, & Xiao Feng Wang, "Finding the Linchpis of the DarkWeb: a Study on topologically Dedicated Hosts on Malicious Web Infrastructures", 2013.
[64] Gabbriel Weimann,"Terrorist Migration to the Dark Web", Perspectives on Terrorism Vol. 10, No.3, 2016.
[65] Alhogbani, A., "Going Dark : S Cratching the S Urface", 469–501. Alhogbani, 2016.
[66] L. Huey, "Social Media, Online Radicalization and the Practice of Political Jamming", Journal of Terrorism Research. The Centre for the Study of Terrorism and Political Violence, Volume 6, Issue 2, 2015.
[67] Dainton, Marianne, Elain D. Zellei, "Applying communication Theory for professional Life", Sage Publications, ISBN 1-4129-7691- X, 2011.
[68] F. Roman, H. Stephan, "Models in science", The Standard Encyclopedia of Philosophy, 2009.
[69] M. Castells, "A Network Theory of Power", University of Southern California, 2011.
[70]Ala Berzinji, Lisa Kaati, Ahmed Rezine. " Detecting Key Players in Terrorist Networks", European Intelligence and Security Informatics Conference, 2012.
[71] Patrick Tucker, "How the Military Will Fight ISIS on the Dark Web", Defense One, February 24, 2015.
[72] J Piskorski, Roman Yangarber, Information Extraction: Past, Present and Future, 2012.
[73] R. Agrawal and M. Batra, "A detailed study on text mining techniques," International Journal of Soft Computing and Engineering (IJSCE) ISSN, pp. 2231–2307, 2013.
[74] Tom Nicholls, Jonathan Bright, Understanding News Story Chains using Information Retrival and Network Clustering Techniques. Communication Methods and Measures baby Taylor & Francis, 2018.
[75] R. Talib, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7 No. 11, Text Mining: Techniques, Applications and Issues, 2016 .
[76] B. Laxman, D. Sujatha, "Improved method for pattern discovery in text mining," International Journal of Research in Engineering and Technology, vol. 2, no. 1, pp. 2321–2328, 2013.
[77] Muhammd Mudassar Yamin, Basel Katt, Detecting Malicious Windows Commands Using Natural Language Processing Techniques, Springers book. 2019.
[78] Krish Krishnan, Shawn P. Rogers, Learn more about Natural Language Processing. Social Data Analytics, 2015.
[79] Michael Williams, Catherine Yan, Mark Zhang, " Deep Web & Dark Web", 2015.
[80] Ryan Ehney, Jack Shorter, " Deep Web, Dark Web, Invisible Web and the post ISIS World", Texas A&M University – Kingsville. Volume 17, Issue IV, pp. 36-41, 2016.
[81] Beshiri Arber and Susurim Arsim. "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review." Journal of Computer and Communications, 2019.
[82] Algaith, Areej et al., "Finding SQL Injection and Cross Site Scripting Vulnerabilities with Diverse Static Analysis Tools." Paper presented at the 14th European Dependable Computing Conference, 2018
[83] Sun, Xiaoyan. "Using Bayesian Networks for Probabilistic Identification of Zero-Day Attack Paths." IEEE Transactions on Information Forensics and Security, 13.10, 2018.
[84] Raja Naeem Akram, "Digital Trust - Trusted Computing and Beyond: A Position Paper" in Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 13th International Conference on 24-26 Sept, 2014.
[85] Tim Berners-Lee,"A Framework for Web Science" Foundations and TrendsÆ in Web Science: Vol. 1: Yet, every doctoral dissertation should have an end. So I rest my case! No. 1, pp 1-130,September 1st 2006.

[86] Raph Levien and Alex Aiken,"Attack-Resistant Trust Metrics for Public Key Certification" published in the Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998.
[87] Matthew Richardson,Rakesh Agrawal and Pedro Domingos,"Trust Management for the Semantic Web" Published In Proceedings of the Second International Semantic Web Conference from Book Proceedings of the Second International Semantic Web Conference pages 351ñ368, 2003.
[88] Ian Jacobi and Lalana Kagal,"Rule-based trust assessment on the semantic web"RuleML'2011 Proceedings of the 5th international conference on Rule-based reasoning, programming, and applications Pages 227-241 ,2011.
[89] Deniz Applebaum, "Securing Big Data Provenance for Auditors: The Big Data Provenance Black Box as Reliable Evidence", Journal of Emerging Technologies in Accounting:Vol. 13, No. 1, pp. 17-36, 2016.
[90] Peter J. Denning, "Fifty Years of Operating Systems", Communications of the ACM, Vol. 59 No. 3, Pages 30-32, 2016.
[91] Michael W. Floyd, Michael Drinkwater, David W. Aha, "Learning Trustworthy Behaviors Using an Inverse Trust Metric", 2016.
[92] Dr. Dan Zwillinger, Gari Palmer, Anne Welwyn, " Creating Trust in Autonomous Systems- The Trust V", Safe & Secure Systems & Software Symposium, 2014.
[93] Behzad Sadrfaridpour, Hamed Saeidi, Jenny Burke, Kapil Madathil, and Yue Wang, " Modeling and Control of Trust in Human-Robot collaborative Manufacturing, 2016.
[94] Dr. Guruduth Bandar, Learning to trust artificial Intelligence Systems-Accountability, compliance and ethics in the age of smart machines", IBM, 2016.
[95] Jonathan A. Obar, Steven S. Wildman, "Social Media Definition and the Governance Challenge: An Introduction to the Special Issue", Telecommunications policy, 39(9), 745-750, 2015.
[96] Jingpei Wang, Sun Bin, Yang Yu, Niu Xinxin," Distributed Trust Management Mechanism for the Internet of Things", Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, 2013.
[97] Serif Bahtiyar, Mehmet Ufuk Caglayan, " Security similarity based trust in cyber space", Knowledge-Based Systems volume 52, 2013.
[98] L.-A. Tang, X. Yu, S. Kim, Q. Gu, J. Han, A. Leung, T.L. Porta, "Trustworthiness analysis of sensor data in cyber-physical systems ', Journal of Computer and System Sciences, 79, pp. 383–401, 2013.
[99] D.Henshel, M.G. Cains, B. Hoffman, T.Kelley, " Trust as a Human Factor in Holistic Cyber Security Risk Assessment", International Conference on applied Human Factors and Ergonomics, 2015.
[100] Lawrence M. Krauss, " A Universe from nothing"., ISBN: 978-1-4516-2445-8 Newyork, 2012.
[101] Carmen Fernandez-Gago, Francisco Monyano, Javier Lopes, "Modeling trust dynamics in the Internet of Things, Network, Information and Computer Security Lab, University of Malaga, 29071 Malaga, Spain, 2017.
[102] Yan, Z, Zhang, P. Vasilakos. "A Survey on trust mangement for Internet of Things. Journal of Network and Computer Applications. 42, 120-134, June 1, ISSN: 1084-8045, 2014.
[103] Fengming Liu, Li Wang, Lei Gao, Haixia Li, Haifeng Zhao, Sok Khim Men, " A Web Service trust evaluation model based on small world networks, Knowledge based systems, 2014.
[104] Krisin Finklea, "Dark Web", Congressional Research Service , 2017.
[105] Yingjie Wang, Guisheng Yin, Zhipeng Cai, Yuxin Dong, and Hongbin Dong. A trustbased probabilistic recommendation model for social networks. Journal of Network and Computer Applications, 2015.
[106] Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, and Azzam Mourad. A survey on trust and reputation models for web services: Single, composite, and communities. Decision Support Systems, 2015.
[107] Bertram Schulte, " Building Digital Trust", Digitalist Magazine, 2019.
[108] A Frost & Sullivan," The Global state of Online Digital Trust", Commissioned by CA Technologies,
[109] Rossout von Solms, Johan van Niekerk, "From Information Security to Cyber Security", Computer & Security 38, 2013
[110] Algamdi, A., Coenen, F., & Lisitsa, A. "A trust evaluation method based on the 96 distributed Cloud Trust Protocol (CTP) and opinion sharing". provider, 5(17), 18, 2017.
[111] Toosi, A. N., Calheiros, R. N., & Buyya, R., "Interconnected cloud computing environments: Challenges, taxonomy, and survey". ACM Computing Surveys (CSUR), 47(1), 7, 2018.

[112] Simin Hall, William McQuay, "Fundamental Features of a Unified Trust Model for distributed system, IEEE 978-1-4577-1041-4/11 , 2011.
[113] Stratis D Viglas, "Data Provenance and Trust", Data Science Journal, Volume 12, 2013.
[114] P.Buneman and Susan, "Data Provenance - the Foundation of Data Quality", 2010.
[115] Olive Qing Zhang, Markus Kirchberg,Ryan K L Ko, Bu Sung Lee, How To Track Your Data: The Case for Cloud Computing Provenance.HP, 2012.
[116] Slavom´ır Kavecky´ Penka Martincova, "Overview of Trust Models: Integrating Trust Management into Grid Computing." International Journal of Computer Applications Volume 129 - No.7, 2015.
[117] F. Moyano, Carmen. Fernandez-Gago, and J. Lopez, "A Conceptual Framework for Trust Models", 9th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2012), LNCS vol. 7449, pp. 93-104, 2012.
[118] Audun Jøsang, Roslan Ismail, and Colin Boyd, "A survey of trust and reputation systems for online service provision". Decision Support Systems, 43(2):618–644, 2017.
[119] Victor, Patricia, Cornelis, Chris, De Cock, Martine, "Trust Networks for Recommender Systems" Atlantis Computational Intelligence Systems, ISBN-10: 9491216074, 2011.
[120] ICAO Bord. ICAO Public Key Directory, ICAO PKD Regulations and Procedures. Update for new ICAO PKD Service. 2016.
[121] European Union Agency for Network and Information Security, Guidelines on initiation of qualified trust services, final draft 0.7 September 2016.
[122] Soshi Hamaugchi, Toshiyuki Kinoshita, and Satoru Tezuka, "An Analysis of Trust Models of Public Key Infrastructure". Japan, International Science Press, Voume 10, Number 30, 2017.
[123] Marc Sel, "A Comparison of Trust Models", ISSE pp 206-215, 2015.
[124] Ishmaev, G. "Blockchain Technology as An Institution of Property". Metaphilosophy, vol 48, no. 97 5, pp. 666-686. Wiley, doi:10.1111/meta.12277, 2017.
[125] Kane, Ethan. "Is Blockchain a General-Purpose Technology?". SSRN Electronic Journal, pp. 457-588. Elsevier BV, doi:10.2139/ssrn.293, 2017.
[126] Debjit Das, Koushik Majumder, Anurag Dasgupta. Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory. Science Direct. International Multi-Conference on Information Processing 2015. IMCIP, 2015.
[127] L Raja, S Santhosh Baboo. An Overview of MANET: Applications, Attacks and Challenges. IJCSMC, Vol. 3, Issue, 2014.
[128] Bankovic, Z., Vallejo, J., Fraga, D., & Moya, J., "Detecting false testimonies in reputation systems using self-organizing maps". Logic Journal of IGPL, 21, 549–559, 2013.
[129] I. Thomas and C. Meinel, "Enhancing Claim-Based Identity Management by Adding a Credibility Level to the Notion of Claims," IEEE International Conference on Services Computing, Bangalore, pp. 243-250. doi: 10.1109/SCC.2009.66, 2009.
[130] David Chappell. Claims Based Identity for Windows: The Big Picture. Pluralsight, 2013.
[131] Lemke and Lins, ERISA for Money Managers, Chapter 1, Thomson West, 2013.
[132] YeeLoong Chong A, Ooi K, Lin B, Tan B, "Online banking adoption: an empirical analysis". Int J Bank Mark 28(4):267–287, 2010.
[133] Villoria M, Ramírez Alujas Á. Development Stages of Electronic Government Models An Analysis from Political Theory. Gestión Y Política Pública [serial online], 2013.
[134] Jon Gabriel, " Artificial Intelligence: Artificial Intelligencefor Humans-Artificial Intelligence, Machine learning", 2016.
[135] Philip C. Jackson, "Introduction to Artificial Intelligence:Second, Enlarged Edition", 2013.
[136] Ranjeev Mittu, Donald Sofge, Alan Wagner, W.F. Lawless, "Robust Intelligence and Trust in Autonomous Systems", Springer US, 2016.
[137] Yu-Chih Wei; Yi-Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANET's", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

Publications

1. Ala Berzinji, Nzar Ali. “Reviewing trust from socital to digital to build unified trust model”. Transylvanian Review Journal, volume XXVVII No. 45. 2019. ISSN: 1221-1249.

2. Ala Berzinji, Nzar Ali. “Identifing roles of Islamic State members through online nodes behaviour analysis”. Transylvanian Review of Administrative Sciences Jornal, number 58 E. 2019. ISSN: 2247-8310.

الخلاصة

يغطي الإنترنت عالمنا بالكامل، فمن مجموع 7,7 مليار من البشر فوق سطح الأرض ، يستخدم أكثر من 5,1 مليار منهم الإنترنت، ومستخدموا الإنترنت لهم أوجه مختلفة، الدول والمنظمات والأشخاص، لأغراض عامة وخاصة، في المجال العسكري، الأمني، السياسي، الاقتصادي، التجاري، العلمي، الديني، الأدبي، الاجتماعي، الفني، التنموي، التسوق، العلاقات، الإعلام والرأي، العمل الخيري والمصلحة العامة، أو لغرض زرع الفرقة والصدام، يستخدمون الإنترنت بلا تردد في كافة مجالات الحياة.

لكن هذا الاستخدام يمثل (الشبكة السطحية) للإنترنت، وهو جزء قليل فقط من ذلك العالم الواسع، أما الجزء الآخر غير المعروف عند أغلب الناس فتتمثل في (الشبكة العميقة) والأعمق منها (الشبكة المظلمة). هذه المستويات والتأثيرات المختلفة والعميقة للإنترنت، الأمن الإلكتروني، تجعل أمن البيانات والمعلومات والبنية التحتية والبيئة ضرورة حياتية، ومجمل هذا الأمن يتجسد في الأمن السيبراني (الإنترنتي).

يمثل الأمن السيبراني الحارس والمهاجم الأصيل للأمن القومي للدول، وليس الدول فقط، بل المنظمات غير الحكومية وعصابات الجريمة المنظمة والجماعات الإرهابية كلها تسعى إلى استخدام إجراءات وتقنية و تكتيك الأمن السيبراني لمصلحتها. فالإرهاب السيبراني كفرع للأمن السيبرني نشاط حديث ظهر في شبكة الإنترنت العالمية ثم نما وتطور، وتعتمد عليه الجماعات الإرهابية لتحقيق أهدافها الإيديولوجية والتأثير في الفرد والمجتمع وإلحاق الأضرار الجسدية والمادية والمعنوية بمناوئيها، فالإرهاب السيبراني يمثل تهديدًا جديًّا على البيانات والمعلومات والبنية التحتية والبيئة للأفراد والمجتمعات والحكومات والدول.

في هذا الإطار ولغرض التصدّي للإرهاب السيبراني وتقليل مخاطره وأضراره، فإنّ معظم الدول وضعت قوانين خاصة بمكافحة أضرار الإرهاب السيبراني وتشكيل مؤسسات وأجهزة مختصة وخبيرة في مجال مكافحة الإرهاب السيبراني، ووضع الدارسون ومراكز البحوث تركيزهم على هذا الموضوع الجديد والمؤثر، ونظرًا لحداثة العمل في مكافحة الإرهاب السيبراني في المجال الأكاديمي فإنّ المصادر والابحاث قليلة في هذا المجال، فالتحديّات والمخاطر على الشبكة السطحية للإنترنت وفي الشبكة المظلمة كثيرة وغير مسيطر عليها وفعّالة، لذا ارتأينا ضرورة إنجاز هذه الدراسة والتي تستطيع المساهمة في إنتاج المعرفة وفتح الباب لإجراء نقاشات أكاديمية أكثر وأوسع.

الغرض من هذه الدراسة مكافحة الإرهاب السيبراني على الإنترنت على صعيدين:

في (الشبكة السطحية) عملت هذه الدراسة على استهداف وإيجاد الأشخاص الذين يعملون للجماعات الإرهابية في مجال التطرف عبر الإنترنت. وفي (الشبكة المظلمة) حاولت هذه الدراسة تشخيص الأفراد والمجموعات التي تعمل لصالح الجماعات الإرهابية عن طريق صنع (نموذج الثقة السيبراني الموحد).

في القسم الأول من الدراسة تم اقتراح (خوارزمية) لإيجاد وتعيين (تحديد الموقع الجغرافي) للأفراد الذين يُعرِّفون أنفسهم كأعضاء لجماعة إرهابية في مجاميع الشبكات الاجتماعية في الإنترنت، هذه الخوارزمية عمِلت على تخمين وتحديد مهمة وعمل كل من الأعضاء ودورهم في هيكلية الجماعة بالاعتماد على تحليل تصرفاتهم، كما عملت على تشخيص وإيجاد الأفراد الذين وقعوا حديثا تحت تأثير العملية النفسية للجماعات التكفيرية، وإذا أخذت الجهات المعنية بنتائج هذه الدراسة فإنّ مشروع مكافحة التطرف للتصدي لمنع زيادة الأشخاص المتأثرين بالإيديولوجية التكفيرية، وتصحيح وجهة حياتهم، وإبعادهم عن العمل الإرهابي، تتقدم خطوة مهمة إلى الأمام.

وفي القسم الثاني، أُقتُرِحَ نموذج الثقة السيبراني (الإلكتروني) الموحد UCTM، كبديل للثقة، وكذلك نظام إدارة الثقة (TMS) في الشبكة المظلمة كبديل للتوصية الذاتية SR .

هذا المشروع باستطاعته إيجاد الأشخاص الذين يستخدمون الشبكة المظلمة لهدف الإرهاب، فالمشروع اقترح نظام الإدارة الذاتية TMS ، حتى يستطيع الشخص المستهدف أن يقيس بنفسه أمان اتصاله بالشبكة وأن لا يضطر إلى وضع ثقته في الاتصال إلى التبادل الإلكتروني الجاري في الشبكة المظلمة على أساس تصويت الأعضاء الآخرين.

يمكن لنتائج هذه الدراسة أن تسهم في إثراء وزيادة النقاشات الأكاديمية حول موضوع (مكافحة الإرهاب السيبراني)، وفي إنتاج معرفة خاصة تستخدم في مكافحة التطرف، في الشبكة السطحية وفي الشبكة المظلمة، للنقاش حول نموذج الثقة (الأمان) المقترح لمكافحة الإرهاب السيبراني، وفي المجال العملي تستطيع هذه الدراسة أن تلعب دورًا في تشكيل وتأسيس البنية الأساسية لمنظمة مكافحة الإرهاب السيبراني، على مستوى الشبكة السطحية والشبكة المظلمة في الإنترنت، في مجالات إيجاد و تشخيص الأفراد المتطرفين، وفي مواجهة الحرب النفسية للإرهاب العالمي، ونصرة مكافحة التطرف والحؤول دون زيادة إنخراط الأشخاص المتصلين حديثا بالشبكات الإرهابية، وتلعب دورًا في معاداة الإرهاب وتكون ذا فائدة في مواجهة الإرهاب السيبراني، للحفاظ على أمن وسلامة الأفراد والجماعات والدول، والمشاركة في ردع التهديدات والمخاطر الخفية التي تظهر يوميًا عن طريق الإرهاب السيبراني في الشبكة المظلمة، ضد الأمن والنظام والبنية التحتية والبيئة ومجمل القيم الإنسانية.

نموذج الثقة السيبراني الموحد
لـمكافحة الإرهاب السيبراني
على شبكة الأنترنت السطحية
و ويب الدارك

أطروحة
مقدمة إلى مجلس كلية العلوم - جامعة السليمانية
كجزء من متطلبات نيل درجة دكتوراه فلسفة
في علوم الحاسوب
(الأمن السيبراني)

من قبل
ئالا عمر أحمد

بإشراف
د. نزار عبدالقادر علي
أستاذ مساعد

أيلول ٢٠١٩ م   خرمانان ٢٧١٩ ك

پوختەی تێز

ئینتەرنێت سەرتاسەری جیهانی ئێمەی داپۆشیوە و لە کۆی ٧,٧ بلیۆن مرۆڤی سەر زەوی، زیاتر لە ٥,١ بلیۆن کەسیان ئینتەرنێت بەکاردەیهنن. بەکارهێنەرانی ئینتەرنێت، رووی جیاوازیان هەیە. دەوڵەتان و رێکخراو و تاکەکان، بە مەبەستی گشتی و تایبەتی، لە بواری سەربازی، ئەمنی، سیاسی، ئابوری، بازرگانی، زانستی، ئاینی، ئەدەبی، کۆمەڵایەتی، هونەری، پێگەیاندن، بازاڕکردن، پەیوەندی بەستن، راگەیاندن و رادەربڕین، بۆ کاری خێرخوازی و چاکەی گشتی، یان نانەوەی دووبەرەکی و پێکدادان، و بێ دوو دڵی، لەسەرجەم کایەکانی ژیان دا ئینتەرنێت بەکاردەهێنن. بەڵام ئەم بەکارهێنانە، تەنها روکاری دەرەوەی ئینتەرنێتە، (سورفەیس وێب) بەشێکی کەمی ئەو جیهانە فراوانەیە، و ئەوەی تری کە لای زۆربەی زۆری خەڵك نەناسراوە، (دیپ وێبە) و قوڵتریش لەو (دارك وێب)ە.
ئەم ئاست و کاریگەرییە جیاواز و قوڵانەی سایبەر، ئاسایشی ئەلیکترۆنی، بۆ دابینکردنی ئاسایش بۆ داتا و مەعلومات و ئینفراستراکچەر و ژینگە دەکات بە پێویستییەکەی حەیاتی، و کۆی ئەم ئاسایشەش لە سایبەر سیکیوریتی دا خۆی بەرجەستە دەکات.

سایبەر سیکیورتی، ئێستا پاسەوان و هێرشبەرێکی رەسەنی ئاسایشی نیشتمانیی دەوڵەتانە، و نەك هەر دەوڵەت، بەڵکو رێکخراوی نا-دەوڵەتی، و باندەکانی تاوانی رێکخراو و گروپە تیرۆریستییەکان، هەوڵدەدەن پرۆسیجەر و تەکنیك و تەکتیکەکانی سایبەر سیکیوریتی لە بەرژەوەندی خۆیان بەکاربهێنن.
لەم روەوە، سایبەر تیرۆیزم وەك لقێکی سایبەر سیکیوریتی، چالاکییەکی نوێیە و لەناو تۆڕی جیهانیی ئینتەرنێتدا دەرکەوتوە، گەشەی کردوە، و گروپە تیرۆریستییەکان بۆ مەرامی ئایدیۆلۆژی، و کارکردنە سەر تاك و کۆمەڵگە، و بەرهەمهێنانی زیانی گیانی و ماڵی و مەعنەوی، دژی نەیارەکانیان پشتی پێ دەبەستن.
سایبەر تیرۆریزم دەبێتە هەڕەشەی جدی لەسەر داتا و مەعلومات و ژێرخان و ژینگەی تاك و کۆمەڵ و حکومەت و دەوڵەتەکان .
لەم چوارچێوەیەدا و بۆ رێگرتن لێی، هەروەها کەمکردنەوەی زیانەکانی سایبەر تیرۆرێزم، زۆربەی دەوڵەتان یاسای تایبەتمەندیان بە قەڵاچۆکردنی زیانەکانی سایبەر تیرۆریزم داڕشتوە، و دەزگای پسپۆڕ و تایبەتمەندیان بۆ کارکردن لە بواری کاونتەر سایبەر تیرۆریزم دا پێکهێناوە، و توێژەر و سەنتەرەکانی توێژینەوەش، فۆکەسیان بەرەو ئەم سەبجێکتە نوێ و کاریگەرە، زیاد کردوە .

لەم چوارچێوەیەدا و بۆ رێگرتن لێی، هەروەها کەمکردنەوەی زیانەکانی سایبەر تیرۆرێزم، زۆربەی دەوڵەتان یاسای تایبەتمەندیان بە قەڵاچۆکردنی زیانەکانی سایبەر تیرۆریزم داڕشتوە، و دەزگای پسپۆڕ و تایبەتمەندیان بۆ کارکردن لە بواری کاونتەر سایبەر تیرۆریزم دا پێکهێناوە، و توێژەر و سەنتەرەکانی توێژینەوەش، فۆکەسیان بەرەو ئەم سەبجێکتە نوێ و کاریگەرە، زیاد کردوە .

بەڵام لەبەرئەوەی کارکردن لەبواری کاونتەر سایبەر تیرۆریزم، لە ئەکادیمیادا زۆر نوێیە، سەرچاوە و توێژینەوەکان لەمبوارەدا کەمن، و هەڕەشە و مەترسییەکان، لە سەر روکاری ئیەنتەرنێت و لەناو دارك وێب دا زۆر و کۆنترۆڵنەکراو و کاریگەرن، ئەنجامدانی ئەم توێژینەوەیە بە گرنگ زانرا. کە دەتوانێت بەشداری، (کۆنتریبیوشن)، بکات لە بەرهەمهێنانی مەعریفە، (نۆڵج)، و دروستکردنی دیبەتی زیاتری ئەکادیمی دا.
مەبەست لەم توێژینەوەیە کاونتەرکردنی سایبەر تیرۆریزمە لەسەر ئینتەرنێت، لەسەر دوو ئاست. لە (سورفەیس وێبدا) ئەم توێژینەوەیە لە رێی بەئامانجگرتن و دۆزینەوەی ئەو کەسانەی لە بواری (ئۆنلاین رادیکاڵیزیشن) دا کار بۆ گروپە تیرۆریستییەکان دەکەن، کاری کردوە. لە (دارك وێب) یشدا لە رێگەی دروستکردنی مۆدێلێکی متمانە پێکراوی یەکخراوی سایبەر، (یونیفاید سایبەر ترەست مۆدێل UCTM) ەوە بۆ جێگرتنەوەی متمانە ،(ترەست)، هەوڵی داوە دەستنیشانی ئەو کەس و گروپەکانە بکات کە کار بۆ گروپە تیرۆریستییەکان دەکەن.

لە بەشی یەکەمی توێژینەوەکەدا، (ئەلگۆریسم)ێك پێشنیار کراوە بۆ دۆزینەوە و دەستنیشانکردنی شوێنی،(جیۆلۆکەیت)کردنی ئەو (نۆد)انەی کە خۆیان وەك ئەندامانی گروپێکی تیرۆریستی دەناسێنن لەناو گروپە ئۆنلاینەکانی سۆشیاڵ میدیادا. ئەم ئەلگۆریسمە، کاری کردوە لەسەر پێشبینی کردنی ئەرك و کاری هەریەك لە نۆدەکان، (ئەندامەکان)، و رۆڵیان لەناو سترەکچەری گروپەکەی دا، بە پشتبەستن بە شیکاریکردنی هەڵسوکەوتیان. هەروەها کارکراوە بۆ دەستنیشانکردن و دۆزینەوەی ئەو نۆدانەی کە تازە کەوتونەتە ژێر کاریگەریی ئۆپەراسیۆنی دەرونی، (سایکۆلۆجیکاڵ ئۆپەرەیشن)ی گروپە تەکفیرییەکان، و ئەگەر لایەنی پەیوەندار سود لە ئەنجامی ئەم توێژینەوەیە وەربگرێت، ئەوا پرۆژەی (دی-رادیکەڵایزەیشن) بۆ رێگرتن لە تووشبونی زیاتری کەسانی توشبوو بە ئایدیۆلۆژیای تەکفیری، و راستکردنەوەی رەوتی ژیانیان، و دورخستنەوەیان لە کاری تیرۆریستی، هەنگاوێکی گرنگ پێشدەکەوێت.

لە بەشی دووەمدا، (UCTM)پێشنیار کراوە بۆ جێگرەوەی متمانە. هەروەها سیستمی بەڕێوەبردنی متمانە، (ترەست مەنجمێنت سیستم TMS) لە دارك وێب دا بۆ جێگرتنەوەی (سەبجێکتڤ ریکۆمێندەیشن SR). ئەم پرۆژەیە دەتوانێت ئەو (نۆد)، یان کەسانەی بۆ مەبەستی تیرۆر، دارك وێب بەکار دەهێنن بدۆزێتەوە. پرۆژەکە (TMS)ی پێشنیار کردوە تا کەسی بەئامانجگیراو، خۆی بتوانێت ترەستی پەیوەندییەکەی بپێوێت و ناچار نەبێت لەسەر بنەمای دەنگدانی نۆدەکانی تر، بە ترەستی پەیوەندییەکە، متمانەی خۆی بەو ئاڵوگۆڕە ئەلیکترۆنییە ببەخشێت کە لە دارك وێب دا روو دەدات.

ئەنجامی ئەم توێژینەوەیە دەتوانرێت لە دەوڵەمەندکردنی دیبەیتی ئەکادیمی لەسەر بابەتی کاونتەر سایبەر تیرۆیزم، و لە بەرهەمهێنانی نۆڵجی تایبەت بە دی-رادیکاڵیزەیشن، لە سورفەیس وێب دا، و لە دارك وێبیشدا بۆ دیبەت کردن لەسەر ترەست مۆدیلی پێشنیارکراو بۆ کاونتەر سایبەر تیرۆریزم بەکاربهێنرێت .

هەروەها لە بواری پراکتیکی دا ئەم توێژینەوەیە دەتوانێت رۆڵی هەبێت لە خستەسەرپێ و بنیادنی کاونتەر سایبەر تیرۆریزم ئۆرگانیزەیشن، کە لە هەردو ئاستی سورفەیس و دارك وێبی ئینتەرنێت دا، لە بوارەکانی دۆزینەوە و دەستنیشان کردنی کەسانی توندڕەو، و لە روبەڕوبوونەوەی شەڕی سایکۆلۆژی لەگەڵ گڵۆباڵ تیرۆریزم، و بۆ سەرخستنی دی-رادیکاڵیزەیشن و رێگرتن لە تێوەگلانی زیاتری کەسانی تازە پەیوەندیکردو بە نێتۆرکە تیرۆریستییەکانەوە، رۆڵ ببینێت. لە دژایەتی کردنی تیرۆر، و لە روبەڕوبوونەوەی سایبەر تیرۆریزم، بۆ پاراستنی ئاسایشی تاك و گروپ و دەوڵەتەکان بەسود بێت, و بەشداری بکات لە رێگرتن لەو هەڕەشە و مەترسییە شاراوانەی کە سایبەر تیرۆریزم لە دارك وێبەوە، لە دژی ئاسایشی سیستم و ژێرخان و ژینگە و کۆی بەها مرۆڤایەتییەکان، رۆژانە بەرهەمی دەهێنێت.

مۆدێلی متمانەی یەکخراوی سایبەر بۆ قەڵاچۆکردنی
سایبەرتیرۆریزم لە سورفەیس و دارك وێب

نامەیەکە پێشکەش کراوە بە
ئەنجومەنی کۆلێجی زانست / زانکۆی سلێمانی
وەك بەشێك لە پێداویستییەکانی بەدەست هێنانی
بڕوانامەی دکتۆرا لە زانستی کۆمپیوتەر
(سایبەر سیکیوریتی)

ئامادە کردن و نوسینەوەی لەلایەن
ئاڵا عومەر ئەحمەد

بە سەرپەرەشتی

پرۆفیسۆری یاریدەدەر
دکتۆر نزار عبدالقار علی

زانکۆی سلێمانی

ساڵی کوردی	ساڵی زاینی
٢٧١٩ خەرمانان	سێپتەمبەر ٢٠١٩