IN THE NAME OF ALLAH,
THE MOST GRACIOUS,
THE MOST MERCIFUL

Kingdom of Saudi Arabia
Ministry of Education
Majmaah University

جامعة المجمعة
Majmaah University

JEAS

JOURNAL OF ENGINEERING AND APPLIED SCIENCES

A Refereed Academic Journal Published by the
Publishing and Translation Center at Majmaah Universtiy

Vol. 6, Issue (2) (November - 2019) ISSN: 1658 - 6638

Publishing & Translation Center - MU

About the Journal

Journal of Engineering and Applied Sciences (JEAS)

Vision

Pioneer journal in the publication of advanced research in engineering and applied sciences.

Mission

A peer-review process which is transparent and rigorous

Objectives

a) Support research that addresses current problems facing humanity.

b) Provide an avenue for exchange of research interests and facilitate the communication among researchers.

Scope

JEAS accepts articles in the field of engineering and applied sciences. Engineering areas covered by JEAS include:

Engineering areas

Architectural Engineering
Chemical Engineering
Civil Engineering
Computer Engineering
Electrical Engineering
Environmental Engineering
Industrial Engineering
Mechanical Engineering

Applied Sciences areas

Applied Mathematics
Applied Physics
Biological Science
Biomathematics
Biotechnology
Computer Sciences
Earth Science
Environmental Science

Computer Sciences areas

Computer Sciences
Information Technology
Information Sciences
Computer Engineering

Correspondence and Subscription

Majmaah University, Post Box 66, Al-Majmaah 11952, KSA
email: jeas@mu.edu.sa

All ideas herein this Journal are of authors and do not necessarily express the Journal view

Journal of Engineering and Applied Sciences

Editorial

Scientific publishing has brought many challenges to authors. With increasing number of scientific journals, varying scopes, reviewing requirements, and cost of publishing to authors, finding the right journal to publish an article is a decision many authors must bitterly confront and resolve. The publication of scientific findings is an integral part of the life of researchers. The process of publishing has evolved to become an efficient system of decimating knowledge and collaboration among scientists. Science journals have institutionalized procedures to manage large volume of article submissions per year. In many cases, journals began to define narrower scopes for a dual purpose: managing submissions and delivering outstanding research.

Based on recent studies, the scientific publishing world consists of more than 25 thousand active journals in various disciplines and fields. Science Direct hosts 3,348 journals (as of February 2014). The Directory of Open Access Journals lists in its search engine more than 9,800 open access online journals.

According to recent estimates, the number of scientific journals grows by 3% per year worldwide. With this large number of journals, journals may find it harder to stay afloat.

In its inauguration, the board of editors is honored to introduce to the scientific community the Journal of Engineering and Applied Sciences - JEAS, another scientific journal from Majmaah University. The board has pledged a commitment to JEAS authors and readers to bring the most dynamic and vibrant journal management with better satisfaction.

Dr. Mohamed Alshehri

Contents

ORIGINAL ARTICLES

Attack on SDN Infrastructure and Security Measures

Hisham Al-Saghier *

Department of Information Technology,College of Computer & Information Sciences,
Majmaah University, Majmaah-11952, Saudi Arabia, h.alsaghier@mu.edu.sa

Abstract

Software Defined Networking (SDN) decouples the network control and network forwarding elements. The centralized controller manages the network and controls the data flow in the network elements. It has received significant attention from industry and researchers, and it has been deploying in different scenarios and environments. A centralized network plane supports programmable network management and flexibility. However, it introduces a single point of failure and scalability issues. SDN security has become a concern and many security challenges are introduced. The control plane still suffers from the number of threats such as a distributed denial of service (DDoS), man in the middle (MITM), and information modification attacks. To address these limitations, we propose a robust, secure, collaborative agent-based SDN infrastructure to detect and mitigate the attacks. We simulate and evaluate the performance of the proposed system when SDN control plan is compromised at build and run time. Simulation results show that security solutions are effective to mitigate the attacks.

Keywords:

Software Defined Networking(SDN);SDN Security; Distributed Denial of Service (DDoS) Attacks

1. Introduction

SDN network devices are divided into two layer’s control plane and data plane [1]. While the data plane is just a fast packet processing layer the control plane deals with various routing protocols and maintains forwarding states [2]. So the control plan has become very complicated and it has led networks to be unstable and difficult to manage. And also these devices are closed and proprietary and it has been a barrier to innovation.

In traditional Networks Control plane is implemented with complicated software and ASIC, it was unstable and increased complexity in management. The platform is closed means vendor-specific and it was hard to modify, hard to add new functionalities, so software defined networking (SDN) comes into existence with separate control plane from the data plane. Advantage of SDN over Traditional Network, SDN provides solutions to current network infrastructure issues such as scalability, reliability, and security [3].

In SDN, the control plane is decoupled from the network devices and the controller manages the entire network in a centralized manner [4]. A centralized network plane supports programmable network management and flexibility. In this way the controllers can easily provide and maintain the global network view and controllers implement northbound API [5]. SDN is a Programmable network i.e. it provides fixed and dynamic network control [6].

However, it introduces a single point of failure and scalability issues. Researchers proposed multiple SDN controllers' architectures to address the challenges with a single point of failure [18].

The Control plane remains the main component in the networks, and attacking the control will compromise the entire network. The control plane still suffers from several threats such as a denial of service (DoS), man in the middle (MITM), and information modification attacks.

Another advantage of SDN is that it is possible to build a network with commodity servers and switches so the cost can be significantly reduced. A lot of challenges arise in SDN due to SDN application and controller have complete control of the network; controller and SDN Applications are built on the general-purpose computing platform. If the controller or application is compromised the whole network is compromised. So it is very hard to prevent all attacks. Many researchers have investigated the attack and vulnerabilities in SDN [7-9] suggested countermeasures [10-12] with different aims. Also, researchers have investigated the detection of network anomalies using the machine learning approach [13-14].

In this paper, attacks are characterized as misconfiguration, malware and insider attack. Detection and countermeasures are the main theme of this paper and proposing an agent-based security framework to collect network traffic from the forwarding plane, apply classification algorithms to detect network anomalies.

This paper is organized as follows. Section 1 includes the introduction, purpose, and significance of this research. Section 2 discussed the related work-study in the domain of SDN Security, Section 3 discussed current SDN infrastructure & security issues, Section 4 discussed the proposed framework, Section 5 discussed the implementation, identification of vulnerabilities, testing method, analysis of computed results, and countermeasures for vulnerabilities. Finally, the main findings and results discussed in the conclusion.

2. Related Work

This section highlights the work done in the domain of SDN security, we classify the relevant research work as SDN overview, security issues & challenges, threats, attack, performance issues of current SDN controllers and countermeasure.

In [1], the authors have discussed SDN network architecture, network services, security and privacy, operating systems security including distributed control plane and SDN security. Reference [5] proposed a distributed controller's architecture for SDN to address scalability and reliability. Relationship between SDN (programmable network) and network virtualization discussed in [6]. In [15] authors proposed a hybrid hierarchical control plane to improve the scalability of an SDN based large-scale networks and fast rerouting algorithm. In [16] authors proposed multiple-controller architecture based on a distributed rule store. In the distributed rule, the application layer calculated the flow rules and distributed it to multiple controllers to resolves the security and performance issues.

Classification of SDN hypervisors and proposed framework for SDN hypervisors are discussed in [17]. In SDN challenges are network's scalability, reliability, and availability, to resolve the issues authors in [18] proposed multiple controller architectures. In [19] authors discuss SDN issues and challenges and proposed mitigation techniques to address security, reliability, scalability, availability, resiliency, and performance. Reference [20] proposed Control path management framework for multi-lateral SDN network to address reliability, control path reliability algorithms also enhance the system performance. In [21] authors discussed software defined networking architecture, challenges, security attacks, countermeasures, and research trends.

In [22], [23] authors proposed Integrated Network Functions Virtualization (NFV) and SDN architectures, NFV virtualize the network and deploy into hardware, while SDN makes networks programmable, to address reliability, performance, and scalability problems. In [24] authors proposed a cross-domain SDN architecture that supports dynamically provision of various applications and services like configuration management and decision making to address challenges and open issues of SDN based network. In [25] authors proposed and implemented a machine learning (ML) based (DDoS) attack detection system, with very well more than ninety percent detection accuracy with a low false-positive rate.

Evolution of SDN and security attacks on SDN i.e. spoofing, tampering, repudiation, information disclosure, denial of service, as well as controls/countermeasures i.e. firewalls, IDS/IPS, access control, auditing, and policy management are discussed in [26]. Security development lifecycle to address threats, risks, and vulnerabilities are discussed in [27]. In [28] authors discussed challenges due to attacks in SDN and proposed a holistic security architecture approach. Reference [29] proposed a programmable data plane to address the configuration attack. In [30] authors proposed Data-Plane extensions to secure the switches and router against Configuration attack. Address resolution protocol poisoning attack i.e. man in the middle attack (MITM) attacks are discussed in [31] and suggested a technique from the ARP Poisoning attack to protect data center networks on SDN. In [32] Due to IoT, cyber-resilient SDN based smart grid is needed, the possible security attacks on the network such as IP spoofing and (DDoS) attacks are discussed and proposed framework to assess security risks.

Distributed Denial of Service (DDoS) attacks or misconfiguration attacks in SDN infrastructure are discussed in [33-35]. Distributed denial-of-service (DDoS) attacks, detection, and protection mechanism in large scale Network are discussed in [33] DNS amplification attack under the threat of Denial of Service affect the DNS server discussed in [34]. DDoS flooding attack problems and countermeasures are discussed in [35]. Defense mechanisms against DDoS Attacks in SDN are discussed in [36]. In [3] authors discuss the advantage of SDN over the traditional network. SDN vulnerabilities caused (DDoS) attack, proposed Advanced Support Vector Machine (ASVM) algorithm to detect DDoS attacks.

Malware attacks, detection and countermeasures on SDN Infrastructure are discussed in [7-11], [14], [37-46]. In [37] authors discussed Open issues in SDN security and proposed security framework for empirical evaluation of classifier security based on attack pattern. In [10] authors discussed possible solutions against DDoS attacks in SDN. Reference [38], [39] discussed how ML help in malware detection and suggested some countermeasures. In [40] authors discussed and implemented Malware hybrid detection using the static and dynamic approach. In [14] authors proposed a method using a machine learning approach to detect unknown malware from executable files based on micro-patterns. In [41] authors proposed ML behavior-based malware detection model. Reference [42], [43] proposed a linear, central and mesh-based approach to mitigate the DDoS attacks in real-time large SDN based Networks. In [9] authors proposed a framework to detect and mitigate Application-specific DDoS attacks. In [44] authors proposed a secure autonomous response network (SARNET) based on SDN and NFV.

In [8] authors proposed a flow-table sharing approach to protect the SDN-based cloud from flow table overloading DDoS attacks by using idle flow-table of other Open Flow. In [11] authors proposed a framework to countermeasure table-miss striking attacks that degrade the performance of the controller.

In [45] authors proposed a secure framework against DDoS attacks to secure application servers as well as other network resources. In [46] authors discussed issues in SDN security, present a comparison of IDS approaches based on machine learning and deep learning approach. Reference [7] discussed DDoS attacks and DDoS detection algorithm to find the attack path using minimum network resources and in minimum time. In [47], [48] authors discussed security threats including masquerading and encrypted attack.

3.SDN & Security Issues

SDN architecture is shown below in Fig. 1. It separates control and data planes to optimize the network workload which provides high speed and intelligence of using the network resources. Also, the control plane provides practical and easy network management via network services. The control plane consists of a controller with Northbound and East/Westbound API. Northbound API enables applications to communicate with the control layer. East/westbound interfaces also allow multiple controllers to interact in distributed SDN [6], [49-50].

SDN controllers i.e. Network operating system (NOS) are external logical entities that enable the network operator to program and manage the forwarding devices based on a logically centralized network view. SDN control plane manages the data plane elements by translating the application layer policies to the underlying data plane devices and provide the network information about the network to the management plane. The basic design of the control plane is using one controller to manage the whole network. However, in the case of large scale networks, multiple controllers are used. Data plane (infrastructure layer), comprises of connected network devices that forward the network data flows based on the assigned flow rules.

The control plane implements these rules through the southbound. The southbound interface allows the control plane to communicate and control the forwarding devices. Open Flow is the main SDN protocol that is used for communication between the data plane and the controller through a secure channel that is usually a TLS/SSL. A centralized network plane supports programmable network management and flexibility. However, it introduces a single point of failure and scalability issues. Fig. 1 shows the SDN threats are attacks on data-control and control-application interfaces, attacks, and vulnerabilities in controllers and application layers.

Fig. 1. Software Defined Networking Architecture

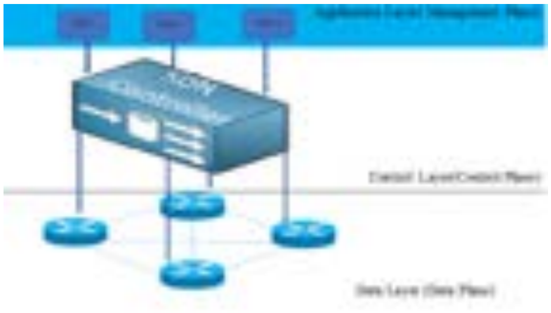
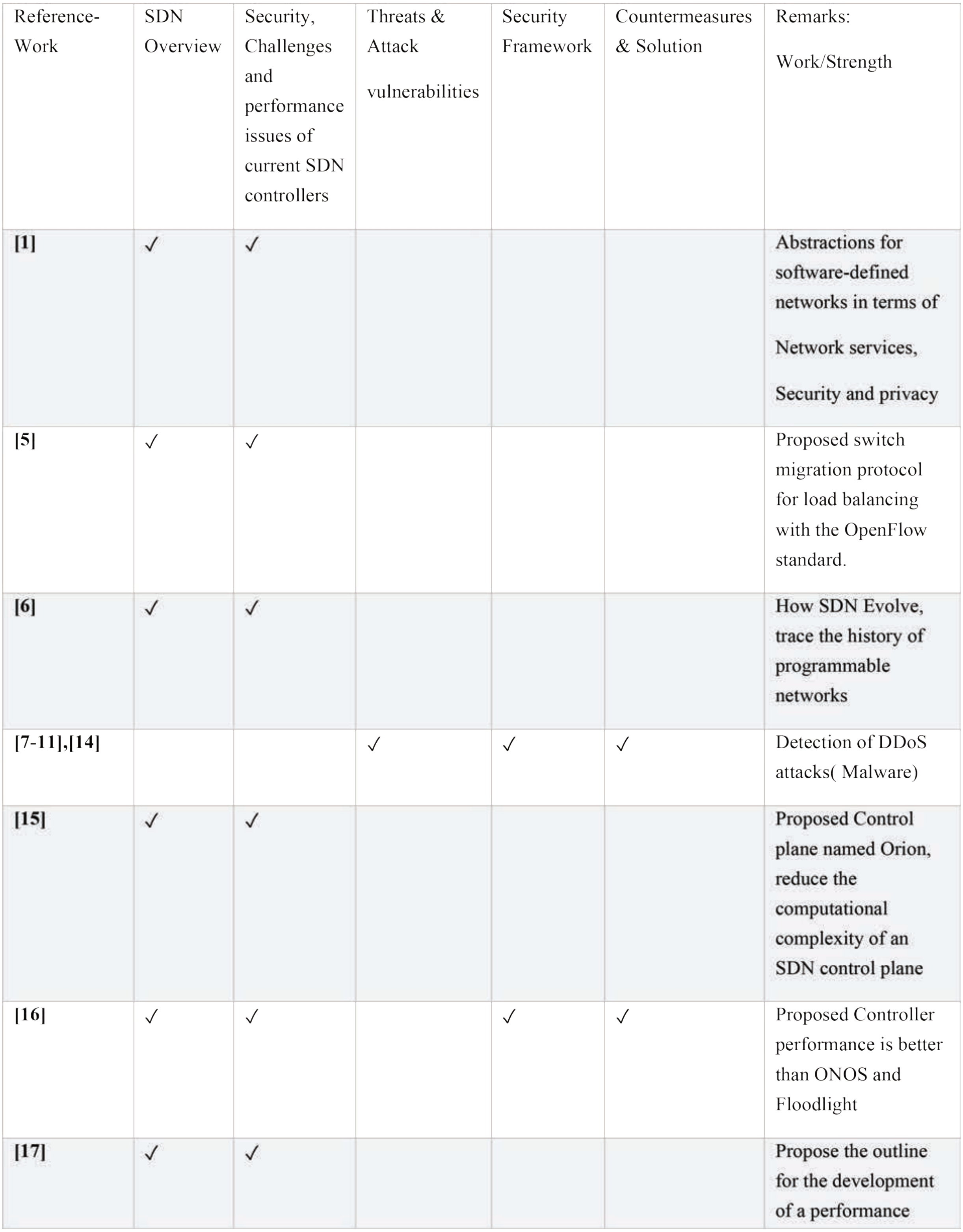
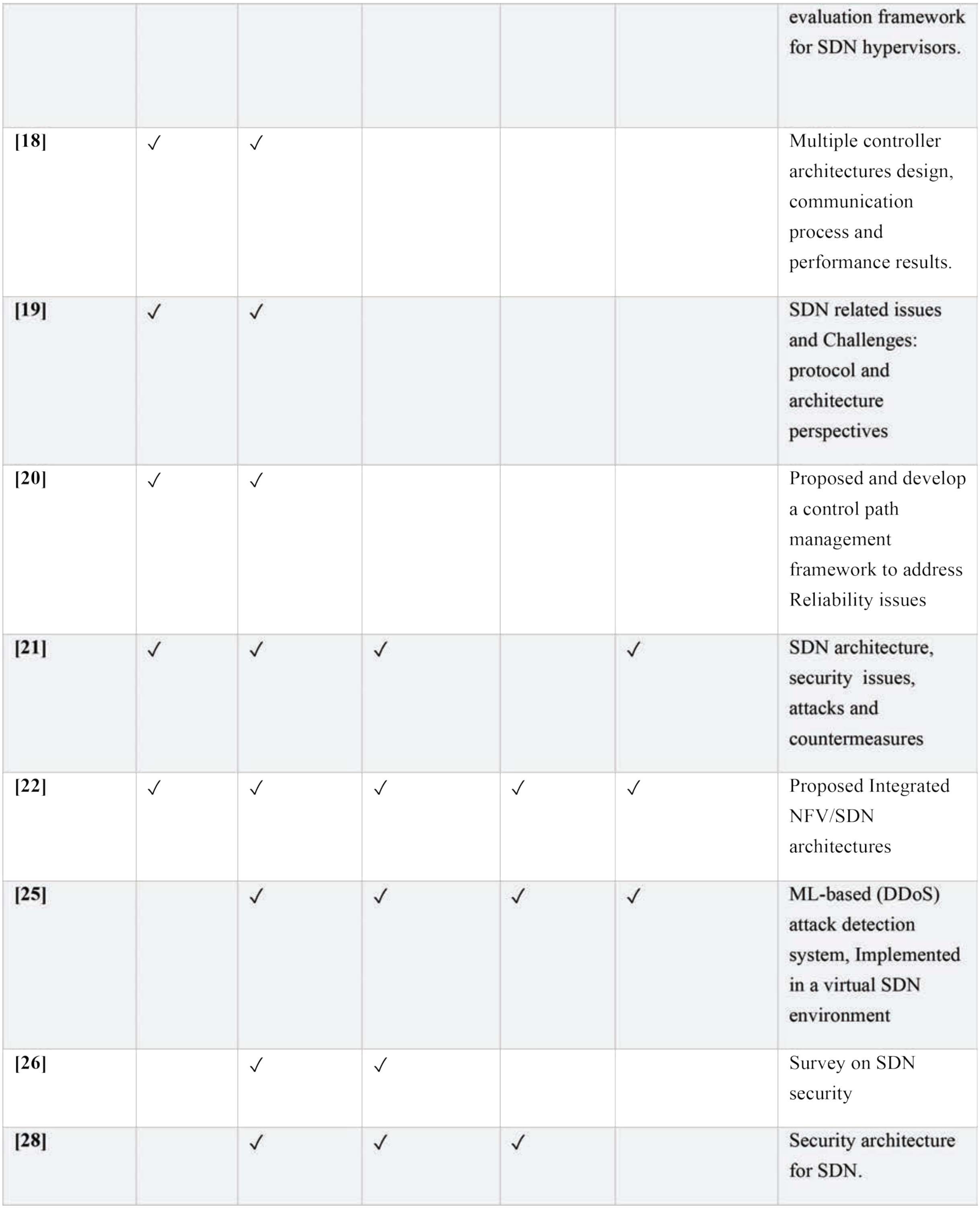

Application Layer (Management Plane)
SDN Controller
Control Layer(Control Plane)
Data Layer (Data Plane)

Table 1. Summary of the Literature Review



Reference-Work	SDN Overview	Security, Challenges and performance issues of current SDN controllers	Threats & Attack vulnerabilities	Security Framework	Countermeasures & Solution	Remarks: Work/Strength
[1]	✓	✓				Abstractions for software-defined networks in terms of Network services, Security and privacy
[5]	✓	✓				Proposed switch migration protocol for load balancing with the OpenFlow standard.
[6]	✓	✓				How SDN Evolve, trace the history of programmable networks
[7-11],[14]			✓	✓	✓	Detection of DDoS attacks(Malware)
[15]	✓	✓				Proposed Control plane named Orion, reduce the computational complexity of an SDN control plane
[16]	✓	✓		✓	✓	Proposed Controller performance is better than ONOS and Floodlight
[17]	✓	✓				Propose the outline for the development of a performance



						evaluation framework for SDN hypervisors.
[18]	✓	✓				Multiple controller architectures design, communication process and performance results.
[19]	✓	✓				SDN related issues and Challenges: protocol and architecture perspectives
[20]	✓	✓				Proposed and develop a control path management framework to address Reliability issues
[21]	✓	✓	✓		✓	SDN architecture, security issues, attacks and countermeasures
[22]	✓	✓	✓	✓	✓	Proposed Integrated NFV/SDN architectures
[25]		✓	✓	✓	✓	ML-based (DDoS) attack detection system, Implemented in a virtual SDN environment
[26]		✓	✓			Survey on SDN security
[28]		✓	✓	✓		Security architecture for SDN.

[29]		✓	✓	✓	✓	Proposed Programmable data plane (PD) Concept
[30]		✓	✓	✓	✓	SDN-based data plane architecture called DPX that supports security services.
[31]		✓	✓	✓	✓	Suggesting a technique to protect the data center networks from the ARP Poisoning attack using SDN
[32],[33],[34]		✓	✓	✓	✓	A framework to assess security risks within an SDN-enabled smart grid communication
[35],[36]			✓	✓		Identification and counter measure of Misconfiguration Attacks on SDN Infrastructure
[37],[38],[39] [40] ,[41], [42] ,[44], [45]			✓	✓	✓	Identification and countermeasure Malware Attack on SDN Infrastructure
[47],[48]			✓	✓	✓	Identification and countermeasure of an insider attack on SDN Infrastructure

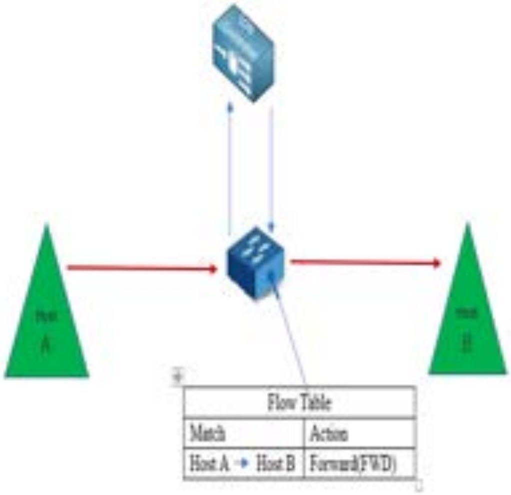
An attacker can exploit the weakness of the TLS/SSL communication channel between the SDN devices and the controller to launch attacks. Malicious SDN controllers and applications can be used to compromise the network. Other threats are forged traffic from data devices, malicious switches, vulnerabilities of administration station. Even though these threats are not specific to SDN networks, the impact on the SDN networks is more severe than traditional networks.

An attacker can use fake traffic to launch DoS/DDoS attacks on SDN switches and controllers. Also, an attacker can exploit switches vulnerabilities and then launch serious attacks against the network entities such as dropping or slow down network data flows and overloading controllers with request packets.

3.1 SDN Operation

Fig. 2 shows network topology with one SDN switch and two network hosts A and B. The switch is connected to an SDN controller.

Fig. 2. Basic SDN Operation



Flow Table	
Match	Action
Host A → Host B	Forward(FWD)

If in this network host A wants to try to talk to host B the switch doesn't know what to do with the packet received from host A, because it doesn't have its controlled plane anymore, so it queries a controller and the controller instructs the switch to forward all the packets from host A to host B by installing this flow Rule. So once this flow rule is installed host A can talk to host B. Some attack factors that could affect SDN infrastructure and particularly on data centers.

Modern data centers deal with a lot of virtual machines. The East-West traffic that travels within the data center has become dominant [51], [52] as shown in Fig. 3. The data centers have recently started employing this leaf-spine design that reduces the latency and the possible bottlenecks caused by the switch with traffic. But even with this new design, there remain other challenges to be solved. So that data center should be able to deal with frequent migrations and also a large number of links. And it is still expensive to scale and maintain the data centers. So this software defined data center(SDDC) is rapidly gaining attention as it can solve the challenges.

The SDDC can reduce the complexity by leveraging the global network view and network program ability offered by SDN and it is also possible to reduce the capital expenditure by building and scaling the data center with commodities servers and switches and also it is possible to readjust the operational costs by centralizing and automating a lot of management tasks.

The control plane is also scalable because it is always possible to spawn more virtual machines to host more controller nodes if needed. The complexity of the network is low, with a global network view, low cost, centralized and automated management, highly available and scalable control plan, distributed SDN controller, VMs to host the controller Nodes.

4. Proposed Frame Work: SDN Security Evaluation

The purpose of the proposed framework shown below in Fig. 4, is to automatically instantiates known attacks against SDN elements across the diverse environment and assists unknown security problems within SDN Deployment. Additional components are agent manager, application agent, agent channel and agent host. Agent Manager control all the additional component, and it runs on managed code i.e. router, controller and forward notification to the application agent, agent channel and agent host. The application agent is an autonomous agent or intelligent agent work in a dynamic environment responsible for achieving goals into actionable tasks. The agent channel is responsible for online channel management, distribution channels effectively among the components. Agent hosts are managed code runs into the data plane.

5. Performance Evaluation

The attack vectors that could affect the

SDN infrastructure are misconfiguration, malware and insider attacks. We simulate and evaluate the performance of our system under these attacks

- Malware 1, Due to this SDN control plane compromises at build-time

- Malware 2- SDN control plane compromises at run-time

5.1. Simulation Set up

Steps:

1- Fetching ONOS source

2- Building ONOS with Maven

3- Creating ONOS package that is deployed in a control plane

4- Deployed this package (ConFig.d to form a three-node ONOS Cluster) to three virtual machines (VM)

5- Reverse cell connected (attacker host)- Three node ONOS cluster created (Victim ONOS)

SDN Control Plane Components: The controllers that we consider in virtual SDN infrastructure are open network operating system(ONOS), and open daylight (ODL). Distributed network operating system, provide a base design for commercial SDN controller products, for example, brocade SDN and controller is based on open daylight.

So the first attack vector is a misconfiguration, on ONOS and open daylight, both implement various interfaces for management purpose and if an attacker can gain access to any one of these interfaces the attacker can freely manipulate the entire SDC network. And regarding this attack vector ONOS and the open daylight community have relieved the security guideline and possible mitigation would be changing default credentials and properly configuring the network.

Second Attack Vector Malware, Malware infection at build time and at run time, Also ONOS is prone to malware and the infection can take place during the build and run time. The possible defense is, to download the project source from a trusted source code repository.

Fig. 3. Software Defined Data Center(SDDC) Network Design and Attack Vector

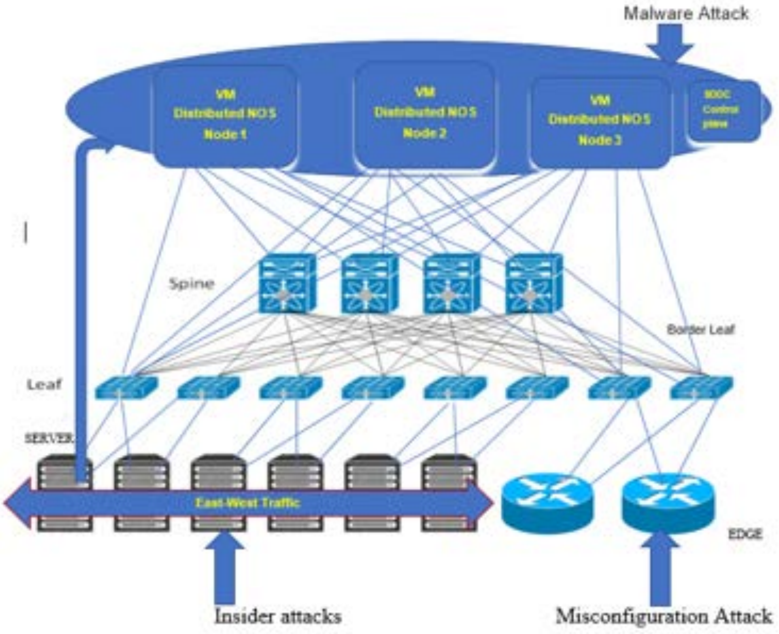
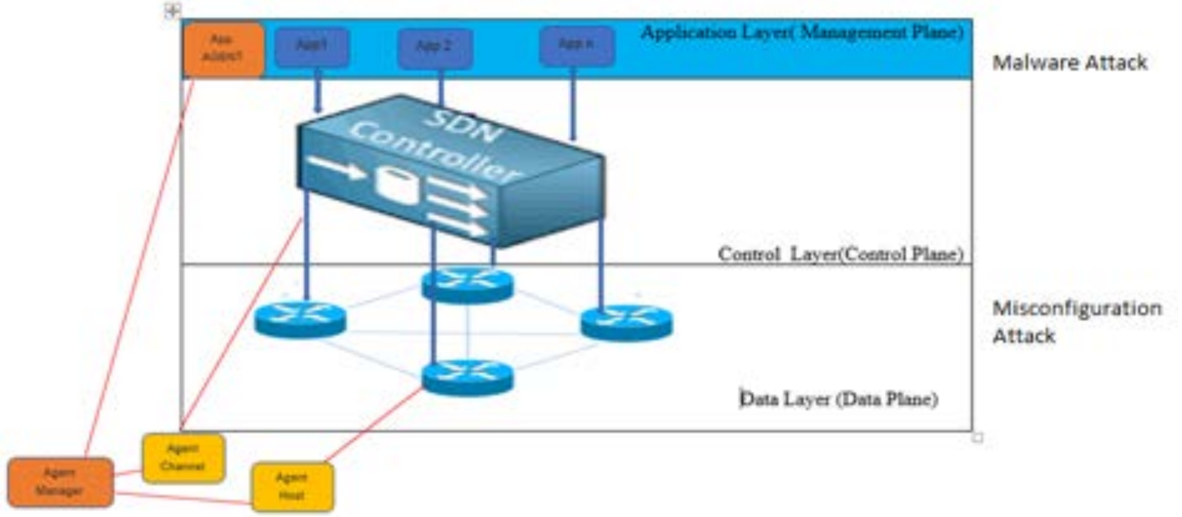


Fig. 4. Proposed Frame Work



Attack Vector - Malware 1, due to this SDN control plane compromises at build-time, it will manipulate host file and settings. If there was a network attack against the built environment, the malicious library could have been pulled from untrusted repositories and injected into the deployable package and causes DNS cache poisoning and ARP spoofing attack. And if this infected package is deployed this may put the entire data center at risk.

Another attack vector (Malware 2- SDN control plane compromises at run-time) is malicious SDN applications, ONOS, and open daylight both support the deployment of SDN applications. So that network administrators and operators can easily install SDN and applications using CLI, GUI or rest API. So to make them download and install malicious applications social engineering texts can be used and once this malicious application is installed. The application can manipulate the behavior of the control plane and the entire network.

And lastly, the SDDC control plane is also prone to insider attacks launched by malicious tenants. The malicious tenants may generate massive network flows to saturate the control plane and also they may send out crafted packets to manipulate the global network view maintained by the controller.

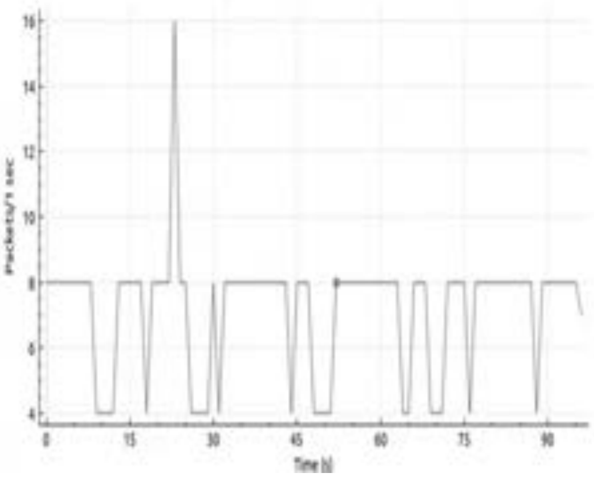
The attack scenarios

Compromising SDN control plane at build time and run time. Two attack scenario is discussed and implemented that breaks the SDDC infrastructure.

In the first attack scenario, we assume that the victim has built on us in an insecure environment and we use a maven repository to inject the malicious library into the deployment package. Once this infected package is deployed the malicious code will be executed and the attacker will get remote access to each hosted control or host machine and then will try to inject an arbitrary ONOS note to the control plane. An ONOS package that is deployable to the control plane. And deploying the package to three different virtual machines. ONOS deployed on the cluster. We have three nodes on the ONOS cluster form and the attacker host. We have a reverse shell connected back to the attacker. And the attacker host it is possible to access and modify all of the onus configurations including the credentials to access CSI and GUI and also rest API. And also it is possible to modify the cluster configurations. So going to manipulate the cluster configurations to inject an unauthorized ONOS node to the cluster. So once the cluster restarts, it has four nodes on this cluster including one unauthorized node and the attacker can easily access the control plane and manipulate the entire SDN network with this unauthorized name.

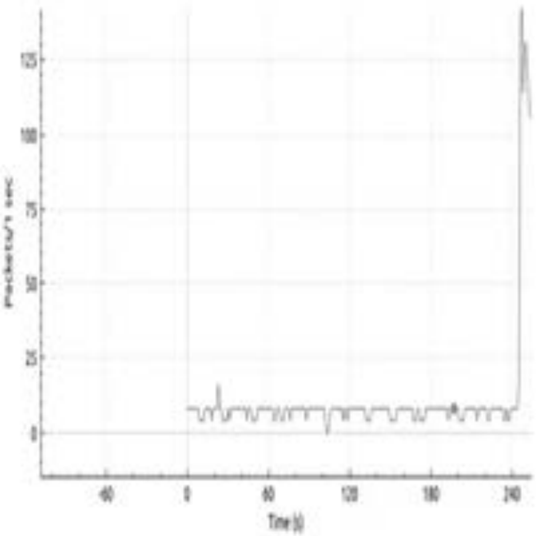
Analysis of the simulated network is also evaluated through Wireshark. Input-Output (IO) graph of Network is in under Normal Operation shown as in Fig. 5.

Fig. 5. Normal Traffic IO Graph



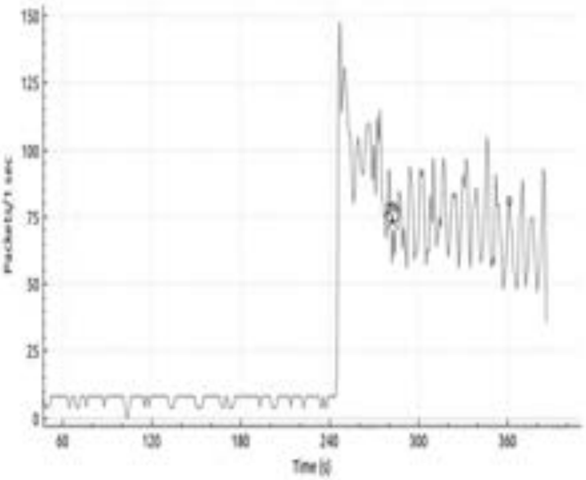
Flood traffic from host h2 to h1 (Victims) is shown in Fig. 6. A sudden higher spike represents the flood traffics.

Fig. 6. DDoS IO Graph



Mitigation of DDoS Attack is shown in Fig. 7, mitigating the malicious traffic which is flooding our victims, in this case, it will be host 1(H1). The sudden drop in the graph shows mitigation is applied

Fig. 7. Mitigation Flow IO graph



The second scenario demonstrates the threat of malicious SDN applications. In this case, we assume that the network operator has been fooled by social engineering attack and downloaded a malicious SDN application. So once the application is installed to the SDN controller Cluster. The application stealthily degrades the over network performance by abusing a weakness of a particular switch form here.

So as a proof of concept we use a simple test that consists of 1 switch device and 2 Network hosts. We have open data like controller console and on the right, we have one of the network costs for performance measurement. And manager assistant application and the other bundles running inside a controller. So when the switches are connected to the controller on the network host we perform the ping test to show our network performance.

Attacks are due to vulnerabilities in the proposed virtual SDN network, the following vulnerabilities are identified;

1- No System Integrity Protection-There is no System Integrity Protection for the NOS component. The integrity of the CORE NOS component must be guaranteed. The first problem is that there is no system where protection for NOS in controllers. Deemed malicious libraries can be injected in the build process and the source code of the SDN controller could be manipulated before a building. But currently, since there is no mechanism to detect a loss of time integrity to the operator might directly deploy a compromise testing controller to the network. So. The code signing or other intuitive The second scenario demonstrates the threat of malicious SDN applications. In this case, we assume that the network operator has been fooled by social engineering attack and downloaded a malicious SDN application. So once the application is installed to the SDN controller Cluster. The application stealthily degrades the over network performance by abusing a weakness of a particular switch form here.

So as a proof of concept we use a simple test that consists of 1 switch device and 2 Network hosts. We have open data like controller console and on the right, we have one of the network costs for performance measurement. And manager assistant application and the other bundles running inside a controller. So when the switches are connected to the controller on the network host we perform the ping test to show our network performance.

Attacks are due to vulnerabilities in the proposed virtual SDN network, the following vulnerabilities are identified;

1- No System Integrity Protection-There is no System Integrity Protection for the NOS component. The integrity of the CORE NOS component must be guaranteed. The first problem is that there is no system where protection for NOS in controllers. Deemed malicious libraries can be injected in the build process and the source code of the SDN controller could be manipulated before a building. But currently, since there is no mechanism to detect a loss of time integrity to the operator might directly deploy a compromise testing controller to the network. So. The code signing or other intuitive protection mechanisms such as checksum could be possible solutions to this problem.

2- No authentication of SDN cluster nodes- This is a serious threat because the arbitrary on ONOS node can completely take over the control of the entire control plane into a network. public key infrastructure (PKI) based authentication could be one of the possible defenses of this threat.

3- No application access control- These applications are granted very powerful authority even though they are just applications running on an operating system. So application including even malicious one can access the core of the controller and freely manipulate the network behavior. The police based access control mechanism could be useful.

4- Switch device firmware Abuse- It degrades the network performance. In SDN, devices implement both hardware-based and software-based flow table. So if a packet is matched by looking up the software table it incurs significant overhead, so such packet matching strategies may vary, depending on the vendor and firmware version. Defense flow rule conflict detection and arbitration possible defense mechanism to mitigate such an attack could be detected and arbitrating global conflicts.

6. Conclusion

The paper aims to design and evaluate the SDN Security framework, that addresses the limitation and detects and mitigates the attacks. Attacks are characterized as misconfiguration, malware, and insider attack. In this paper we discussed SDN Architecture, SDN operation, attacks on software defined Data Center(SD-DC). Literature review section highlights the work done in the domain of SDN security and countermeasure. Simulation and performance evaluation was evaluated due to misconfiguration, malware and insider attack. Attacks are due to vulnerabilities in the proposed virtual SDN network, the main vulnerabilities are identified as no system integrity protection, no application access control and switch device firmware abuse. Possible defense and countermeasures of are discussed. Future work can also involve improving in Software defined data center (SDDC) security architecture with additional resilient recovery mechanisms.

References

Casado, M.; Foster, N.; Guha, A. (SDN Abstraction, Overview) Abstractions for software-defined networks. Commun. ACM 2014, 57, 86–95.

Akyildiz IF, Lee A, Wang P, et al., 2014. A roadmap for traffic engineering in SDN-OpenFlow networks. Comput Netw, 71:1–30.

Myint Oo, Myo, Sinchai Kamolphiwong, Thossaporn Kamolphiwong, and Sangsuree Vasupongayya. “Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN).” Journal of Computer Networks and Communications 2019 (2019).

Salsano S, Blefari-Melazzi N, Detti A, et al., 2013. Information-centric networking over SDN and OpenFlow: architectural aspects and experiments on the OFELIA testbed. Comput Netw, 57(16):3207–3221.

Dixit A, Hao F, Mukherjee S, et al., 2013. Towards an elastic distributed SDN controller. ACM SIGCOMM Comput Commun Rev, 43(4):7–12.]

Feamster N, Rexford J, Zegura E, 2014. The road to SDN: an intellectual history of programmable networks. ACM SIGCOMM Comput Commun Rev, 44(2):87–98].

Chen, Wen, Suchao Xiao, Leijie Liu, Xueqin Jiang, and Zhangbin Tang. “A DDoS attacks traceback scheme for SDN-based smart city.” Computers & Electrical Engineering 81 (2020): 106503],

Bhushan, Kriti, and Brij B. Gupta. “Distributed denial of service (DDoS) attack mitigation in the software defined network (SD-N)-based cloud computing environment.” Journal of Ambient Intelligence and Humanized Computing 10, no. 5 (2019): 1985-1997.

Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah. “DDoS attack detection and mitigation using SDN: methods, practices, and solutions.” Arabian Journal for Science and Engineering 42, no. 2 (2017): 425-441.

Kalkan, Kubra, Gurkan Gur, and Fatih Alagoz. “Defense mechanisms against DDoS attacks in the SDN environment.” IEEE Communications Magazine 55, no. 9 (2017): 175-179.

Xu, Jianfeng, Liming Wang, and Zhen Xu. “An enhanced saturation attack and its mitigation mechanism in software-defined networking.” Computer Networks (2019): 107092.

Sufian Hameed ,ID and Hassan Ahmed Khan, SDN Based Collaborative Scheme for Mitigation of DDoS Attacks,2018 MDPI

Sen, Sajib, Kishor Datta Gupta, and Md Manjurul Ahsan. “Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS Attack.” In Proceedings of International Joint Conference on Computational Intelligence, pp. 49-60. Springer, Singapore, 2020

Hashemi, H.; Hamzeh, A. Visual malware detection using a local malicious pattern. J. Comput. Virol. Hacking Tech. 2018, 15, 1–14. [CrossRef]]

Fu, Yonghong, Jun Bi, Ze Chen, Kai Gao, Baobao Zhang, Guangxu Chen, and Jianping Wu. “A hybrid hierarchical control plane for flow-based large-scale software-defined networks.” IEEE Transactions on Network and Service Management 12, no. 2 (2015): 117-131.

Wang, Huan-zhao, Peng Zhang, Lei Xiong, Xin Liu, and Cheng-chen Hu. “A secure and high-performance multi-controller architecture for software-defined networking.” Frontiers of Information Technology & Electronic Engineering 17, no. 7 (2016): 634-646.

Blenk, Andreas, Arsany Basta, Martin Reisslein, and Wolfgang Kellerer. “Survey on network virtualization hypervisors for software defined networking.” IEEE Communications Surveys & Tutorials 18, no. 1 (2015): 655-685.

Blial, Othmane, Mouad Ben Mamoun, and Redouane Benaini. “An overview on SDN architectures with multiple controllers.” Journal of Computer Networks and Communications 2016 (2016).

Benzekki, Kamal, Abdeslam El Fergougui, and Abdelbaki Elbelrhiti Elalaoui. “Software“defined networking (SDN): a survey.” Security and communication networks 9, no. 18 (2016): 5803-5833.

Song, Sejun, Hyungbae Park, Baek-Young Choi, Taesang Choi, and Henry Zhu. “Control path management framework for enhancing software-defined network (SDN) reliability.” IEEE Transactions on Network and Service Management 14, no. 2 (2017): 302-316.

Rawat, Danda B., and Swetha R. Reddy. “Software defined networking architecture, security and energy efficiency: A survey.” IEEE Communications Surveys & Tutorials 19, no. 1 (2016): 325-346.

Bonfim, Michel S., Kelvin L. Dias, and Stenio FL Fernandes. “Integrated NFV/SDN architectures: A systematic literature review.” ACM Computing Surveys (CSUR) 51, no. 6 (2019): 114.

Hoang, Doan B., and Sarah Farahmandian. “Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies.” In Guide to Security in SDN and NFV, pp. 3-32. Springer, Cham, 2017. book

Shi, Yongpeng, Yurui Cao, Jiajia Liu, and Nei Kato. “A cross-domain SDN architecture for multi-layered space-terrestrial integrated networks.” IEEE Network 33, no. 1 (2019): 29-35.

Sen, Sajib, Kishor Datta Gupta, and Md Manjurul Ahsan. “Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS

Attack." In Proceedings of International Joint Conference on Computational Intelligence, pp. 49-60. Springer, Singapore, 2020.

Alsmadi, Izzat, and Dianxiang Xu. "Security of software defined networks: A survey." computers & security 53 (2015): 79-108.

Al-Fedaghi, Sabah, and Abdulrahman Alkandari. "On Security Development Lifecycle: Conceptual Description of Vulnerabilities, Risks, and Threats." International Journal of Digital Content Technology and its Applications 5, no. 5 (2011): 296-306.

Scott-Hayward, Sandra, Sriram Natarajan, and Sakir Sezer. "A survey of security in software defined networks." IEEE Communications Surveys & Tutorials 18, no. 1 (2015): 623-654.

Feng, Wendi, Zhi-Li Zhang, Chuanchang Liu, and Junliang Chen. "Clé: Enhancing Security with Programmable Dataplane Enabled Hybrid SDN." In Proceedings of the 15th International Conference on emerging Networking EXperiments and Technologies, pp. 76-77. ACM, 2019.

Park, Taejune, Yeonkeun Kim, Vinod Yegneswaran, Phillip Porras, Zhaoyan Xu, KyoungSoo Park, and Seungwon Shin. "DPX: Data-Plane eXtensions for SDN Security Service Instantiation." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 415-437. Springer, Cham, 2019.

Ali, Ali Faiq, and Wesam S. Bhaya. "Software Defined Network (SDN) Security Against Address Resolution Protocol Poisoning Attack." Journal of Computational and Theoretical Nanoscience 16, no. 3 (2019): 956-963.

Maziku, Hellen, Sachin Shetty, and David M. Nicol. "Security risk assessment for SDN-enabled smart grids." Computer Communications 133 (2019): 1-11.

François, J.; Aib, I.; Boutaba, R. FireCol: A collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans. Netw. (TON) 2012, 20, 1828–1841.

Anagnostopoulos, M.; Kambourakis, G.; Kopanos, P.; Louloudakis, G.; Gritzalis, S. DNS amplification attack revisited. Comput. Secur. 2013, 39, 475–485.

Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. Commun. Surv. Tutor. IEEE 2013, 15, 2046–2069.

.Kalkan, K.; Gur, G.; Alagoz, F. Defense Mechanisms against DDoS Attacks in SDN Environment. IEEE Commun. Mag. 2017, 55, 175–179.

Biggio, B.; Fumera, G.; Roli, F. Security evaluation of pattern classifiers under attack. IEEE Trans. Knowl. Data Eng. 2014, 26, 984–996. [CrossRef]

Chen, L.; Ye, Y. SecMD: Make Machine Learning More Secure against Adversarial Malware Attacks; Springer International Publishing: Cham, Switzerland, 2017; Volume 10400, pp. 76–89.

Biggio, B.; Corona, I.; Maiorca, D.; Nelson, B.; Srndic, N.; Laskov, P.; Giacinto, G.; Roli, F. Evasion Attacks against Machine Learning at Test Time; Springer: Berlin/Heidelberg, Germany, 2017; pp. 387–402.

Damodaran, A.; di Troia, F.; Visaggio, C.A.; Austin, T.H.; Stamp, M. A comparison of static, dynamic, and hybrid analysis for malware detection. J. Comput. Virol. Hacking Tech. 2017, 13, 1–12.

Galal, H.S.; Mahdy, Y.B.; Atiea, M.A. Behavior-based features model for malware detection. J.

Hameed, Sufian, and Hassan Ahmed Khan. “SDN based collaborative scheme for mitigation of DDoS attacks.” Future Internet 10, no. 3 (2018): 23.

.Kalkan, K.; Gur, G.; Alagoz, F. Defense Mechanisms against DDoS Attacks in SDN Environment. IEEE Commun. Mag. 2017, 55, 175–179.

.Koning, Ralph, Ben de Graaff, Gleb Polevoy, R. Meijer, C. de Laat, and Paola Grosso. “Measuring the efficiency of sdn mitigations against attacks on computer infrastructures.” Future Generation Computer Systems 91 • 2018

Bawany, Narmeen Zakaria, and Jawwad A. Shamsi. “SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks.” Journal of Network and Computer Applications 145 (2019): 102381.

.Hande, Yogita, and Akkalashmi Muddana. “A Survey on Intrusion Detection System for Software Defined Networks (SDN).” International Journal of Business Data Communications and Networking (IJBDCN) 16, no. 1 (2020): 28-47.

.Neu, Charles Varlei. “Detecting encrypted attacks in software-defined networking.” (2019).

Chen, Wen, Suchao Xiao, Leijie Liu, Xueqin Jiang, and Zhangbin Tang. “A DDoS attacks traceback scheme for SDN-based smart city.” Computers & Electrical Engineering 81 (2020): 106503.

Retrieved from https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf

Nunes, B.A.A., Mendonca, M., Nguyen, X.-N., Obraczka, K., Turletti, T.: A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Commun Surv Tutorials. 16(3), (2014)

Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/

white-paper-c11-731860.html.

Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-735863.pdf.

An Exploratory Study of E-Government Usage: A Saudi Perspective

Rana Alabdan*

College of Computer and Information Science, Majmaah University ,
Al Mjamaah 11952, Saudi Arabia, r.alabdan@mu.edu.sa

Abstract

Electronic technology is increasing gradually in Saudi Arabia and using e-services among Saudi users become more popular due to its effectiveness and efficiency. The aim of this study is to investigate the usage of electronic government (e-government) or (eGovernment) among Saudi users, especially with the transformation according to vision 2030. There is a vast paradigm shift in using e-government in the Kingdom of Saudi Arabia, especially with the surrounding eGovernment services such as Absher. This study will provide a thorough review of the usage of eGovernment across the regions of Saudi Arabia and the reasons for non-usage as well. The word eGovernment and E-government will be used interchangeably in the context.

Keywords:

eGov; Saudi; statistical analysis; e-government services; Absher

1. Introduction

E-government involves the application of information and communication technology (ICT) to deliver efficient services of eGovernment to the users and business owners as well (Alzahrani et al., 2017). E-government usage allows increasing the efficiency of government services provided to the users either personal or business. In the previous decade, eGovernment as a term of e-commerce has been grown dramatically. Nowadays, eGovernment has been spread widely in studying programs (MSc and Ph.D.), conferences which emphasized on this topic, journals dedicated specifically to eGovernment; books, and more than 4,630,000,000 webpages refer to eGovernment (Heeks & Bailur, 2007).

Communications in Saudi Arabia are mainly based on mobile phones. As mobile phones became widespread. On a large scale of 99.16% at the level of families in the Kingdom, which confirms the transformation and rapid spread of this service. It reveals a recent acceleration in access to information technology and the use of communications within the population. Also that 75.19% of individuals of all ages used a mobile phone. Besides, 92.66% of the individuals who ranged ages 12 to 65 years old used them in 2018 (General Authority for Statistics, 2018).

EGovernment is beneficial for users and government agencies as well (General Authority for Statistics, 2018). The government will have cost reduction and more efficiency, while users will perform faster more convenient services anytime anywhere, they prefer (Alzahrani et al., 2017). Previous researches presume that the factors influence eGovernment, i.e., technology, skills, work environment, and culture (Heeks & Bailur, 2017). In mid of 2019 the total population of Saudi Arabia was 19,739,056 males, 14,479,113 females, and a total of 34,218,169 (General Authority for Statistics, 2020).

The percentage of eGovernment usage among Saudi individuals according to gender 38.12 and 10.78 for males and females respectively, which represents 27.19 from the usage of the Internet among other services in Saudi Arabia (General Authority for Statistics, 2020). Saudi Arabia government initiated multiple projects to improve services and to shift services into another paradigm to make government services easier and more effective.

In the next few years, eGovernment projected to grows in Saudi Arabia until 2030 (Vision 2030). Nowadays, the top countries using eGovernment are South Korea, Netherlands, France, Singapore, and Australia (Clement, 2018a). The government will allow the citizen to save time and effort when services are shifted to be paperless by using different government services electronically, this will be more transparent and will fight corruption (Arab News, 2016). Saudi Arabia was ranked 36 out of 193 among countries in these services (Arab News, 2016). Further, in 2030 Saudi will be classified among the top five countries around the world, especially within the Interior Ministry system, Absher which all serve Saudi citizens and make their life easier (Arab News, 2016).

E-government in Saudi Arabia is developed under the Royal Decree by the Ministry of communication and information technology. The main goal of this government is to facilitate citizens about the quick service and enhance the efficiency of facilities. The Yesser is contributing to different government agencies to get sustainable progress, which can build structural improvement. Key services under eGovernment are Absher, medical consultancy, e-visa, umrah, instant tourism visa, and intelligent hajj, Authentication of mortgage and health services platforms (El-sofany et. al., 2012). The consequences of using e-service will be positive for the population, in terms of getting education, knowledge and seeking growth. It is relevant to Saudi Arabia due to the country's potential and growth. It will ease all the main processes and improve government productivity. Using eGovernment services from Saudi users, will spread the benefits within the country. E-government implementation in Saudi Arabia is significant and quite relevant to cater to this large population's needs. This process will empower individuals to take part in government activities. The scope of the online payment system in Saudi Arabia will get recognition at the international level.

1.1. Justification of the Study

The current study aims at discussing the vision 2030 and its impact on Saudi users, in terms of efficiency. The influence of technology on Saudi citizens can be estimated by their daily usage and dependence on technology. Due to information and communication channeling, people are more aware of global trends and get use of electronic services. This study is significant in this regard to map up government services and its benefits for citizens. The focus of this study is to convey into consideration related research papers and evidence to make it clearer for the users. This study will be beneficial to the users, in terms of information related to e-government, services efficiency, and trends of service usage in population. The study will also provide a key framework of the Saudi government for the population regarding its efficacy. This research is backed with empirical and theoretical evidence from literature.

1.2. Purpose of the Study

The main purpose of this paper is to investigate the usage of eGovernment among Saudi regions and explore the reasons to adopt/not adopt within Saudi regions. This study will answer the following research questions which will provide us with the insight of eGovernment services in Saudi Arabia:

RQ1: What are the factors which influence the adoption of eGovernment system among Saudi users?

RQ2: What are the reasons which prevent Saudi users from using eGovernment?

The study will be organized to the following structure: after the introduction, related work is presented, which is followed by the methodology. Finally, analysis and results are presented followed by the conclusion of the study.

2. Related Work

In this section, this paper will focus on eGovernment studies from a distinctive perception identifying multiple frameworks. The study of Heeks and Bailur (2007) focused on exploring eGovernment from another perspective which are models, factors' lists, or definitions. For example, it provided a deep understanding of human factors, which affect eGovernment. The researchers conducted eGovernment research using different types of knowledge frameworks (see Table 1) (Heeks & Bailur, 2007).

- Theory based work: it means using/applying/testing a theory.

- Framework based work: framework usage, which inherits from a theoretical background.

- Model based work: using a model without a deep understanding of a framework.

- Concept based work: it means using a particular concept in eGovernment.

- Category based work: this introduces a set of categories, or several factors, which is found on eGovernment.

- Non-framework-based work: this particular framework does not use distinct knowledge framework, it only delivers a set of ideas and data.

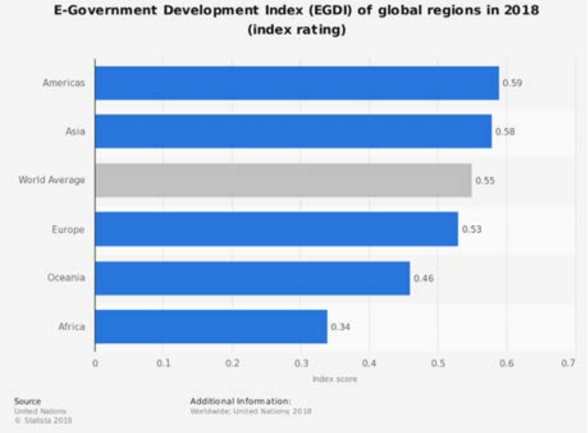
So, table 1 demonstrates the frameworks' frequency that are used in the literature. It seems the most usage knowledge framework is model based work.

Table 1. Types of Knowledge Frameworks presented in eGovernment research

Knowledge Framework	**Frequency**
Theory-Based work	1
Framework based work	10
Model based work	29
Schema based work	8
Concept based work	4
Category based work	22
Non framework-based work	10

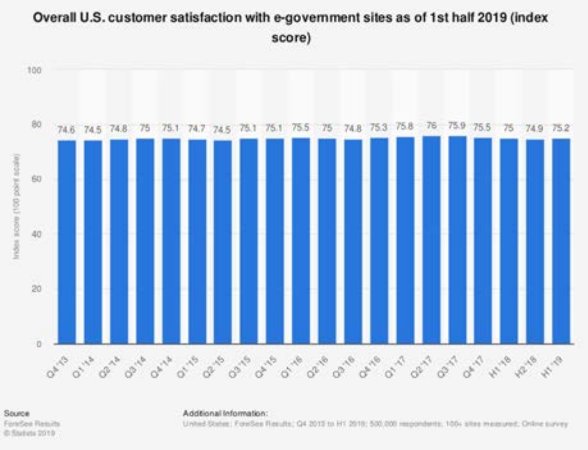
By observing Fig 1, the statistic showed ranks of the international regions based on the EGovernment Development Index (EGDI) as of 2018. The EGDI is derived from three factors: online service, telecommunication infrastructure, and human capital. It is presented in Fig 1 that America was the highest region uses eGovernment service among other regions, represents 0.59. Asia is almost similar to the Americas representing 0.58, while the lowest rank is Africa representing 0.34 (Carter, L., & Belanger, 2004).

Fig. 1. E-government Development Index Worldwide (Clement, 2018a).



Furthermore, the satisfaction with eGovernment sites in the first quarter of 2019 is %75.2. the result was accomplished by using an online survey among 500,000 respondents in the United States for more than 100 sites measured. In Fig 2, the similarity of satisfaction from 2013 until 2019 can be identified, which seems noteworthy (Clement, 2018b).

Fig. 2. The US customer satisfaction (Clement, 2018b).



Source
ForeSee Results
© Statista 2019

Additional Information:
United States; ForeSee Results; Q4 2013 to H1 2019; 500,000 respondents; 100+ sites measured; Online survey

. 2. The US customer satisfaction (Clement, 2018b). The countries worldwide allow their citizens to use eGovernment services, i.e., customers used eGovernment in paying their utility bill in 140 countries, pay fines in 111 countries, applying for marriage certificate in 82 countries, and apply or personal identity card in 59 countries (Clement, 2019) (see Table 2).

Table 2. Offerings of transactional eGovernment services 2014-2018

EGovernment Services	2014	2016	2018
Utilities (internet, gas, tv provider…etc.)	41	104	140
Submit income taxes	73	114	139
Register a business (i.e., new company)	60	97	126
Apply for a birth certificate	44	55	86
Apply for a marriage certificate	39	53	82
Register motor vehicle	33	47	76
Apply for driver's license	29	38	62
Apply for personal identity card	27	31	59

2.1 E-Government from an Arabian Perspective

In the Arab world, eGovernment is working efficiently to cope with the demand of users. The users get related assistance from government electronic applications. However, the experience of Arab about eGovernment is not free from technical, cultural and strategic challenges. The performance is dependent on the income level in the country, so independent factors in this regard need the elimination of some economic conditions (Al-Nuaim, 2009). The key issues are related to IT infrastructure, funding, and limited resources. In addition, there are some limitations discovered in Arab experience regarding internet subscription and funding (El-sofany et. al., 2012). Arab countries have also less vision about technology, so the strategic challenges came out in the form of framework strategy. The cultural challenges related to gender discrimination and lack of awareness or education about technology also matters a lot (El-sofany et. al., 2012). Some examples of how your references should be listed are given at the end of this template in the 'References' section, which will allow you to assemble your reference list according to the correct format and font size.

E-Government impact on Arab users can also be seen in terms of income level. Online services need a clear strategy and decent adoption rate. Nevertheless, the goals of eGovernment to facilitate users in all over the regions is related to certain targets and national and sectoral level. The vision of government is broader under specific indicators to satisfy users and enhance their motivation (Al-Nuaim, 2009). User experience in Arab world related to technical efficiency is based on trust in administration to bring about all the related changes (Alssbaiheen & Love, 2016). Users have shown e-readiness in government agencies regarding assessment. The scope of business and using technologies is expanded in Saudi Arabia because data is available about mobile, PC and internet usage. The role of eGovernment is always considered beneficial to improve the administration for the public by offering efficient services. Alateyah (2014) reported that users are benefiting from easy access to social and political rights due to better governance. The eGovernment maturity is monitored through the development index, by the United Nations. The online services and telecommunication services have ranked the country at the higher level (Alhashimi, 2019).

This experience has made eGovernment follow a road map for users to develop a significant framework for the efficacy of service delivery.

2.2 E-Government Factors

In Germany, there are some factors that prevent users from using eGovernment services. The most crucial factor is lack of needed service online, a lack of security, and user awareness regarding these services (Koptyug, 2019). According to Carter and Belanger (2004), the influencing factors for eGovernment usage are perceived usefulness, relative advantage, and compatibility. Carter and Belanger conceptualized the eGovernment factors using the Technology Acceptance Model (TAM) and diffusions of innovation theory (DOI).

A research paper by Mellouli et al., (2016) on eGovernment among Tunisian citizens to identify their acceptance and level of trust in this service. The researchers identified information and system quality, compatibility, and trust in government and Internet as well. However, trust has the most effect on the citizens in comparison to other factors. Lallmahomed et al., (2017) surveyed 247 users in Mauritius to examine the acceptance of eGovernment among them. The researchers demonstrated that behavioral intention has positively impact performance expectancy and facilitating conditions. Computer self-efficacy has also a negative impact on pre-adoption and using eGovernment services. Further, trust is an important value to encourage users to use the services via ensuring security and privacy are accomplished (Lallmahomed et al., 2017).

2.3 Trust as an Influential Factor

One of the vital factors which influenced eGovernment usage among users is trust; however, trust is a very complicated factor (Alzahrani et al., 2017). Increase the level of trust among users, it will also increase their intention to use eGovernment, this will ensure their usage and adoption of eGovernment services. Trust defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer et al., 1995, p. 712).

Multiple scholars studied the importance of trust in eGovernment usage (Mellouli et al., 2016; Alzahrani et al., 2017; Lallmahomed et al., 2017). Also, ease of use, usefulness (Chee-Wee Tan et al., 2008; Alsaghier et al., 2009; Wang & Lo., 2012; Ayyash et al., 2013; Ozen et al., 2018) that influence users’ trust to use eGovernment. Further, Khasawneh et al., 2013 studied the importance of trust and risk, which may affect eGovernment usage. However, Abu-Shanab and Al-Azzam (2012) did not support risk as a factor to influence eGovernment usage among users, only trust.

Horsburgh et al., (2011) emphasized there is no correlation between trust and government in different eGovernment services. Alzahrani et al., presented multiple aspects which influence eGovernment usage which is technological factors, governmental factors, users’ characteristics, and risk factors. Distinctly, these factors, including the subfactors influence trust in eGovernment services and intention to use this services as well. The eGovernment factors are:

1. Technological Factors: it represents the factors, which influence beliefs of citizens

- System quality
- Service quality
- Information quality

2. Governmental Factors: it represents the agency reputation and the user experience with this agency

- Reputation of the agency
- Past experience

3. Users' Characteristics: the users' characteristics which influence trust in eGovernment.

- Disposition of trust
- Internet experience
- Education
- Gender

4. Risk Factors: is a crucial factor which impact users in trust

- Performance risk
- Time risk
- Security and privacy

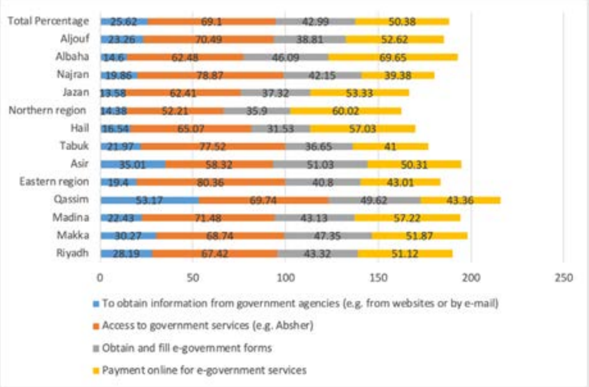
3. Methodology

The study primary source is from General Authority for Statistics (GAS), in addition to some secondary data from Statista. This kind of data classified as secondary resource data which the analysis done at ecological level and the unit of analysis are Saudi users. According to GAS, the sample was randomly selected across Saudi Regions.

4. Analysis and Results

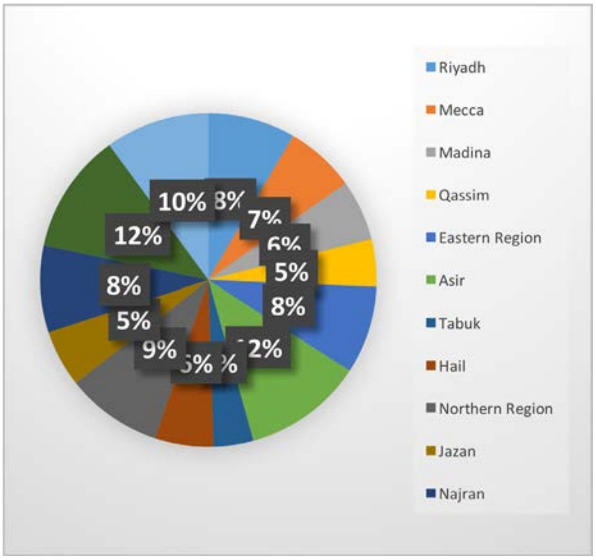
In this research study, the scholar performs a data analysis among Saudi regions to present the main factors of the eGovernment acceptance within the country. This paper identified there are four main services used via eGovernment websites. First, use the eGovernment website to obtain information from government agencies (e.g. from websites or by e-mail). Second, to access to government services (e.g. Absher). Third, to obtain and fill eGovernment forms. Fourth, to make a payment online for eGovernment services. The maximum usage of eGovernment according to the regions are Eastern Region, Najran, and Tabuk, which represents 80.36%, 78.87%, 77.52% respectively (see Fig 3.).

Fig. 3. Relative distribution of eGovernment services used by individuals via Internet



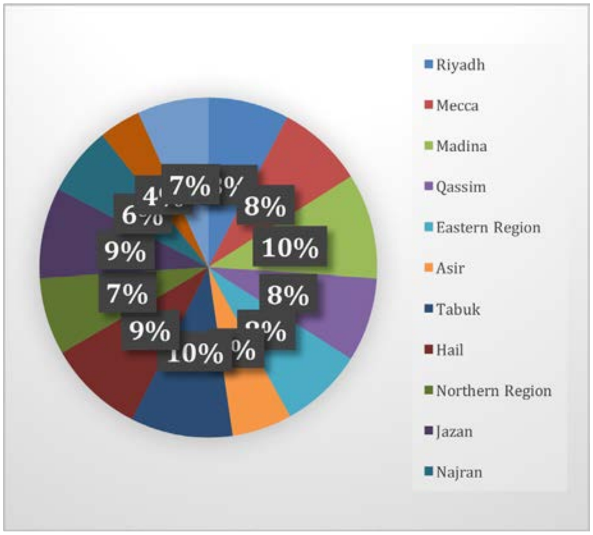
The highest usage of the first service is within Qassim 53.16%, second service within Eastern region 80.36%, third service within Asir %51.03 and the last one within Albaha %69.65.03. The usage of eGovernment services which used last week among Saudi is similar in different regions, for example, the highest rank usage is in Asir and Albaha 12% followed by Riyadh which represents 10% and the least was in Qassim and Jazan (see Fig 4).

Fig. 4. Last time individuals performed government transactions online by administrative regions "Last week"



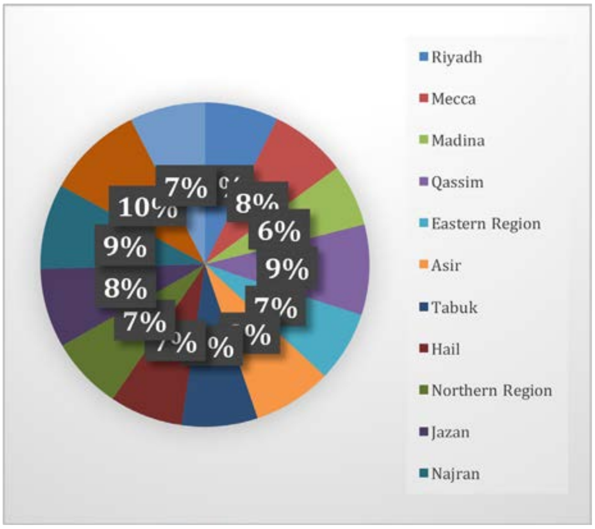
Albaha is also the highest rate of usage among Saudi in services within more than a week and less than a month. While the rest of the regions is slightly similar to each other (see Fig 5).

Fig. 5. Last time individuals performed government transactions online more than a week and less than a month



Madina and Tabuk were the most regions where the individuals used the eGovernment the least which is approximately more than a month and less than three months (see Fig 6).

Fig. 6. Last time individuals performed government transactions online more than a month and less than three months



online more than a month and less than three months

The factors impact the users' attitude to use eGovernment ranked from the most concerning factor to the least (see Appendix A):

1. Lack of knowledge or skills – 29.64%

2. Security concerns (e.g. bank account details) – 3.75%

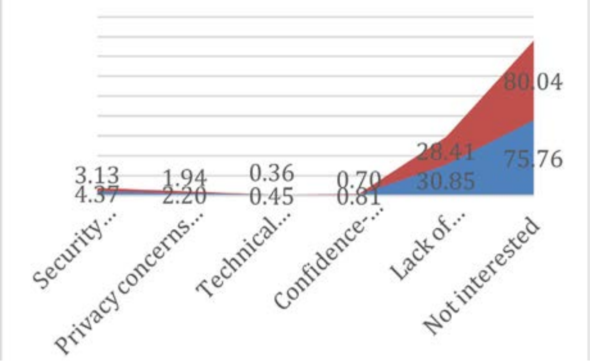
3. Privacy concerns (such as providing personal details) – 2.07%

4. Technical concerns (e.g. poor services provided by some government agencies online) – 0.75%

5. Trust-related concerns (e.g., concerns about ways to receive and return products) – 0.41%

The percentage of the factors are categorized depending on the total percentage of Saudi population, the rest of the population is not interested in these services by 77.88%. It is also recognized that there is a gender difference among males and females who are not using eGovernment, i.e. the percentage of lack of knowledge and skills among males is 30.85% while females are 28.41%, which means male lacking skills to use such services more than females (see Fig 7).

Fig. 7. Percentage distribution of reasons why individuals do not perform government transactions via the internet according to gender.
Note: Blue represents male and red represents female



According to Fig 7 which represents the reason why Saudi do not use eGovernment services and which answers the RQ2 is divided according to gender.

The researcher identified a positive correlation among the level of education and reasons why Saudi users do not use eGovernment. By using the following equation from (Statistics How To):

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2]\,[n\sum y^2 - (\sum y)^2]}} \quad (1)$$

Note that: r (value of Pearson correlation)

n – sample size of

x education

y other factors

There is a positive correlation among the level of education and security concern represents 0.66 which means educated users have more security concerns than uneducated users. Privacy is positively correlated with the level of education by 0.20, technical concerns by 0.60, confidence level by 0.66. However, lack of skills and knowledge is negatively correlated with the education level which means educated people have more skills and knowledge to use such services.

To answer RQ1, the factors that encourage Saudi to adopt eGovernment are: trust, computer competency (skills and knowledge), privacy and security. The eGovernment services should increase the level of trust and the level of security, in addition to implementing strict rules to ensure users' privacy and transparency. Moreover, conducting training, workshops, and provide more ads to increase the usage of such serves is recommended. The results agreed with previous scholars such as (Alzahrani, 2017; Lallmahomed et al., 2017; Khasawneh et al., 2013).

Conclusion

This study investigated the usage of eGovernment among Saudi users. The researchers identified that lack of knowledge, trust level, privacy, security are the most critical factors which prevent Saudis from using services of eGovernment. However, the government requires to enhance the infrastructure which will improve level of awareness and trust among users to recognize the importance of using eGovernment and its advantages.

The study has used empirical evidence to highlight the implications of eGovernment in Saudi Arabia. For instance, Qassim, Eastern region, Asir, and Albaha are the highest regions, which uses eGovernment services. This study acknowledged some factors influence eGovernment services usage. For instance, privacy is positively correlated with the level education by 0.20, technical concerns by 0.60, lack of knowledge and skills is 29.64%, security concerns 3.75%, and technical concerns are 0.75%. The findings proved research questions of this study that how eGovernment can improve these factors to bring more efficiency. The positive correlation among the level of education and reasons discussed of why some users do not use eGovernment.

Further study should research the gender difference of eGovernment usage among Saudis. Another study to which compares the eGovernment website such as Absher to identify the deep understanding of the website factors which encourage users to adopt such services.

Conflict of Interest

The author does not have conflict of interest to declare.

Acknowledgements

The author would thank the General Authority for Statistics to provide the required data to conduct this this study.

References

Alateeyah, S., Crowder, R., & Wills, G. B. (2014). Identifying Factors Affecting the Intention of Saudi Arabian Citizens to Adopt E-Government Services. International Journal of Innovation, Management and Technology, 5(4).

Alhashimi, H. (2019). Chapter 16 E-Government Strategy and Its Impact on Economic and Social Development in Saudi Arabia. Politics and Technology in the Post-Truth Era, 237–243. doi: 10.1108/978-1-78756-983-620191016

Al-Nuaim, H. A. (2009). How" E" are Arab municipalities? An Evaluation of Arab capital municipal web sites. International Journal of Electronic Government Research (IJEGR), 5(1), 50-63

Alssbaiheen, A., & Love, S. (2016). Mobile Government in Saudi Arabia. International Journal of Mobile Human Computer Interaction, 8(3), 18–37. doi: 10.4018/ijmhci.2016070102

Alzahrani L, Al-Karaghouli W and Weerakkody V (2017) Analysing the critical factors influencing trust in eGovernment adoption from citizens' perspective: A systematic review and a conceptual framework. International Business Review. 26(1): 164–175.

Carter, L., & Belanger, F. (2004, January). Citizen adoption of electronic government initiatives. In 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the (pp. 10-pp). IEEE.

Clement, J. (2018a, August 2). E-Government Development Index (EGDI) by region 2018. Retrieved January 26, 2020, from https://www.statista.com/statistics/421584/egdi-eGovernment-development-index-region/

Clement, J. (2018b, August 2). Transactional eGovernment services 2018. Retrieved January 26, 2020, from https://www.statista.com/statistics/421610/global-transactional-government-website-services/

Clement, J. (2019, November 21). U.S. customer satisfaction with eGovernment 2019. Retrieved January 26, 2020, from https://www.statista.com/statistics/184361/us-consumer-satisfaction-egovernment/

El-sofany, H. F., Al-Tourki, T., Al-Howimel, H., & Al-Sadoon, A. (2012). EGovernment in Saudi Arabia: Barriers, challenges and its role of development. International Journal of Computer Applications, 48(5).

General Authority for Statistics. (2018, May 10). ICT Access and Usage by Households and Individuals Survey. Retrieved January 28, 2020, from https://www.stats.gov.sa/en/952

General Authority for Statistics. (2020). Population Estimates. Retrieved 23 January 2020, from https://www.stats.gov.sa/en/43

Heeks, R., & Bailur, S. (2007). Analyzing eGovernment research: Perspectives, philosophies, theories, methods, and practice. Government information quarterly, 24(2), 243-265.

Khasawneh, Rabayah, W and Abu-Shanab, E. (2013) E-Government acceptance factors: trust and risk. The 6th International Conference on Information Technology.

Koptyug, E. (2019, December 10). E-Government: usage barriers in Germany 2019. Retrieved January 27, 2020, from https://www.statista.com/statistics/450415/eGovernment-usage-barriers-germany/

Lallmahomed, M. Z., Lallmahomed, N., & Lallmahomed, G. M. (2017). Factors influencing the adoption of eGovernment services in Mauritius. Telematics and Informatics, 34(4), 57-72.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

Mellouli, M., Bentahar, O., & Bidan, M. (2016). Trust and eGovernment acceptance: The case of Tunisian on-line tax filing. The Electronic Journal Information Systems Evaluation, 19.

Ozen, A. O., Pourmousa, H., & Alıpourc, N. (2018). Investigation Of The Critical Factors Affecting E-Government Acceptance: A Systematic Review And A Conceptual Model. Innovative Journal of Business and Management, 7(3), 77-84.

Statistics How To. (n.d.). Correlation Coefficient: Simple Definition, Formula, Easy Calculation Steps. Retrieved from https://www.statisticshowto.datasciencecentral.com/probability-and-statistics/correlation-coefficient-formula/

Top 5 ranking for Saudi eGovernment by 2030. (2016, May 7). Arab News. Retrieved from https://www.arabnews.com/news/top-5-ranking-saudi-eGovernment-2030

Vision 2030. Retrieved from KSA Vision 2030 Strategic Objectives and Vision Realization Programs

Appendix A

Percentage distribution of reasons why individuals do not perform government transactions via the Internet

Age	*1 Lack of knowledge or skills*	*2 Trust-related concerns (e.g., concerns about ways to receive and return products)*	*3 Technical concerns (e.g. poor services provided by some government agencies online)*	*4 Privacy concerns (such as providing personal details)*	*5 Security concerns (e.g. bank account details)*	*6 Not interested*
19-15	*27.03*	*0.54*	*0.42*	*1.88*	*2.66*	81.65
24-20	*23.99*	*0.86*	*0.68*	*2.69*	*4.55*	80.86
29-25	*28.30*	*1.05*	*0.48*	*2.23*	*4.58*	77.67
34-30	*30.73*	*0.84*	*0.38*	*2.75*	*4.60*	76.21
39-35	*32.38*	*0.70*	*0.46*	*2.30*	*4.37*	74.56
44-40	*33.05*	*0.87*	*0.30*	*2.15*	*3.76*	74.67
49-45	*32.87*	*1.05*	*0.30*	*1.77*	*3.84*	76.09
54-50	*31.67*	*0.54*	*0.16*	*1.52*	*3.15*	77.22
59-55	*29.83*	*0.47*	*0.28*	*1.14*	*3.50*	77.56
65-60	*27.97*	*0.21*	*0.21*	*1.05*	*2.73*	80.02
Total Percentage	*29.64*	*0.75*	*0.41*	*2.07*	*3.75*	77.88

Fingerprint Smoothing Using Different Interpolation Techniques

Abdullah Bajahzar*

Department of Computer Science and Information, College of Science at Zulfi,
Majmaah University, Zulfi 11932, Saudi Arabia, a.bajahzar@mu.edu.sa

Abstract

Classical fingerprint analysts use binary images in the minutiae recognition and extraction processes. These obtained images do not have a sufficient quality that allows the extraction of the robust primitives, either during the contours detection or during skeletonization. In this study, a mathematical approach for the fingerprint curves modeling have been performed. The adopted smoothing technique is based on two geometric interpolation types adapted to fingerprint images. The obtained results reveal that the Bezier curve method has an error lower than that by the cubic spline method. The Bézier curve method has a RMS value of 0.035 pixels and an average maximum error of the order of 0.33 pixels. On the other hand, the cubic spline method has a RMS value about of 0.043 pixels and an average maximum error about of 0.37 pixels. We can see that the proposed method facilitates the design process of real-world objects and makes the fingerprint curves smooth.

Keywords:

Fingerprint image; Bézier curve method; Cubic spline method; Gabor filter; smooth curve.

1. Introduction

Biometrics is a method of identifying individuals either by their physical characteristics such as fingerprints, face, and iris or by their behavioral characteristics such as speech. Despite the evolution of new biometric methods considered as more reliable and more robust, the fingerprint identification remains the most widely used method (Soundharadevi and Pushparani, 2016- Conti et al., 2017). Indeed, the fingerprint offers an effective solution to identify people and it is very easy to acquire. In addition, this biometric technology is considered one of the cheapest in terms of cost.

Understanding the structure of fingerprint curves plays a capital role in the minutiae recognition and extraction process. Usually, conventional fingerprint-based recognition techniques go through the binarization and skeletonization step to extract the minutiae existing in the fingerprint image (Saleh et al., 2011- Nagar et al., 2010). Generally, the bending edges state is also an important fingerprint characteristic. However, false curves are generated if the image quality is poor and it can be observed that the bending curve tendency is irregular. On the basis of these observations, we propose in this paper a new algorithm for smoothing these curves. In this algorithm, a pre-processing and fingerprint image enhancement step is performed to simplify the curve detection and minutiae extraction task. This phase requires using the Gober filter to improve the image (Sojan and Kulkarni, 2016, Mohammedsayeem-uddin et al. 2014, Hussain et al., 2016), and then the conversion of the fingerprint image into a binary image (Shetter et al., 2018- Rani and Kothuru, 2017). The next step requires the implementation of the skeletonization algorithm to reduce the center-line thickness to one pixel (Karani and Aithal, 2017, Bataineh, 2018, Leslie and Sumathi, 2018). Then, a 3*3 matrix is used to extract the minutiae types (Jothi and Palanisamy, 2016, Ain et al., 2018, Krish et al., 2019). Based on the curves and minutiae detected, we introduce a fine-tuning algorithm that automatically detects the control points and uses them as nodes for curve interpolation. Finally, two interpolation types are implemented to smooth the fingerprint curves and assess the performance of the considered algorithm.

In this paper, an approach to smooth the fingerprint curves is developed. In section 2, a brief description of related works is given. In section 3, we provide an expression of a potentials idea adapted to our problem. In Section 4, we present the segmentation technique of fingerprint images used and the minutiae detection method. Then, section 5 describes the theoretical aspect for the two interpolations types used. The experimental results and the error calculation are presented in sections 6. Finally, we finish with the discussion and the conclusion in sections 7 and 8, respectively.

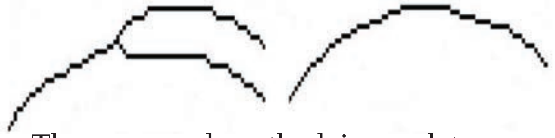
2. Related Works

Over the years, many interpolation methods such as the polynomial interpolation, linear or cubic spline methods, least squares method, fractal interpolation and Bezier curve method have been applied to smooth curves in different domains and to facilitate the design process of real-world objects. Ballan M. (1998) has used the smoothing, classification and fingerprints identification on the basis of singular points (delta and core points) to introduce the directional fingerprints processing. He has used the directional histograms of a fingerprint to detect delta and core points. His proposed algorithm involves directional image representation as well as singular point detection. Perumal and Ramaswamy, 2009 have proposed an innovative and efficient scheme for the fingerprint images compression. They have used representations of the Bézier curve to achieve this aim. Their proposed technique involves two major steps; the first step is to extract the peaks present in the fingerprint image with their coordinate values. Thereafter, they have used the Bézier curve technique to detect the control points. These control points have been used to reconstruct the image of the fingerprint using the Bézier curves. Vijayaragavan et al., 2014 have suggested a model to compare the knowledge from the signature. They have used the Bézier curve algorithm to categorize points on the curve and they have used the signature behaviors for verification. Bezier curves are segmented from the signature by examining the pixel color. Chong et al., 1992 have proposed a data compression method for digitized fingerprint images based on the B-spline functions. They have developed algorithms for extracting, classifying or recognizing fingerprint characteristics in the first instance. Then, they have given a description of two B-spline representation approaches for compressing data from a fingerprint image. Guedri et al., 2017a have proposed a mathematical approach for 2D reconstruction of the retinal vascular tree. They have extracted the graph of unsupervised topology of the blood vessel from the image of the human retina. They have used three types of interpolations, i.e. the least squares method, linear spline method and cubic spline method, to smooth the blood vessel curves. Guedri et al., 2017b have presented a method to avoid the major disadvantage of skeletonization of the human retina image. They have used, in a first phase, all the segmentation steps to detect the blood vessels curve including image binarization, skeletonization and finally the step for location identification of characteristic points (endpoints, middle-point, and bifurcation-points). In a second phase, they have used the B-Spline interpolation method to improve the blood vessels curvature quality and to obtain smoother curves and more realistic effects.

3. Problem proposal

The main objective of this work is to eliminate the negative effect of digital image processing in the study of fingerprint image, such as the irregularities and singularities of a curve from the obtained skeletal images. After using the Gober technique to improve the image quality, we use a binarization technique to obtain a binary image; we can extract the central-line by the skeletonization technique. But, the drawback of this approach is that the fingerprint curves connectivity is not realistic, as shown in Figure 1.

Fig. 1. The negative effect of digital image



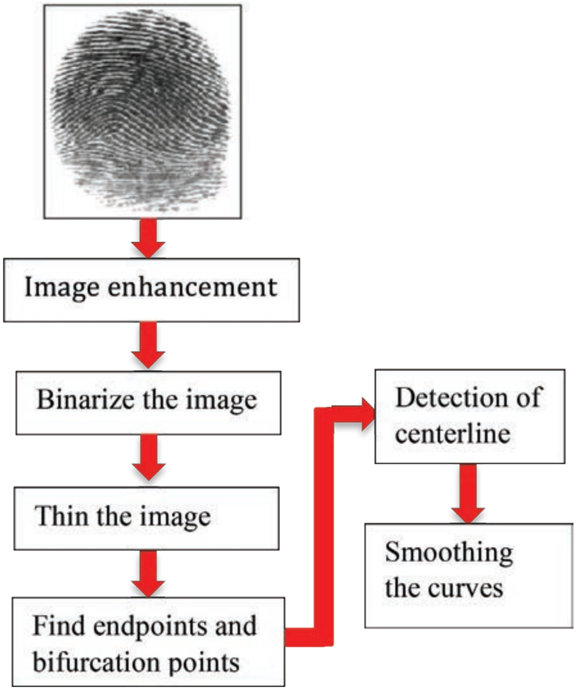
The proposed method is used to reconstruct the most authentic fingerprint curves and at the same time to mitigate the drawbacks of digital image processing. The first objective is to enhance the acquired image quality. Subsequently, we elicit data from image by segmentation techniques such as binarization as the first task. Then, the image skeletonization is the second task and finally extraction of the minutiae and the fingerprint curves. The final step in the proposed algorithm is to use two interpolation types to get a smooth center-line closer to nature. Figure 2 shows the block diagram of this approach.

4. Image Pre-processing

4.1. Fingerprint image enhancement

First, fingerprint images are enhanced based on Gabor filters as proposed in Sojan and Kulkarni, 2016. The filter properties that it is at the same time selective in frequency and orientation, moreover it has an optimal joint resolution in the space and frequency domains (Mohammedsayeemuddin et al. 2014- Hussain et al., 2016). Let the fingerprint image be represented by I (x, y). The symmetrical two-dimensional Gabor filter is given by:

Fig. 2. Block diagram of the proposed method



$$g(x,y:\theta,f)=\exp\left\{-\frac{x_\theta^2}{\sigma_x^2}+\frac{y_\theta^2}{\sigma_y^2}\right\}.\cos\left(2\pi f.x_\theta\right) \quad (1)$$

where θ is the filter orientation, [xθ, yθ] are the coordinates of [x, y] after a clockwise Cartesian axes rotation the by an angle (90°-θ), as shown by the following Eq. 2:

$$\begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} \cos(90-\theta) & \sin(90-\theta) \\ -\sin(90-\theta) & \cos(90-\theta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$$= \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (2)$$

In the Eq. (1), f is the frequency of the sinusoidal plane wave in the direction θ from the x axis, and σx and σy are the space constants of the Gaussian envelope along the x and y axes. Four values of θ, namely 0, 45, 90, 135 degrees, are used to obtain four different filters. These filters are convolved with the image I (x, y) to obtain the corresponding filtered outputs given by Eθ (x, y) = g (x, y, f, θ) * I (x, y) (Sojan and Kulkarni, 2016).

4.2. Binarization

This phase focuses on the images segmentation and seeks an effective method to clearly separate the background and the object. In other words, it is about finding a binarization method that can effectively determine the threshold for each image point. Binarization consists of transforming a multi-bit pixel into a 1-bit image (Shetter et al., 2018- Rani and Kothuru, 2017). For that, we will do a thresholding. If the pixel value is below the threshold; we associate it with the value 0. If the pixel value is equal to or greater than the threshold we associate it with the value 1.

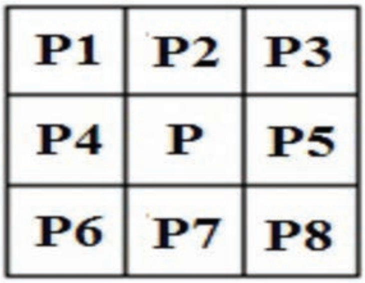
4.3. Skeletonization

The skeleton is a compact and efficient representation of the form. It is widely used in the image analysis field; the skeleton represents the line centered in the form. Thinning is the chosen skeletonization method. Thinning is a method of “peeling” the shape until one gets a connected point set of a pixel wide that retains the shape topology (Karani and Aithal, 2017). In other words, the principle of this method is to examine, in a predetermined order, the form contour points in order to delete them iteratively (Bataineh, 2018- Leslie and Sumathi, 2018). The contour points are then marked for deletion after the identification iteration. These two phases avoid deleting a skeleton complete branch in iteration.

4.4. Minutiae extraction

In this method, a skeleton image is used for minutiae extraction (Jothi and Palanisamy, 2016, Ain et al., 2018, Krish et al., 2019). It involves the use of a 3x3 window to check the neighboring area of each image pixel, as shown in Figure 3. A pixel is classified as an isolated point if it has no neighboring pixel, and as an endpoint if it has a single neighboring pixel in the image, and as a continuing ridge point if it has 2 neighboring pixels, and as a bifurcation point if it has 3 neighboring pixels, and as a crossing point if it has 4 neighboring pixels (Ain et al., 2018).

Fig. 3. The 8 Neighborhoods



P1	P2	P3
P4	P	P5
P6	P7	P8

5. Interpolation

Let given dataset points

$$P\binom{x_i}{y_i} = \{(x_0, y_0);\ (x_1, y_1);\ \dots\ ;\ (x_n, y_n)\} \in \mathbb{R}^2.$$

The purpose of the polynomial interpolation is to find a polynomial that passes through all data points (Roy et al., 2013).

The main purpose of the interpolation is to find a function to approximate the functional values and the data of the original values (Parsania and Virparia, 2016). The interpolation function usually goes through the original dataset, with the curve point adjustment; we just want a function that fits well into the original data points. With curve fitting, the approximation function does not have to go through the original data set.

5.1. Bezier Curve

Bézier curves are parametric polynomial curves described by Pierre Bézier in 1962. They are used to design auto parts (Gousenbourg et al., 2016- Fierz, 2018). They are also used in several applications such as image synthesis, font rendering, animation, environment design and robotics (Baydas and Karakas, 2019).

Let (Pi = (xi, yi), i = 0, 1, 2, ..., n) be the control points of the Bezier curve. The Bezier curve of degree n can be defined by the following Eq. 3 (Gousenbourg et al., 2016):

$$\begin{cases} x(t) = \sum_{i=0}^{n} x_i B_i(t) \\ y(t) = \sum_{i=0}^{n} y_i B_i(t) \end{cases} \qquad 0 \leq t \leq 1 \qquad (3)$$

with (x(t),y(t)) are the points on the curve, B_i (t) (i=0,1,…,n) are the Bernstein polynomials. They are used as the basis functions, for polynomial order n. The ith basis function is defined by the following Eq. 4:

$$B_i(t) = \frac{n!}{i!\,(n-i)!} t^i (1-t)^{n-1} \qquad (4)$$

The main advantage of Bezier curves is that the number of control points can be very large without the curve becoming impossible to manipulate (Fierz, 2018- Baydas and Karakas, 2019). It also allows to have interpolation points in the middle of the curve and not only at the ends.

5.2. Interpolation by cubic splines

The cubic spline interpolation is a piecewise interpolation, let y (x) over an interval [x0, xn] that has been partitioned into subintervals [xi-1, xi], i = 1,2, ..., n (Abdul-Karim et al., 2018).

This interpolation type consists in replacing, on each subinterval, the function y by a third degree polynomial (Yaghoobi et al., 2017- Wu et al., 2015), so that the interpolating function is continuous, as well as its first and second derivatives on the whole interval [x0, xn] (Parveen and Tokas, 2015).

The interpolation cubes are defined by the following Eq. 5 (Wu et al., 2015) :

$$f_i(x) = a_i x^3 + b_i x^2 + c_i x + d_i \qquad (5)$$

In the above equation, x_(i-1)≤x≤x_i and i=1,2,…,n. Let use the notation for the second derivative: f_i^” (x_i)=f_i”.

Using the function continuity, after some algebraic manipulations, it is straightforward to obtain the following expression:

$$f_i(x) = f''_{i-1}\frac{(x_i - x)^3}{6h_i} + f''_i\frac{(x - x_{i-1})^3}{6h_i} + \left[\frac{y_{i-1}}{h_i} - f''_{i-1}\frac{h_i}{6}\right](x_i - x) + \left[\frac{y_i}{h_i} - f''_i\frac{h_i}{6}\right](x - x_{i-1})$$

The functions f_i (x) will be fully known after calculating values of f_i”.

To obtain these values, it is necessary to use the conditions of continuity of the first derivatives at the interior points:

$$f'_i(x_i) = f'_{i+1}(x_i) \quad , \quad i = 1,2,\ldots,n-1$$

We deduce, the following equation:

$$h_i f''_{i-1} + 2(h_i + h_{i+1}) f''_i + h_{i+1} f''_{i+1} = \frac{6}{h_{i+1}}(y_{i+1} - y_i) + \frac{6}{h_i}(y_{i-1} - y_i) \quad ; \quad i = 1,2,\ldots,n-1.$$

We thus obtain a linear system of (n-1) equations with n+1 unknown, the f_i”.

There remains therefore the possibility of imposing two additional conditions, obtained for example by the interval boundary conditions at x_0 and x_n. We impose the following two conditions:

$$f''_1(x_0) = 0 \quad and \quad f''_n(x_n) = 0$$

The natural cubic splines are therefore obtained unambiguously.

The n-1 unknowns f_1^”,f_2^”,…,f_n” are then solution of the linear system written above. This tridiagonal system is symmetrical. This system has a unique solution because its tri-diagonal matrix is diagonally dominant and is therefore invertible.

If the interpolation points are uniformly distributed on [x0, xn], all hi are equal and the system becomes, for i = 1, 2, ..., n-1:

$$f''_{i-1} + 4f''_i + f''_{i+1} = \frac{6}{h^2}\left[y_{i+1} - 2y_i + y_{i-1}\right]$$

5.3. Error calculations

The objective of this work is to achieve the fingerprint curves reconstruction by using two mathematical interpolations (Fortin et al., 2014, Brereton, 2018, Wang and Lu, 2018). Since it is impossible to arrive at exactly the same result, the experiment success must be evaluated by some comparisons between the obtained result values and the initial values. For this purpose, we use the root-mean-square error (RMS error) and the absolute value of the maximum error.

- **Root-mean-square error (RMS)**

This method is used to measure the difference between the initial data and the reconstructed data, as shown in Eq. 6 below (Fortin et al., 2014, Brereton, 2018):

$$RMS = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(f_i - f_{i,ini}\right)^2} \qquad (6)$$

where N is the data number, f_i is the reconstructed data and f_(i,ini)i is the initial data.

Absolute value of the maximum error:

The absolute value of the maximum error between the reconstructed data and the original data is defined according the following equation (Wang and Lu, 2018- Al-Janabi et al., 2018):

$$MAE = \max_{i=1:N}\left|f_i - f_{i,ini}\right| \qquad (7)$$

6. Result

To evaluate our approach, the proposed algorithm is implemented on a workstation equipped with an Intel Pentium B960 processor at 2.20 GHz and 4 GB of RAM processor and Windows 7 OS, using the Matlab language. In this study, we use fingerprint images from the Fingerprint Verification Competition database (FVC2006). It contains four sub-databases, DB1, DB2 and DB3, which are acquired with different sensors, and B4 which is created with a synthetic generator. Fingerprint images have different sizes with a resolution of 500 dpi and they are devised in two sets:

- Set A: consisting of fingers numbered from one to 100

- Set B: made up of fingers numbered from 101 to 110 and made available to users.

6.1. Image segmentation

The fingerprint raw image is extracted from the database. Subsequently, to enhance these images quality, the Gabor filter is used, as shown in Fig. 4. Then, the thresholding method is used to transform the grayscale image into a binary image. We use a thinning algorithm to determine the fingerprint skeleton and detect the curves with a one-pixel width. The obtained image guarantees an efficient extraction of the minutia points. The scanning of the skeleton image with a 3 * 3 matrix makes it possible to detect each pixel type (Endpoint, Bifurcation point) as shown in Fig. 4 e and f.

6.2. Smoothing the fingerprint curve

After determining the central line positions and the extraction of the points of minutiae, we use two interpolations types, namely Bezier Curve and cubic splines, to reconstruct the smooth fingerprint curves. The obtained results are shown in Fig. 5:

Fig. 4. Image Pre-processing: (a) raw image, (b) enhanced image, (c) Binary image, (d) Skeletonization image, (e) Endpoints (Red points), (f) Bifurcation points (Blue points).

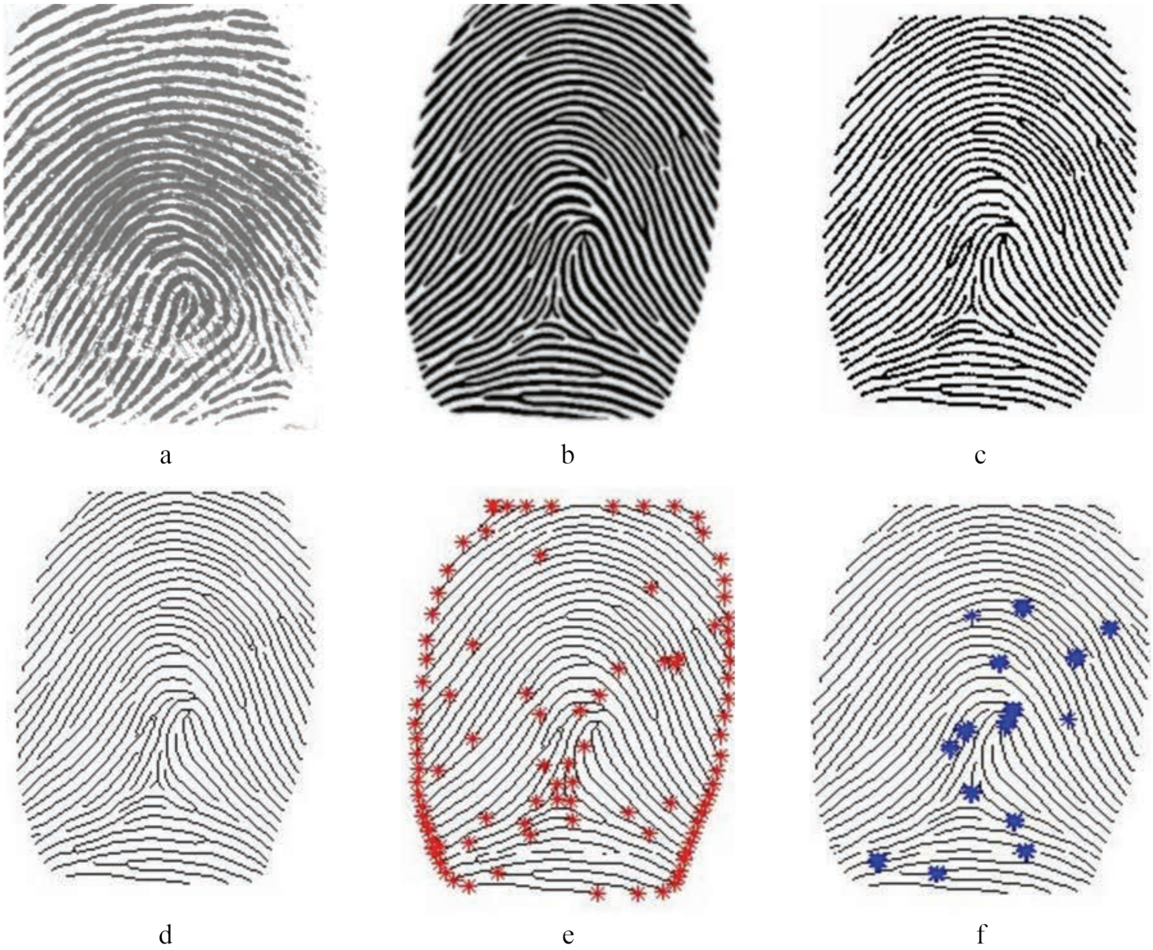


Fig. 5. Interpolation examples of a fingerprint curve, (a) original data, (b) Bezier Curve interpolation, (c) Cubic spline interpolation.

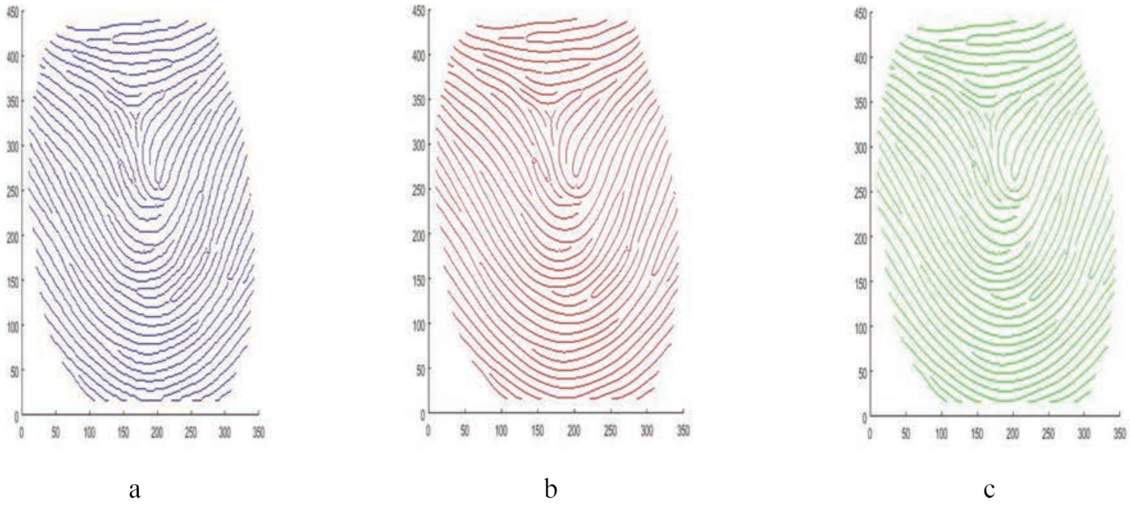


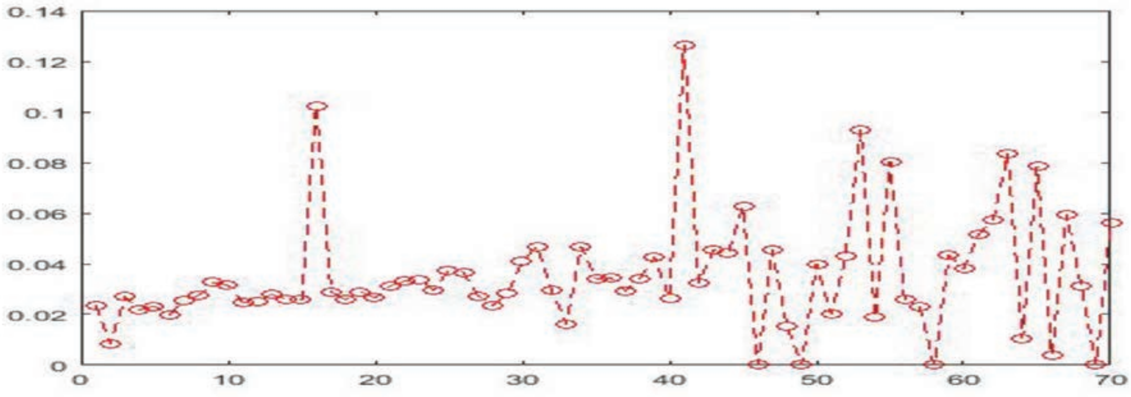
Figure 5 shows the typical processing results on a sample of fingerprint curves. Figure 5.b shows the interpolation result with the Bézier curve method and Figure 5.c with the cubic splines method. From these results, we can see that the curves are very close to each other. They are almost identical either for the curve using the interpolation Bezier Curve or for the second interpolation type i.e. interpolation by cubic splines. We can also notice that the two obtained curves have very realistic connectivity and are very close to the natural models.

6.3. Experimental tests performance

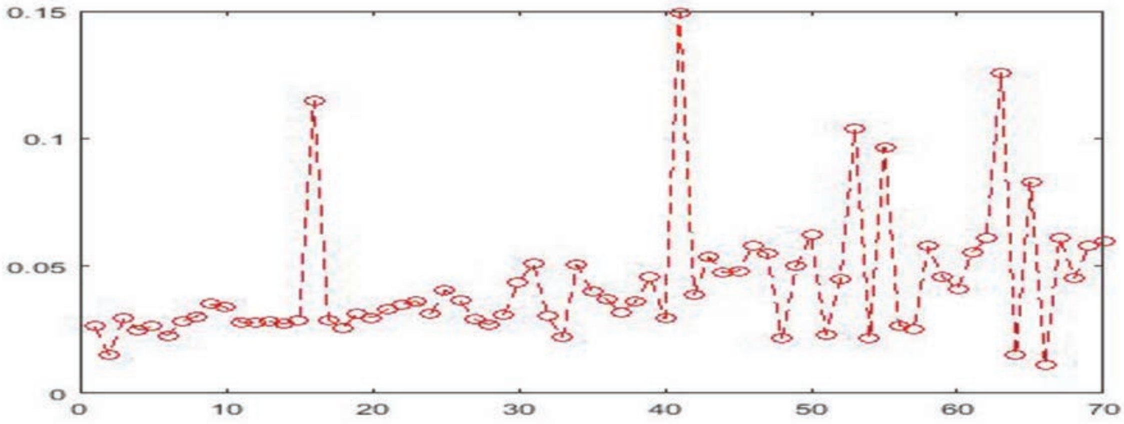
In this section, we propose the results of a symmetric association calculation between two interpolated curves and the original curve, based on a computation of all the distances between each points of these two curves (providing a potential map). In both cases, the mathematical representations that we manipulate are curves that we want to compare two by two. The result is somehow a measure reflecting their similarity.

Figure 6 shows the performance results for the experimental tests by applying the two interpolation types proposed to fingerprint curves having a different arc length (from 5 to 482 points). Figure 6.a shows the RMS error measure that reflects the distance between the reference curves points and the interpolated curves points by Bézier curve method. In the same context, Figure 6.b shows the RMS error measure for cubic splines interpolation.

Fig. 6.   RMS error: (a) Bézier curve method error, (b) cubic spline method error



a



The obtained results reveal that the cubic spline method generates an error slightly higher than that produced by the Bézier curve method. Indeed, a value about 0.37 pixels is reached for the average maximum error and a value about 0.043 pixels is obtained for the average RMS for the cubic spline method. Nevertheless, the Bézier curve method is more powerful than the other proposed methods using the above criteria. Actually, the average maximum error is in the order of 0.33 pixels and the average RMS value is equal to 0.035 pixel.

6.4. Processing time:

The algorithm described in this document takes a lower time of one second to interpolate a single curve. Indeed, the execution time related to the Bézier curve method is about 56 seconds for 70 curves and 58 seconds for the same curve number using the cubic spline method.

7. Discussion

In this section, we compare our numerical results with the results found in other studies. For the method proposed by Aylward and Bullitt, 2002, it has a mean error less than 0.5 voxel. Cavinato et al., 2013 suggested a method characterized by an error on the centre-line of 0.62 ± 0.17 voxel. On the other hand, the method proposed by Guedri et al., 2017 has an average effective value about 0.12 pixels for the cubic spline method, about 0.26 pixels for the linear spline and 0.35 pixels for the least square. On the contrary, the method proposed in this work gives better result in terms of error It has an average RMS error about 0.035 pixels for the Bézier curve method and 0.043 for the cubic spline method, which reveals the reliability and validity of the proposed method. Furthermore, it gives a smooth curve closest to the initial curve and the closest to reality. It also makes these curves natural with the minimum error.

8. Conclusion

Fingerprint based biometric systems involve image enhancement and minutiae extraction as the most commonly used technique. This paper presents a review of various techniques to smooth the fingerprint curves in order to make it closer to reality, and allows us to eliminate the noise present in digitized images. The proposed method is based on two major phases. The first phase concerns the pre-treatment and segmentation for the fingerprint image. It is divided into three parts. The first part aims to enhance image with the Gabor filter whereas the second part is devoted to image binarization. The third part deals with the central lines detection from the fingerprint and minutiae extraction. The second phase is devoted to the smoothing technique of these central lines. Two interpolation types, namely Bezier curve and cubic splines, have been investigated. The proposed approach produced results which are very close to reality with very small errors when using these two interpolation types. As indicated above, the average RMS value is about 0.035 pixels and the maximum error value is about 0.33 pixels for the Bezier curve method. However, the cubic spline method has an average RMS value of 0.043 pixels and a maximum error of 0.37 pixels.

Conflict of Interest

The authors declare no conflict of interest.

References

Abdul-Karim, S. A., Ismail, M. T., Othman, M., Abdullah, M. F., Hasan, M. K., Sulaiman, J., 2018. Rational Cubic Spline Interpolation for Missing Solar Data Imputation, Journal of Engineering and Applied Sciences

13, pp 2587-2592.

Ain, N. U., Shaukat, F., Nagra, A.S., Raja, G., 2018. An efficient algorithm for fingerprint recognition using minutiae extraction, Pakistan Journal of Science 70(2), pp 169-176.

Al-Janabi, S., Salman, M. A., Fanfakh, A., 2018. Recommendation System to Improve Time Management for People in Education Environments, Journal of Engineering and Applied Sciences 13, pp 10182-10193.

Aylward, S. R., Bullitt, E., 2002. Initialization, noise, singularities, and scale in height ridge traversal for tubular object centerline extraction, IEEE Transactions on Medical Imaging 21(2), pp 61–75.

Ballan, M., 1998. Directional Fingerprint Processing, International Conference on Signal Processing 2, pp. 1064-1067.

Ballan. M, 1998 “Directional Fingerprint Processing”, International Conference on Signal Processing 2, pp. 1064-1067.

Bataineh, B., 2018. An Iterative Thinning Algorithm for Binary Images Based on Sequential and Parallel Approaches, Pattern Recognition and Image Analysis 28(1), pp 34–43.

Baydas, S., Karakas, B., 2019. Defining a curve as a Bezier curve, Journal of Taibah University for Science 13(1), pp 522-528.

Brereton, R. G., 2018. Sources of error, Journal of Chemometrics 32(9), e3017, pp 1-5.

Cavinato, A., Ballerini, L., Trucco, E., Grisan, E., 2013. “Spline-based refinement of vessel contours in fundus retinal images for width estimation,” IEEE 10th International Symposium on Biomedical Imaging, San Francisco, CA ,pp 872 – 875.

Chong, M.M.S., Gay, R.K.L., Tan, H.N., Liu, J. 1992. Automatic representation of fingerprints for data compression by b-spline functions, Pattern Recognition 25(10), pp. 1199-1210

Clark, T., Woodley, R., De Halas, D., 1962. Gas-Graphite Systems, in “Nuclear Graphite” R. Nightingale, Editor. Academic Press, New York, pp 387-394.

Conti, V., Militello, C., Vitabile, S., 2017. Biometric authentication overview: a fingerprint recognition sensor description, Int J Biosen Bioelectron 2(1), pp 26–31.

Deal, B., Grove, A., 1965. General Relationship for the Thermal Oxidation of Silicon, Journal of Applied Physics 36, pp 3770-3785.

Deep-Burn Project: Annual Report for 2009, Idaho National Laboratory, Sept. 2009.

Fachinger, J., 2006. Behavior of HTR Fuel Elements in Aquatic Phases of Repository Host Rock Formations. Nuclear Engineering & Design 236 (3), pp 54-71.

Fachinger, J., den Exter, M., Grambow, B., Holgerson, S., Landesmann, C., Titov, M., Podruhzina, T., 2004. “Behavior of spent HTR fuel elements in aquatic phases of repository host rock formations,” 2nd International Topical Meeting on High Temperature Reactor Technology. Beijing, China, paper #B08.

Fierz, W., 2018. Application of Bézier Curves for Calculating Likelihood Ratios for Plasma Amyloid-β Biomarkers for Alzheimer’s Disease, Frontiers in Aging Neuroscience 10, Article 276, pp 1-5.

Fingerprint Verification Competition 2006 (FVC2006) web site (http://bias.csr.unibo.it/fvc2006/)

Fortin, V., Abaza, M., Anctil, F., Turcotte, R., 2014. Why Should Ensemble Spread Match the RMSE of the Ensemble Mean?, Journal of

Hydrometeorology 15, pp 1708- 1713.

Gousenbourg, P.Y., Absil, P.A., Wirth., B., Jacques, L., 2016. "Interpolation on manifolds using Bézier functions," In: Proceedings of the third international Traveling Workshop on Interactions between Sparse models and Technology" iTWIST'16, Aalborg, Denmark.

Guedri, H., Ben Abdallah, M., Belmabrouk, H., 2017b. "Modelization Using the B-Spline method of blood vessel curve for the human retina," 2017 International Conference on Control, Automation and Diagnosis (ICCAD) ICCAD'17, pp. 411-415 Hammamet - Tunisia.

Guedri, H., Ben Abdallah, M., Nasri, F., Belmabrouk, H., 2017a. "Computer method for tracking the centerline curve of the human retinal blood vessel," 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia.

Hussain, W., Munawar, T., Shahzaib, M., Masood, M., 2016. Automated Enhancement of Compromised Fingerprint Images, Journal of Biochemistry, Biotechnology and Biomaterrials (JBCBB) 1(2), pp 27-33.

Jothi, R. A., Palanisamy, V., 2016. Analysis of Fingerprint Minutiae Extraction and Matching Algorithm, International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) 3(20), pp 398-402.

Karani, K. P., Aithal, P. S., 2017. A Conceptual Study on Fingerprint Thinning Process Based on Edge Prediction, International Journal of Applied Engineering and Management Letters (IJAEML) 1(2), pp 98-111.

Krish, R. P., Fierrez, J., Ramos, D., Alonso-Fernandez, F., Bigun, J., 2019. Improving automated latent fingerprint identification using extended minutia types, Information Fusion 50, pp. 9-19.

Leslie, S., Sumathi, C. P., 2018. A Robust Hierarchical approach to Fingerprint matching based on Global and Local Structures, International Journal of Applied Engineering Research 13, pp 4730-4739.

Mohammedsayeemuddin, S., Gonsai, S. K. Vandra, D., 2014. Efficient Fingerprint Image Enhancement Algorithm Based On Gabor Filter, International Journal of Research in Engineering and Technology 3(4), pp 809-813.

Nagar, A., Rane, S., Vetro, A., 2010. "Alignment and Bit Extraction for Secure Fingerprint Biometrics," Conference: Media Forensics and Security II, part of the IS&T-SPIE Electronic Imaging Symposium, San Jose, CA, USA.

Parsania, P. S., Virparia, P. V., 2016. A Comparative Analysis of Image Interpolation Algorithms, International Journal of Advanced Research in Computer and Communication Engineering 5(1), pp 29-34.

Parveen, S., Tokas, R., 2015. Faster Image Zooming using Cubic Spline Interpolation Method, International Journal on Recent and Innovation Trends in Computing and Communication 3(1), pp 22-26.

Perumal, V. and Jagannathan Ramaswamy, J., 2009. An Innovative Scheme for Effectual Fingerprint Data Compression Using Bezier Curve Representations, (IJCSIS) International Journal of Computer Science and Information Security 6(1), pp. 149-157

Rani, J. T., Kothuru, M., 2017. Personal Identification using quality image resulting from binarization and thinning techniques, International Journal of Advanced Scientific and Technical Research 7(5), pp 70-82.

Roy, R., Pal, M., Gulati, T., 2013. Zooming Digital Images using Interpolation Techniques, International Journal of Application or Innovation in Engineering & Management 2(4), pp. 34-45.

Saleh, A., Bahaa, A., Wahdan, A., 2011. Fingerprint Recognition. Advanced Biometric Technologies, InTech, pp 201- 224.

Shetter, A., Prajwalasimha, S. N., Swapna, H., 2018. “Finger Print Image Enhancement Using Thresholding and Binarization Techniques.” 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). Coimbatore, India.

Sojan, S., Kulkarni, R. K., 2016. Fingerprint Image Enhancement and Extraction of Minutiae and Orientation, International Journal of Computer Applications 145(4), pp 14-19.

Soundharadevi, N., Pushparani, M., 2016. Analysing on multimodal biometric frame work with face, iris and fingerprint images, Shanlax International Journal of Arts, Science & Humanities 4 (1), pp165-172.

Vijayaragavan, A., Visumathi, J. and Shunmuganathan, K. L. 2014. Cubic Bezier Curve Approach for Automated Offline Signature Verification with Intrusion Identification, Mathematical Problems in Engineering 2014, pp. 928039-928046,

Wang, W., Lu, Y., 2018. “Analysis of the Mean Absolute Error (MAE) and the Root Mean Square Error (RMSE) in Assessing Rounding Model,” IOP Conf. Series: Materials Science and Engineering 324, pp. 1-10.

Wu, W.-C., Wang, T.-H., Chiu, C.-T., 2015. Edge Curve Scaling and Smoothing with Cubic Spline Interpolation for Image Up-Scaling, Journal of Signal Processing Systems 78(1), pp 95-113.

Yaghoobi, S., Moghaddam, B. P., Ivaz, K., 2017. An efficient cubic spline approximation for variable-order fractional differential equations with time delay, Nonlinear Dynamics 87(2), pp 815–826.

Tracing the Roots of Construction Conflicts: Explaining Problems, Preferences, and Process

Abdullah M. Alshehri

Department of Civil and Environmental Engineering, College of Engineering,
Majmaah University, Majmaah 11952, Saudi Arabia, a.m.alshehri@mu.edu.sa

Abstract

The construction industry is continuously struggling to resolve the conflicts equitably and economically. Therefore, the present study aims to trace the roots of construction conflicts by explaining problems, preferences, and processes associated with the construction industry. Quantitative research design has been employed and 116 owners, constructors, consultants, and stakeholders were recruited because of their direct involvement in the construction industry. A questionnaire was distributed among the respondents to trace the problems, preferences, and processes associated with conflicts the construction industry. The results showed that that lack of communication and coordination, contract provisions, ambiguities, bid rigging, contracting classification system, unforeseen ground conditions, and discrepancies were major reasons of conflict. The study has concluded that productivity of construction industry is significantly influenced through the implementation of realistic schedule and plan for the construction project.

Keywords:

Construction Conflicts, Problems, Preferences, Process, Saudi Arabia;

1. Introduction

There is significant increase in complexity of construction project in nature nowadays. The organizational and contractual structures are addressed by the construction procurement by bringing the project under it. Individuals or organizations are brought together through construction projects that were initially disparate to be united and are also known as temporary project coalition or temporary multi-organization (Dada, 2013). However, increased chance of interactions on project lead to conflicts in non-traditional procurement methods, where individuals are sometimes under a single organization. Studies have shown that conflicts are a great challenge within the construction industry as they may lead to litigation, project failures, and in severe cases project abandonment (Tsai & Chi, 2009; Kassab et al., 2010; Tazelaar & Snijders, 2010).

Construction industry is predisposed to disputes and conflicts due to increased pressure, toughness, and harshness associated with this industry. This makes it obvious that contractual disputes and conflicts affect the prosperity of publicly funded construction projects, negatively (Dada, 2013). Construction related conflicts may also arise as a result of involvement of multi-disciplinary in the projects that are inevitable, when the industry itself is facing many uncertainties (Arditi & Pulket, 2005). The conflicts developing within the construction industry are mostly related to contractual matters such as time extension, availability of information, management and administration, quality of technical approaches, determination, and unrealistic customer expectations (Jaffar et al., 2011).

The construction stakeholders consider conflict as alarming for the construction industry and they believe that it is highly important to avoid or resolve the conflicts as soon as possible. Moreover, it has also been shown that conflicts in construction industry may impose functional and dysfunctional impact on the organization and its employees (Jaffar et al., 2011). The disagreement among the internal stakeholders like contractors, subcontractors, and employees is focused in relation to the conflict management in the construction projects. The important factors that enhance project viability include; increase in the personal welfare demands and social conflicts among the external stakeholders (Lee et al., 2017). Min et al. (2018) examined different types of infrastructure patterns, when conflict occurs. On examination, the study revealed major factor that is procedure of deciding facility's location and its route.

The construction industry is continuously struggling to resolve the conflicts equitably and economically. It is important to propose the conflict analysis framework for investigating the occurrence of conflict and its causes by considering the characteristics of public infrastructure projects. The understanding related to mechanisms exerting influence at the team level is limited (Tabassi et al., 2019). In the similar context, the present study aims to trace the roots of construction conflicts by explaining problems, preferences, and processes associated with the construction industry. The construction industry has been chosen in this study because the undertaking of temporary projects in this sector are multicultural in nature, with their own cultural norms and values. This study would help in identifying the problems causing conflicts in the construction industry and would also help in reducing the development of conflicts in this industry.

2. Literature review

The construction related conflicts possess instinct nature and characteristics as their sources vary from one project to another. Li et al. (2012) recruited the stakeholders and analyzed their concerns related to conflicts and its management in the infrastructure projects. The results depicted a great difference in the observations of the stakeholders due to mismatch in certain expectations and perceptions related to development. This mismatch was considered to be the major reason of conflicts in the construction projects. Similarly, Dada (2013) used the traditional and integrated procurement method to investigate the frequency and intensity of conflicts in the construction projects. The study found out certain issues that lead to conflicts in construction industry including the administrative matters and technical issues. The results also showed that traditional method possessed major weaknesses of confrontational and adversarial relationships.

Jaffar et al. (2011) conducted a study to analyze the factors causing conflicts in the construction industry by focusing on behavioral, technical, and contractual problems. The results demonstrated poor communication and reluctance to check for constructability as the factors if conflict due to behavioral problems. The technical problems included failure of the contractor to work competently and not receiving proper instructions from the engineer and architects on time (Jaffar et al., 2011). Moreover, factors of conflict due to contractual problems include unclear contractual terms and conditions, giving late possessions, and delay in interim payment. The mechanism of conflict management is important as it imposes negative impact on the financial status of the industry.

Conflicts are likely to develop when there is disagreement between two or more parties. Ahlers (2012) showed that litigious and acute conflict between contractors and project developers occur due to subsurface condition during construction. Mediation and litigation along with significant impact on project schedule, profit, and relationship occur as a result of budget constraints, delay due to weather conditions, and error in construction documents (Ning & Ling, 2013). Conflict in the form of interpersonal conflict is capable of hampering communication between the stakeholders, which diminishes the project's productivity and hinders the constructive negotiations (Brockman, 2013). It is important to consider the conflict management in construction industry and its impact on performance and profit generation for the sake of leadership personnel and professional management in the construction industry.

The construction industry is not able to manage and provide possible solutions; although, it is well-aware about the conflicts. Therefore, it is important to extend the theory of relationship conflict into the construction management and explain its positive impact on the construction industry (Brockman, 2013). The internal conflicts and disputes are observed within the construction projects because of their dynamic nature affecting productivity of the industry, delayed handover, and decrease in product quality. Ibadov (2015) explained that there is significant impact of selecting right contractor on time required to complete the entire project and manage the prospects for conflict. The contractor is responsible for assisting the organization of construction projects for managing the associated risks considering the increased scope of construction projects in Saudi Arabia.

Alshehri (2013) demonstrated that majority of the conflicts in Saudi construction industry arise due to alteration in the designing and procurement of the project. This alteration is likely to affect the productive capacity of owners, contractors, as well as the consultant team supervisors. Soni et al. (2017) showed that communication within the project is significantly disrupted due to increasing conflicts that makes the project management quiet challenging. Similar to this, Brairrah (2013) narrated that arousal of conflicts declines the team spirit resulting in increase in total cost of the project and also has negative impact on business association among the parties.

3. Material and Methods

A quantitative method has been adopted in this study to investigate the problems causing conflicts in the construction industry and would also help in reducing the development of conflicts in this industry.

3.1 STUDY SAMPLE

The respondents for this study have been selected through random sampling from three different sites in Saudi Arabia. A total of 116 owners, constructors, consultants, and stakeholders have been recruited in this study because of their direct involvement in the construction industry that helped in collecting validated data.

3.2 DATA COLLECTION

The data for this study was collected using self-administered questionnaire that was developed on the website named as survey monkey. Each question in the questionnaire has its own scale that helped in tracing the conflicts and problems arising within the construction industry. The demographic detail of all the respondents including their designation and years of experience was recorded. There was a total of five items on the questionnaire that constituted various issues and conflicts in the effective management of construction projects. The research instrument has traced problems, preferences, and processes associated with conflicts the construction industry as it results in significant increase in the specified cost and also delays the project completion. This procedure of data collected has assisted in gathering information in an effective way that would allow to take corrective measures in effective management of construction project.

3.3 DATA ANALYSIS

The data obtained through the questionnaire was analyzed statistically using Microsoft Excel and presented through tables and graphs. This approach used for data evaluation has helped in tracing problems, preferences, and processes associated with conflicts the construction industry that affect the management of construction project.

4. RESULTS

The responses gathered through the questionnaire were evaluated critically to trace the problems, preferences, and processes associated with conflicts in the construction industry management. Table 1 has presented the demographic details of all the respondents showing that majority of the individuals recruited from the construction industry (35.34%) were contractors. The consultants were ranked at second position with a percentage of 28.44% followed by the owners (20.68%) and the stakeholders (15.51%) (Table 1). Table 1 has also depicted the years of experience of the participants. On the basis of the responses received from the respondents 5-10 years, 10-20 years, and more than 20 years were same i.e. 26.72%; whereas, only 19.82% of the respondents had experience of 0-5 years.

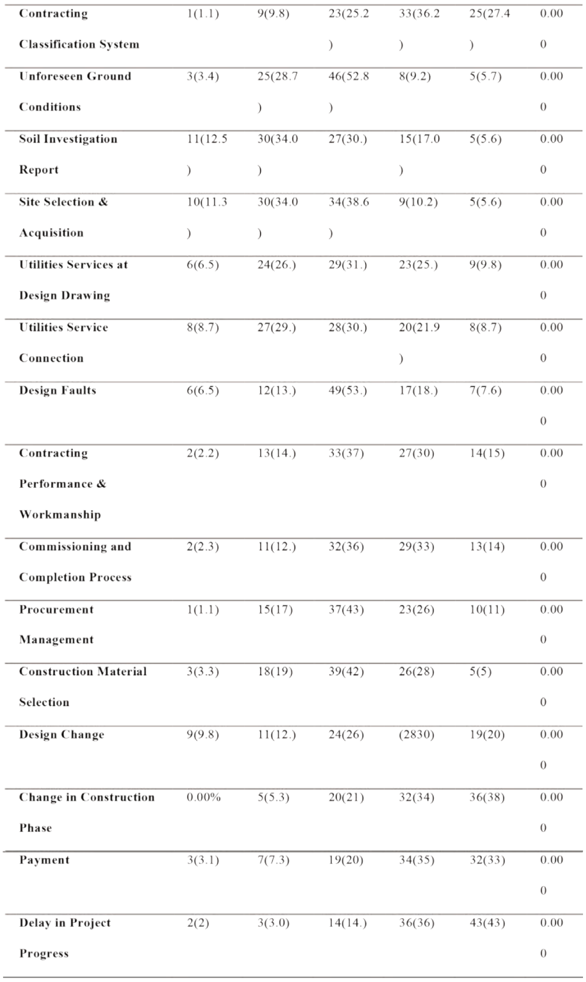
Table 1: Demographic Detail of the Respondents

Measure	Items	Frequency	Percentage (%)
Designation	Owner/Client Organization	24	20.68%
	Contractor	41	35.34%
	Consultants	33	28.44%
	Stakeholders	18	15.51%
Years of Experience	0 – 5 years	23	19.82%
	5 – 10 years	31	26.72%
	10 – 20 years	31	26.72%
	> 20 years	31	26.72%

The results of this study have shown the problems, preferences, and processes that are linked with the arousal of conflict in the construction industry. The respondents were asked to judge the conflicts that are likely to hamper the construction projects in Saudi Arabia. Likewise, the items included in the questionnaire have been illustrated in table 2. The results have depicted that lack of communication and coordination, contract provisions, ambiguities, and discrepancies were major reasons of conflict. Other reasons resulting in conflict development include client's non-compliance (3.09), bid rigging (2.91), contracting classification system (3.79), unforeseen ground conditions (2.85), soil investigation report (2.69), site selection and acquisition (2.65), utilities service at design drawing, (3.05), sitemap utilities service connection (2.92), and design faults in compliance and communication phase (3.08). The results have also shown that all the factors considered in this study had significantly affected the development of conflict in the construction industry (p-value = 0.000).

Table 2: Tracing the frequency of conflict

	Never	Rarely	Seldom	Often	Always	p-value
	Frequency (%)					
Project Briefing	3(3.19)	12(12.7)	24(36.1)	26(27.6)	19(20.2)	0.000
Early Cost Estimation	7(7.6)	18(19.5)	24(36.9)	19(20.6)	14(15.2)	0.000
Architect Selection	6(6.0)	12(12.1)	45(45.4)	19(19.1)	17(17.1)	0.000
Contractor Selection	4(4.3)	4(4.3%)	36(39.1)	33(35.8)	15(16.3)	0.000
Tender Process	6(6.5)	12(13.0)	35(38.0)	27(29.)	12 (13.0)	0.000
Tender Cost Estimation	3(3.3)	14(15.7)	36(40.4)	26(29.2)	10(11.2)	0.000
Lack of Communication/Co-ordination	3(3.3)	14(15.7)	38(42.7)	20(22.4)	14(15.7)	0.000
Contract Provisions	6(6.7)	17(19.1)	28(31.4)	23(25.8)	15(16.8)	0.000
Ambiguities/Discrepancies	2(2.2)	18(20.4)	29(32.)	22(25.0)	17(19.3)	0.000
Client's Non-Compliance	7(7.8)	24(26.9)	24(26.)	22(24.)	12(13.4)	0.000
Bid Rigging	6 (6.5)	33(35.)	27(29.)	15(16.3)	11(11.9)	0.000



Contracting Classification System	1(1.1)	9(9.8)	23(25.2)	33(36.2)	25(27.4)	0.000
Unforeseen Ground Conditions	3(3.4)	25(28.7)	46(52.8)	8(9.2)	5(5.7)	0.000
Soil Investigation Report	11(12.5)	30(34.0)	27(30.)	15(17.0)	5(5.6)	0.000
Site Selection & Acquisition	10(11.3)	30(34.0)	34(38.6)	9(10.2)	5(5.6)	0.000
Utilities Services at Design Drawing	6(6.5)	24(26.)	29(31.)	23(25.)	9(9.8)	0.000
Utilities Service Connection	8(8.7)	27(29.)	28(30.)	20(21.9)	8(8.7)	0.000
Design Faults	6(6.5)	12(13.)	49(53.)	17(18.)	7(7.6)	0.000
Contracting Performance & Workmanship	2(2.2)	13(14.)	33(37)	27(30)	14(15)	0.000
Commissioning and Completion Process	2(2.3)	11(12.)	32(36)	29(33)	13(14)	0.000
Procurement Management	1(1.1)	15(17)	37(43)	23(26)	10(11)	0.000
Construction Material Selection	3(3.3)	18(19)	39(42)	26(28)	5(5)	0.000
Design Change	9(9.8)	11(12.)	24(26)	(2830)	19(20)	0.000
Change in Construction Phase	0.00%	5(5.3)	20(21)	32(34)	36(38)	0.000
Payment	3(3.1)	7(7.3)	19(20)	34(35)	32(33)	0.000
Delay in Project Progress	2(2)	3(3.0)	14(14.)	36(36)	43(43)	0.000

5. DISCUSSION

The results have depicted that construction industry is tasked with constructing the built environment; therefore, it is considered as a large and complex industry. The present study has presented certain factors that are associated with conflicts in the construction industry including; lack of communication and coordination, contract provisions, client's non-compliance, unforeseen ground conditions, site selection and acquisition, and design faults in communication phase. These results were consistent with the study of Vaux (2014) stating that unforeseen circumstances like any change in the construction project and extreme weather and site conditions foster rapid increase conflicts in the construction industry.

There is significant impact of alteration in project design after contract finalization leading to delays in project completion causing disputes and conflicts. These results were consistent with Mahamid et al. (2011), who highlighted the fact the change in design results in conflicts. Moreover, Mohammed and Isah (2012) demonstrated that management of construction project tend to face many problems in its planning and construction phases at the preliminary stage. The study in consistent with present study recommendation stating the importance of smooth communication and involvement of economy manger to ensure effective and timely completion of the construction process. In the present study, delay in project completion is considered as second major complication that disrupts the effective management in construction industry.

In the present study, the views of owners, contractors, consultants, and stakeholders have been analyzed to explain the problems, preferences, and processes associated with the construction industry. Similarly, Yousefi et al., (2010) specified the important role played by decision makers in negotiating during different stages of construction project. Various parties get involved in the construction process and their preferences are either affected positively or negatively concerning the performance of construction project that ensures the project's success. The findings of present study have also depicted that conflict mostly arise in the payment system as ineffective claims and any delay in making payments lead to conflict between two parties. Moreover, Dada (2012) endorsed that the difficulty in the payment occurs due to the inadequate administration of the project's resources, involvement of the multidisciplinary parties, and their regulation.

The study analysis has also shown that working capacity, contracting classification system, unforeseen ground conditions, soil investigation report, and site selection and acquisition cause problems in project management. This fact can be explained on the basis of diversified workforce of Saudi population in terms of skill set. It has been shown that work productivity of the contractors is associated with the overall productivity of the project. Moreover, the project working capacity is associated with the payment system as functioning of involved parties is significantly affected as a result of the delays in payments (Pawar & Patil, 2014). Furthermore, Huang (2011) asserted that selection of contractors is monitored based on certain categories that include their financial competencies and technical capabilities.

6. CONCLUSION

The present study has traced the roots of construction conflicts by explaining the problems, preferences, and processes undergoing in the Saudi construction industry. The results have clearly depicted that there are various factors that are responsible for the development of conflicts in a construction project. The results have concluded that the successful completion of any project depends on how capable the project management team is. The productivity of construction industry is significantly influenced through the implementation of realistic schedule and plan for the construction project. The study results have suggested that the chances of conflicts in the Saudi Arabia construction industry can be improved by setting a realistic timeline with proper backhand working. It also signifies the importance of adequate financial resources to make made in time so to ensure adequate and timely delivery of the construction projects. However, these results are limited because it has just considered a specific population and these results cannot be applied to any other developing or developed countries due to difference in their economic conditions that includes regulatory mechanism, socio-demographic status of consumer, and technological advancements. Moreover, it was difficult to separate necessary factors effecting profit from relationship conflict because of the complexity of the construction industry. Future studies need to address the impact of relationship conflicts on profit among subcontractor management teams to generalize the findings to general contractors.

CONFILCT OF INTEREST

The author declares no conflict of interests.

FUNDING

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

ACKNOWLEDGMENT

The author is very thankful to all the associated personnel in any reference that contributed in/for the purpose of this research.

References

Ahlers, R., Brandimarte, L., Kleemans, I., & Sadat, S.H. (2014). Ambitious development on fragile foundations: Criticalities of current large dam construction in Afghanistan. Geoforum, 54, 49-58.

Alshehri, A.M. (2013). Conflict in Architectural Projects: Diagnosis and Avoidance: a Study Based on Saudi Arabian Construction Industry (Doctoral dissertation, University of Manchester).

Arditi, D., & Pulket, T. (2005). Predicting the outcome of construction litigation using boosted decision trees. Journal of Computing In Civil Engineering © ASCE, 387-393.

Braimah, N. (2013). Construction delay analysis techniques—A review of application issues and improvement needs. Buildings, 3, 506-531. Doi: 10.3390/buildings3030506

Brockman, J.L. (2013) Interpersonal Conflict in construction: Cost, cause, and consequence. Journal of Construction Engineering and Management, 1-12.

Dada, M.O. (2013). Conflicts In Construction Projects Procured Under Traditional And Integrated Methods: A Correlation Analysis.

Huang, X. (2011). An analysis of the selection of project contractor in the construction management process. International Journal of Business and Management, 6, 184.

Ibadov, N. (2015). Contractor selection for construction project, with the use of fuzzy preference relation. Procedia Engineering, 111, 317-323.

Jaffar, N., Tharim, A.A., & Shuib, M.N. (2011). Factors of conflict in construction industry: a literature review. Procedia Engineering, 20, 193-202.

Kassab, M., Hegazy, T., & Hipel, K. (2010). Computerised DSS for construction conflict resolution under uncertainty. Journal of Construction Engineering and Management, 136, 1249-1257.

Lee, C., Won, J. W., Jang, W., Jung, W., Han, S. H., & Kwak, Y. H. (2017). Social conflict management framework for project viability: Case studies from Korean megaprojects. International Journal of Project Management, 35, 1683-1696.

Li, T.H.Y., Ng, S.T., & Skitmore, M. (2012). Conflicts or consensus: An investigation of stakeholder concerns during the participation process of major infrastructure and construction projects in Hong Kong. Habitat International, 36, 333-342.

Mahamid, I., Bruland, A., & Dmaidi, N. (2011). Causes of delay in road construction projects. Journal of Management in Engineering, 28, 300-310.

Min, J. H., Jang, W., Han, S. H., Kim, D., & Kwak, Y. H. (2018). How conflict occurs and what causes conflict: Conflict analysis framework for public infrastructure projects. Journal of Management in Engineering, 34 04018019.

Mohammed, K.A., & Isah, A.D. (2012). Causes of delay in Nigeria construction industry. Interdisciplinary journal of contemporary research in business, 4, 785-794.

Ning, Y., & Ling, F.Y.Y. (2013) Reducing hindrances to adoption of relational behaviors in public construction projects. Journal of Construction Engineering Management, 139.

Pawar, O.A., & Patil, R.S. (2014). Conflicts & Disputes in Construction Projects. International Journal of Innovations in Engineering and Technology, 3(3), 48-53.

Soni, S. Pandey, M. Agrawal, S. (2017). Conflicts and Disputes in Construction Projects: An Overview. Journal of Engineering Research and Application, 40-42.

Tabassi, A. A., Abdullah, A., & Bryde, D. J. (2019). Conflict Management, Team Coordination, and Performance Within Multicultural Temporary Projects: Evidence From the Construction Industry. Project Management Journal, 50, 101-114.

Tazelaar, F., & Snijders, C. (2010). Dispute resolution and litigation in the construction industry. Evidence on conflicts and conflict resolution in The Netherlands and Germany. Journal of Purchasing and Supply Management, 16, 221-229.

Tsai, J.S., & Chi, C.S. (2009). Influences of Chinese cultural orientations and conflict management styles on construction dispute resolving strategies. Journal of Construction Engineering and management, 135, 955-964.

Vaux, J. S. (2014). Relationship conflict in construction management and how it affects performance and profit.

Yousefi, S., Hipel, K.W., & Hegazy, T. (2010). Attitude-based negotiation methodology for the management of construction disputes. Journal of Management in Engineering, 26(3), 114-122.

Journal of Engineering and Applied Sciences (JEAS)