DIGITAL INNOVATION ADOPTION: ARCHITECTURAL RECOMMENDATIONS AND SECURITY SOLUTIONS

Editors:
Muhammad Ehsan Rana
Manoj Jayabalan

Bentham Books

Digital Innovation Adoption: Architectural Recommendations and Security Solutions

Edited By

Muhammad Ehsan Rana
School of Computer Science
Asia Pacific University of Technology & Innovation
Kuala Lumpur
Malaysia

&

Manoj Jayabalan
School of Computer Science & Mathematics
Liverpool John Moores University
Liverpool
UK

Digital Innovation Adoption: Architectural Recommendations and Security Solutions

Editors: Muhammad Ehsan Rana & Manoj Jayabalan

ISBN (Online): 978-981-5079-66-1

ISBN (Print): 978-981-5079-67-8

ISBN (Paperback): 978-981-5079-68-5

First published in 2024.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of the U.A.E. as applied in the Emirate of Dubai. Each party agrees that the courts of the Emirate of Dubai shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.
3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Ltd.
Executive Suite Y - 2
PO Box 7917, Saif Zone
Sharjah, U.A.E.
Email: subscriptions@benthamscience.org

CONTENTS

FOREWORD

I am delighted to write this foreword because I believe deeply in the importance of the topics and of high quality of the contents. There is latest and so much useful information being delivered into its 15 chapters which should not be missed. Thus it gives me a great pleasure to contribute this foreword.

As I reviewed the manuscript prior to writing this foreword, I was impressed by many unique features that I would like to share with you. The book explores the important aspect of the architectural requirements including emerging technologies and security-based concerns for digital innovation adoption. This work would be an important resource of exposure towards the Internet-of-Thing (IoT) and Artificial Intelligence (AI) in various important application domains.

Smart Cities and 5G Networks highlighted the advantages and disadvantages of radio and device-to-device in the context of multiple IoT use cases. IoT in Waste Management introduced an intelligent smart bin system to automate waste handling and management to contribute to green technology. Stock Monitoring System Using IoT Based Automation provided a set of recommendations for a hypermarket stock monitoring system using IoT automation. Secure Healthcare Using Blockchain Technology reviewed blockchain architecture in a health domain in order to secure patients' medical records. E-Voting System Using Blockchain Technology implemented blockchain for e-voting systems of medium and large-scale size.

Decentralised News Using Blockchain Technology explained the implementation of blockchain via a decentralised application to combat misinformation. Cyber Threats in IoT-based Connected Cars exposed vulnerabilities for IoT-based connected cars and their implications. The use of IoT in Contact Tracing: Vulnerabilities and Countermeasures reviewed contact tracing application with IoT. AI-based Intrusion Detection System for IoT Security proposed a solution for security treats for IoT network with Intrusion Detection System. Fake News Detection Using Data Mining Approaches introduced a data mining as a technique to predict fake news.

EEG Signal Classification Using AI Techniques analysed the classification methods for EEG signals. Malware Analysis and Malicious Activity Detection Using Machine Learning reviewed AI techniques to protect and prevent security threats in the IT infrastructure. Interestingly the authors have proposed a machine-learning based detection system to classify suspicious objects. Security Vulnerabilities and Threats for IoT-based Home revealed the security vulnerabilities for the smart home concept and its protection. IoT Policy and Governance Reference Architecture discussed IoT reference architecture, policy and governance for the integrity and security of the information being transmitted within the IoT ecosystem. Organizational Security Improvement in Preventing Deepfake Ransomware highlighted the impact of deep fake ransomware to the organisation and its protection.

The content provides a widely useful compilation of ideas, cases, innovative approaches, and practical strategies for enhancing digital innovation adoption mainly covering the architecture and security. This book should be read by anyone including researchers, educators, industry practitioners and technology specialists who intend to learn, practice, and adopt innovative technology in their respective areas of interest to bring digital transformation by indulging in the architectural requirements and security concerns.

Wan Nurhayati Wan Ab. Rahman, Ph.D
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
Selangor
Malaysia

PREFACE

Digital innovation assists organizations in innovating and driving services to bespoke clients that leverage high value. The integration of major disruptive technologies such as cloud, big data, IoT and blockchain has ignited the retransformation of the entire industrial arena. As a result of this convergence of technologies, organisations need to go through a mandatory process of change at a rapid pace. Every industry, from agriculture to manufacturing, transportation to education, pharmaceutical to health services, is forced to be revolutionised using innovative approaches. Organisation's products, services, and operations need to embrace a technological shift to differentiate themselves in the competitive arena and satisfy their customers' ever-increasing needs. Billions of digitally enabled devices will create the dawn of a whole new era by utilising their sensing, processing, and connectivity power through the use of the Internet of Things (IoT). Consumer-based companies rely heavily on mobile devices to deliver personal experiences. Cloud is redefining the way businesses were previously done. It is a paradigm shift from traditional IT to a more efficient, scalable, and secure infrastructure. Blockchain offers a decentralised structure that demonstrates transparency and trust and provides individual control of data. Organisations need to lay down the sophisticated architectural requirements of the proposed solutions to take advantage of the evolving digital technology. The extensive reliance on these technologies has also possessed some security challenges for providers and consumers. The ubiquitous data access *via* multiple end-user devices has paved the way for security and cyber threats. As information security is critical for contemporary businesses, organisations have an essential role in protecting the information to deal with highly augmented security and privacy threats. This book is intended to explore the architectural requirements of these digitally transformed systems by adopting emerging technologies and examining security-based concerns considering the vulnerabilities and countermeasures for these systems.

Muhammad Ehsan Rana
School of Computer Science
Asia Pacific University of Technology & Innovation
Kuala Lumpur
Malaysia

&

Manoj Jayabalan
School of Computer Science & Mathematics
Liverpool John Moores University
Liverpool
UK

List of Contributors

Attique Ur Rehman	School of System and Technology, University of Management and Technology, Pakistan
Ainkaran Doraisamy	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Abdullah Khalid	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Daniel Mago Vistro	School of Computing, Asia Pacific University, Kuala Lumpur, Malaysia
Intan Farahana Kamsin	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Janesh Kapoor	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Julia Juremi	Forensic and Cyber Security Research Center, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Khalida Shajaratuddur Harun	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Maryam Var Naseri	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Muhammad Shoaib Farooq	School of System and Technology, University of Management and Technology, Pakistan
Muhammad Jawed Chowdhury	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Manoj Jayabalan	School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK
Nor Azlina Abdul Rahman	Forensic and Cyber Security Research Centre, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Nur Khairunnisha Zainal	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
Shiksha	School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK
Waleed Zafar	School of System and Technology, University of Management and Technology, Pakistan
Yap Chi Yew	School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia

CHAPTER 1

Access and Secure Patient Medical Records using Blockchain Technology based Framework: A Review

Daniel Mago Vistro[1,*], Muhammad Shoaib Farooq[2], Attique Ur Rehman[2] and **Waleed Zafar[2]**

[1] *School of Computing, Asia Pacific University, Kuala Lumpur, Malaysia*

[2] *School of System and Technology, University of Management and Technology, Pakistan*

Abstract: Blockchain technology has a key role in electronic health record systems for storing, accessing and securing patients' medical records. Patients' medical information is being stored like personal bio, diagnosis, treatments, *etc.* This information is very sensitive and private, and it has remained a big challenge to access and secure patient medical records in a decentralized manner. Blockchain has become very important for its use in storing, accessing and managing patient medical records in a very secure and decentralized manner. In this paper, a systematic literature review has been done to review blockchain architecture for electronic health records systems to store, access and secure patient medical records. The main objective of this paper is to highlight the use of blockchain in accessing and securing patient medical records. Moreover, some blockchain-based electronic health records systems have been presented to secure the records. Lastly, some challenges and gaps in using blockchain-based medical health records systems have been presented.

Keywords: Block Chain, Centralized, Electronic health records, Framework, Patient medical records, Technology.

1. INTRODUCTION

Patient medical records contain very important information about a patient's health history, medications, and allergies. This information is used by many health care providers and research institutes to provide better care and to conduct research that can lead to new treatments and cures [2]. Different institutions are using the technology to save and secure patient information, but private patient data security is the main issue [3]. The data for patients like personal information,

* **Corresponding author Daniel Mago Vistro:** School of Computing, Asia Pacific University, Kuala Lumpur, Malaysia; E-mail: Daniel.mago@apu.edu.my

Muhammad Ehsan Rana & Manoj Jayabalan (Eds.)

diagnosis, treatments, symptoms, region, *etc.*, is growing with the passage of time. Patient medical record systems that store and manage patient data are being used by different institutions, and it is becoming an important technology [4]. There are many stakeholders that are involved in managing and accessing patient data. But it has with many challenges like data insecurity and accessibility [5]. Patients need to visit different hospitals, clinics or any health care system for medical diagnosis, treatments *etc*, in such cases, patient data sharing is important for better treatment and medications [4]. The patient does not have access to their medical records, which could make it difficult for them to get the care they need. Additionally, patient data can be shared with an unauthorized person or stolen, which could lead to identity theft or other problems.

Blockchain technology is becoming more important these days because it provides many features like decentralized immutability and security of data [1]. Blockchain technology is being used in electronic health record systems that help share the data of patients among many stakeholders. Through blockchain technology, a patient can control who can access the data. It provides security to data by using its advanced algorithms [6].

In this paper, we have presented how blockchain technologies help to improve patient data accessibility and security in electronic health record systems. We have described the architecture of blockchain to understand its working and how it can help to improve the current patient records system. The challenges and gaps in using blockchain have also been presented in this article.

2. RELATED WORK

Patient information is highly sensitive and private; it is being shared with multiple stakeholders. The challenge is to secure the information by using emerging technology such as blockchain because it is quite considerable due to its highly secured hashing algorithms. A survey has been done on the use of blockchain in healthcare that discusses accessibility, security and privacy challenges in electronic health records [2]. However, the challenges in using blockchain-based record systems have not been discussed. The role of blockchain technology has been discussed in telehealth and telemedicine [7]. But the blockchain architecture has not been presented for managing patient records. A systematic literature review of blockchain for electronic health records systems has been done [6] for the security and privacy challenges. However, the security architecture has not been discussed. The use of information in health care by using blockchain technology has been discussed in a study [8]. They have discussed the challenges that affect the transition of patient information. A systematic review has been

done on using of blockchain applications in the health sector. But the blockchain architecture has not been presented.

The novelty in this paper is that we have focused on the role of blockchain in patient medical records in the sense of storing and sharing data. Our study focuses on the security of patient data by using the blockchain. We have discussed the challenges and gaps of blockchain-based electronic health records in this paper.

3. RESEARCH METHODOLOGY

A systematic literature view method has been selected for this paper to review the use of block technologies framework to ensure the availability and security of patient records. The objectives of this review are to provide an overview of how blockchain methods are helping to improve the accessibility and security of patient records in a system. We have used the proposed method by Kai Petersen [9]. We have followed the steps as mentioned in Fig. (**1**).

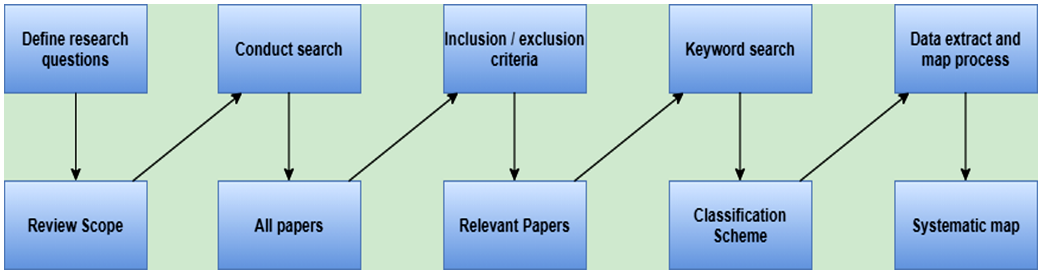

Fig. (1). Steps to conduct a systematic review.

4. RESEARCH OBJECTIVE

The objectives of this research are:

RO1. The main focus is to highlight the use of blockchain methods in accessing, securing managing patient medical records.

RO2. Improving the security of patient medical records while using blockchain.

RO3. Explore challenges and gaps in using blockchain-based electronic health record systems.

5. RESEARCH QUESTION

The important thing in systematic literature views is defining the research questions. After reading a detailed literature review, we have defined the following questions as in Table (**1**).

CHAPTER 2

Identifying Cyber Threats in IoT based Connected Cars for Enhanced Security

Ainkaran Doraisamy[1], Nor Azlina Abdul Rahman[2,*] and **Khalida Shajaratuddur Harun[1]**

[1] *School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

[2] *Forensic and Cyber Security Research Centre, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

Abstract: The Internet of Things (IoT) has garnered many ideas to create new IoT products as well as enhance their existing products with the help of the internet. Tesla is an example of an IoT device from the automotive industry. The most prominent feature of the vehicle was the over-the-air (OTA) updates. A few vulnerabilities were found in Tesla despite being one of the most secure vehicles in the world. The first vulnerability was in the vehicle's key system, where radio signals from the key fob were intercepted in a relay attack. The next vulnerability was due to the Tesla app, where the hacker obtained the owner's login credentials. Besides, the infotainment system of the vehicle also was compromised and hacked using a web browser bug known as a JIT bug. Lastly, Tesla vehicles also had a vulnerability in their navigation system too. This was demonstrated by a group of researchers who staged a GPS spoof attack on Tesla model 3 while it was in Autopilot mode. Fake satellite coordinates were transmitted by the researchers, who were then received by the GPS receiver. This caused the vehicle to decelerate and made an emergency turn-off at a narrow pit stop. These vulnerabilities can be fixed by following safety measures to counter cyber-attacks. More layers of security should be installed on the existing security system to ensure the vehicle does not get exploited easily by hackers.

Keywords: Cyber attacks, Internet of things, IoT vulnerabilities, Key fob, Smart car application and IoT defence.

[*] **Corresponding author Nor Azlina Abdul Rahman:** Forensic and Cyber Security Research Centre, Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia; E-mail: nor_azlina@apu.edu.my

Muhammad Ehsan Rana & Manoj Jayabalan (Eds.)

1. INTRODUCTION

The purpose of IoT is to enable simple things to be connected to the internet in order to gather and exchange data that does not require much human or computer involvement. With IoT, the power of the internet can be extended to a wide range of things such as bottles, mugs, watches, coffee makers and many more. It converts an existing object into a "smart" object in which these things are able to send and receive information. This adds additional value to these objects since more features and opportunities can be unlocked from the objects that make them multifunctional.

Industries have come up with many ideas to create new IoT products as well as to enhance their existing products by implementing and recreating a "smart" product with the help of the internet. There are many advantages of IoT, such as creating more business opportunities. Advanced analytics can be used to obtain insights related to business which may assist in reducing costs on operations. IoT is capable of predicting an issue and acting before it occurs. This is because the network of IoT is able to provide insights from the collected data, which may help to reduce or even prevent maintenance issues or system breakdowns. IoT can also be used as a way to further improvise their products and services to customers. The utilisation of IoT can be a turning point for almost any industry or organisation since it helps to elevate the products or services according to customers' needs [1].

The top 10 IoT application areas in 2020.

The transportation or automotive industry is ranked second in this analysis. It is also evident that the use of IoT in this industry shows a positive trend. In the automotive industry, connected cars are vehicles that run on their own internet connection. Tesla cars are one such prominent example of IoT devices in this industry. There are many applications of IoT in Tesla cars [2]. In terms of connectivity, Tesla has a standard 3G mobile connection that connects the car to the internet, which is free for its users for navigating purposes. Features and the search results for maps are sorted and organised according to distance. Apart from that, there is also a package for premium connectivity in which Tesla car owners are able to gain access to many other applications such as visuals of live traffics, streaming of media and music using Spotify while driving and Netflix as well as YouTube applications while the car is parked. There are also other built-in features such as Bluetooth and Homelink, which automatically control gates, garage doors, lights and even a home security system [3].

Besides, Tesla has an API that helps the owners to lock or unlock their car, to find their car and also to read data. This can be done by installing a Smart car

application and connecting their car to it. By doing this, the car can be locked or unlocked using the mobile application with just some codes lines. Another unique feature of Tesla is that it has Over the Air (OTA) updates. OTA enables the vehicle to update its software versions automatically. These updates are done on the cars on a regular basis to improve the performance and safety of the car. Some of the updates include upgrading the existing design features such as the touchscreen, which are upgraded by modifying the look of it in order to satisfy their customers. OTA updates help to reduce visits to the dealer for maintenance purposes as well as save cost and time. Furthermore, Tesla collects all the performance data of their cars and monitors each car. According to the data collected, if any car needs further maintenance, Tesla would contact the owner to inform and schedule a slot for maintenance of the car [4]. These large amounts of data also will be used by engineers in Tesla for further improvements and to track the driving patterns of their customers. There are sensors in the car that enable screening of the driver to detect and track any reckless driving pattern which might be caused by factors such as the level of fatigue. The monitoring system will then take control of the car speed in order to prevent road accidents.

This system is made up of components such as alcohol, impact and eye blink sensors which are used to locate the car with the help of Google Maps. This system can also be used to detect the exact location of stolen cars by using GPS. The server of the application will receive satellite signals according to the coordinates of the location, and the vehicle owner can be notified and informed after tracking the location of the car, (Fig. **1**).

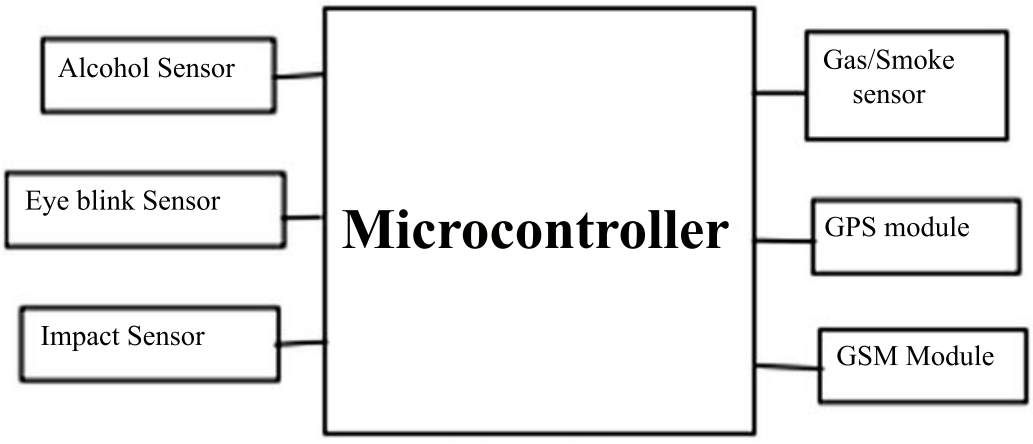

Fig. (1). Monitoring system of a car [4].

CHAPTER 3

Malware Analysis and Malicious Activity Detection using Machine Learning

Muhammad Jawed Chowdhury[1], Julia Juremi[2,*] and **Maryam Var Naseri[1]**

[1] *School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

[2] *Forensic and Cyber Security Research Center, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

Abstract: Criminals are working day and night to get hold of the data. They are also getting more intelligent and are also using AI-powered threats to exploit vulnerabilities to perform an attack. Information security is at a higher risk, now more than ever. Due to the popularity of internet usage by users, the IT infrastructure is prone to security threats. The damage done by computer malware and viruses is known to cost billions of US dollars. Hence, this paper reviews the ways of integrating technology such as machine learning, neural networks, deep learning, *etc*. which can help to develop an intelligent system to protect and prevent the IT infrastructure from security threats. The authors proposed AIVA, a Machine learning (ML) based detection system which is able to classify a suspicious object as "safe" or "dangerous". AIVA is composed of three core components: static analysis, machine learning, and malicious detection.

Keywords: Confusion matrix, Machine learning, Malware analysis, Portable executable (PE) file.

1. INTRODUCTION

Due to the high usage of the internet, it is prone to security threats. Therefore, we need intelligent solutions such as Artificial Intelligence (AI) to combat security threats [1]. A study defines AI as an advanced algorithm that mimics traditional human abilities such as problem-solving and learning from its experiences. As artificial intelligence becomes more powerful, we can use it in the field of cybersecurity to detect security threats such as malware, *etc*.

* **Corresponding author Julia Juremi:** Forensic and Cyber Security Research Center, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia; E-mail: Julia.juremi@apu.edu.my

To implement the various techniques of artificial intelligence to detect security threats, we must also discuss the evolution of security threats such as malware, viruses, *etc*. Malware and virus can spread quickly due to the presence of ever-increasing use of networks and the internet. According to a study done by FireEye [2], 47% of the organizations have faced malware incidents [3]. Another study proposed technological solutions that can be added to increase the effectiveness and performance of malware detection. These solutions include cloud computing, network-based detection systems, web, virtual machines, and hybrid methods and technologies [4]. A study states that traditional defense systems use signature-based techniques. These techniques are unable to detect malware.

The purpose of malware analysis is to provide a deeper understanding of several aspects, such as malware behaviour and its evolution. It can analyse the malicious code in the malware and understand its risks and true intentions. It can also capture the properties that can be used to improve security measures and make it difficult to avoid detection [6]. Hence the author supports the process of using machine learning to extract features from Windows executable. Among various platforms such as Android, MacOS, *etc*., Windows Operating System remains the preferred target among the rest due to its popularity.

As illustrated in Fig. (**1**), malware analysis by using machine learning can be divided into three major categories. The first category defines the objectives of the analysis, the second describes the features that the malware analysis is based on and finally the third one being what type of machine learning algorithm is used.

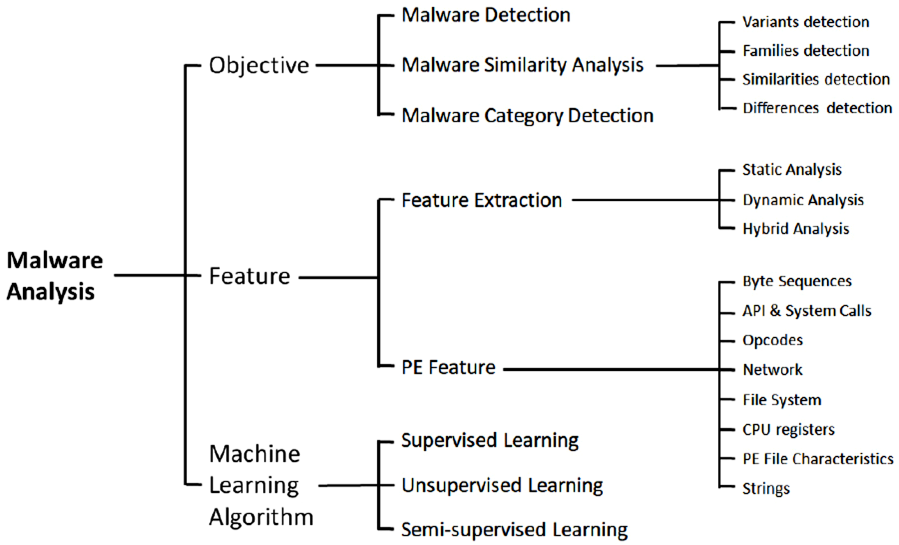

Fig. (1). Taxonomy of malware analysis.

The objective of analysing malware is to detect whether a given file is malicious. From the findings, the author emphasizes the importance of knowing whether a file is malicious in advance as it allows it to get blocked before the malware becomes harmful. The second objective is to spot the similarities among malware, to help understand how new malwares are evolving and how they differ from the previous malware. The analysis of the malware can be derived by detecting their variants, families, similarities, and differences. Attackers often reuse the available codes and resources from previous malware samples to develop variants. By recognizing malware as a variant, it helps to understand how the variant has evolved from its predecessor. By knowing the similarities, it helps to narrow down the search more towards the features that have not been discovered before. Analysing the differences can give us new information to look forward to for new insights. The authors [5] mention categorizing the malware according to their malicious behaviour as it helps to describe the malware. For example, if the malware is encrypting and asking for a ransom, it can be classified as "Ransomware".

Detection systems that are developed with malware analysis can decide if an object is a threat based on the data that the system has collected. This data may be collected at different phases: Pre-execution phase and Post-execution phase. The pre-execution phase is basically static analysis which is knowing anything about the file without its execution whereas post-execution is basically dynamic analysis which is analysing the file and recording its behaviour and activity during its execution process.

Feature extraction is the process of identifying the key features in a Portable Executable (PE) file and extracting the features [6]. For the machine learning algorithm, we need to consider what features to analyse, how to extract these features from a Portable Executable (PE) file by using static, dynamic or hybrid analysis. Static analysis is performed before the malware is executed. It analyses what its true intentions are and what code it is trying to execute. Dynamic analysis, on the other hand, is performed after the malware has already been executed, analysing its functionality. This is mostly carried out in a safe environment such as the Sandboxes [7]. A study mentions some of the examples of information that can be extracted by dynamic analysis. They include API calls, system calls, instruction traces, registry changes, memory writes, *etc*. Moreover, hybrid analysis is a combination of both static and dynamic analysis. It merges two aspects of analysis which are signature specifications of malware code and then combines it with malware behavioural parameters. Due to this approach, hybrid analysis overcomes the limitation of merging these two aspects of static and dynamic analysis [8].

CHAPTER 4

Secure IoT based Home Automation by Identifying Vulnerabilities and Threats

Abdullah Khalid[1], Nor Azlina Abdul Rahman[2] and **Khalida Shajaratuddur Harun[1,*]**

[1] *School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

[2] *Forensic and Cyber Security Research Center, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

Abstract: The Internet of Things (IoT) is a mesh network of "electronic things" that are capable of acquiring data using embedded sensors and customized software or technologies, amalgamating and exchanging the information with other devices, as well as executing a customized action. This encompasses everything connected to the internet from the smallest devices such as coffee makers to sophisticated industrial control systems. As the IoT aggressively becomes interwoven in every aspect of our lives, cyber-security has become a necessity. This research aims to highlight the security vulnerabilities in IoT-based Home Automation, discuss the risks that end users can be faced with, as well as provide defense against the classified risks.

Keywords: Business continuity planning, Home automation, Internet of things, Smart home, Smart home security, Smart home vulnerabilities.

1. INTRODUCTION

The term "Internet of Things" was coined by Kevin Ashton back in the 1990s, where his idea was simply to install an RFID tag, a tiny microchip, in everything that his company produced [1]. The recent aggressive boom in the production of IoT and its applications has not only made a huge impact on people's daily lives but also on businesses. The world of IoT is presently gigantic, according to Priceonomics [2], there are currently 50 billion IoT devices, which will generate 4 zettabytes of data as of 2020. The yearly sales revenue from IoT devices is forecasted to hit $1.6 trillion by 2025 from just $200 billion today. This will make you to be able to conserve more energy as well as be less worried about the security of your home since all of the installed devices can be accessed remotely

* **Corresponding author Khalida Shajaratuddur Harun:** School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia; E-mail: khalida@staffemail.apu.edu.my

Muhammad Ehsan Rana & Manoj Jayabalan (Eds.)

from anywhere. Lastly, the Smart home architecture is completely scalable, providing homeowners the feasibility of upgrading their existing appliances or adding new ones to the existing network which remain updated to the latest technology trends [3].

2. SMART HOME IOT

The enormous diffusion of various devices connected to each other in the number of billions has created the serious necessity of implementing robust security measures, as all these devices are continuously connected to the internet in one way or another. The convenience of controlling your home lights and garage doors just with a few taps on your smartphone is becoming a habit for many people, thus making the smart home industry worth billions of dollars. It was expected that by the end of 2019, the smart home devices sold would add up to a whopping 1.9 billion. Furthermore, it is predicted that the smart home market could grow to $53 billion by the year 2022 [4].

As shown in (Fig. **1**), the market shares of various IoT sectors, it can be seen that smart home automation holds the four largest market shares from all the IoT sectors.

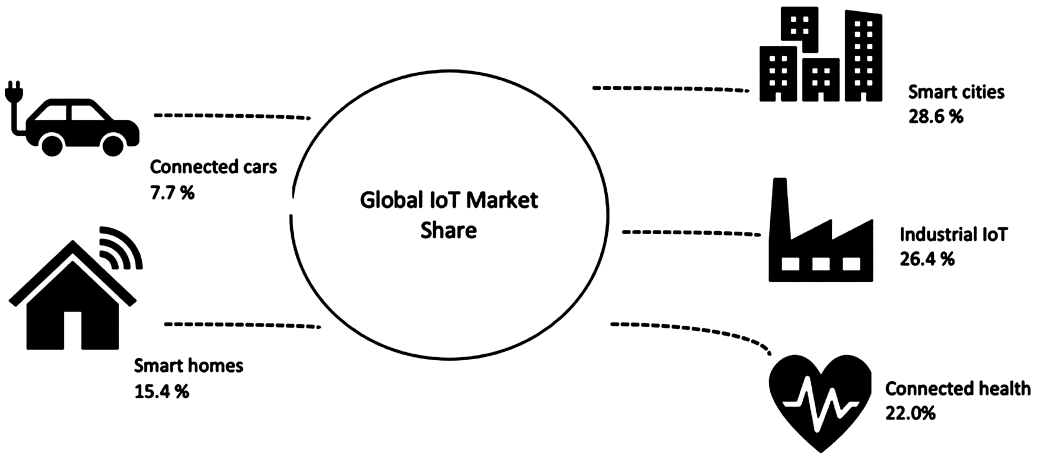

Fig. (1). Global IoT market share [4].

Due to the low-cost availability of most of these devices, the manufacturers do not spend an ample amount of time or effort in properly securing them and continuously improving towards the betterment of their security. These devices have ended up, in turn, being an attractive choice of targets for cyber-criminals [5]. There is a rapid increase in the number of threats, with the attacks increasing both in sophistication and in number. Alongside the increase in the number of

attackers, the tools they are utilizing have become more efficient and effective than before. The larger the number of connected devices, the greater the attack surface they provide for cyber-criminals. Not all IoT devices having vulnerabilities are considered insecure, however, in many cases, they can only be exploited by physical access to the device itself. This will result in there being a lesser risk for the average end-user. Yet again there are many ways the devices can be penetrated remotely through the internet, and be abused with malicious intentions [6]. It is crucial to identify the vulnerabilities that currently and potentially exist, along with finding out what the impact exploiting these could have on the end-user.

2.1. Smart Homes Architecture

The primary goal of smart home architecture is to connect all IoT devices and achieve access, remote control, and monitoring of the home environment whilst using the internet as the communication backbone [7]. Technically the home automation system consists of five separate blocks: the devices that are under control, the devices containing sensors and actuators, the network through which all the devices are being controlled, the controller, and the remote-controlled devices [8]. In Fig. (**2**) shown below, the IoT devices can be any smart home appliances ranging from electric kettles to smart TV's, from humidity sensors to smart home security monitoring cameras, from smart gardening to smart central heating of homes, from RFIDs to smart wearables, from smart door locks to personal AI assistants such as Amazon's Alexa. The IoT gateway interacts between different types of communication technologies which may vary in different protocols and establishes a bridge between the IoT devices and the internet. Prior to sending the data onwards through the internet, the gateway aggregates all the data it receives from the devices, translates the sensors protocols, and performs the pre-processing of data. The IoT devices connect to the IoT gateway using wireless transmission modes such as Bluetooth, ZigBee, LTE, or Wi-Fi, followed by bridging them further onto the public cloud [9]. Finally, all the collected data travels to the specified web servers or the customized IoT applications which perform the analysis on the collected real-time monitoring data as well as perform the required actions. An example of said actions is lowering and adjusting the temperature and humidity of the home environment after being detected as high by the sensors, and further enhancing the onboard intelligence to change the temperature to the same settings every day at this very specific time, Fig (**2**).

CHAPTER 5

IoT Policy and Governance Reference Architecture: Integrity and Security of Information Across IoT Devices

Yap Chi Yew[1], Intan Farahana Kamsin[1] and **Nur Khairunnisha Zainal[1,*]**

[1] *School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

Abstract: The Internet of Things (IoT) technology has been applied to our daily life infrastructure to make our lives easier and more comfortable. However, various variations in the IoT reference architecture represent that the developers need to be aware in order to implement the technology in a secure and accurate form. The knowledge of these reference architectures is important as they provide the guidelines for IoT developers and enterprises to develop high-quality IoT products. Requirements such as security, data process, and privacy issues must always be concerned. The reference architectures are used in the development of IoT products. This paper discusses and explores IoT-related field topics ranging from IoT reference architecture to policy to governance. Different kinds of variations in the reference architecture and the IoT governance policy are discussed to ensure the integrity and security of information transmitted across devices in the IoT ecosystem.

Keywords: Architecture, Governance, IoT, Policy.

1. INTRODUCTION

The implementation of IoT technology is growing immensely nowadays. The overwhelming use of technology by humanity should be considered from fair management architectures under major governance. Therefore, IoT management and governance are paramount to be enforced on those who is directly or indirectly benefited from the technology currently and in the future. The architecture was designed to ensure that connectivity, data processing, and security systems of IoT technology can provide a reference architecture to solve the complexities and management of the IoT. Governance is vital to control the

[*] **Corresponding author Nur Khairunnisha Zainal:** School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia; E-mail: khairunnisha.zainal@staffemail.apu.edu.my

Muhammad Ehsan Rana & Manoj Jayabalan (Eds.)

IoT technology development today [1 - 5]. IoT policy is needed to monitor the development of IoT technology. Therefore, we need to study how management and governance work and affect the IoT technology.

2. REFERENCE ARCHITECTURE OF IOT

Reference architecture is usually a model framework architecture that is suitable and adaptive to be repeated over time. IoT technology needs architecture to be managed because the old IT technology is based on fragmented software implementations which proved to be difficult for monitoring and controlling in the past [1]. An architecture is introduced to serve as a guidance standard to make the management work easier than before. There are big requirements for reference architecture of IoT technology in the enterprise to make the development more tangible and profitable [1]. Therefore, some variations and innovations have evolved the reference architecture currently, to fit the ecosystem of IoT that keeps changing according to times. The evolved reference architectures that are commonly used today are Internet of Things-Architecture (IoT-A), Industrial Internet Reference Architecture (IIRA), and Service-Oriented Architecture (SOA). These reference architectures are purposed to assist interoperability, monitor invention, and moderate usage of IoT technology, Fig. (**1**).

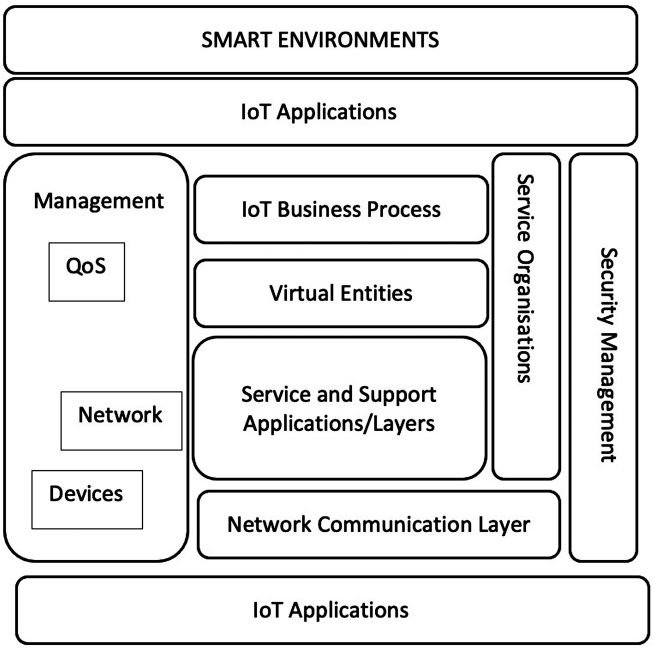

Fig. (1). Internet of things—architecture (IoT-A) [2].

Internet of Things—Architecture (IoT-A) gives a comprehensive view of the data and information of IoT technology [1]. IoT-A is greatly used in today's development environments due to its advantages. The IoT-A focuses on the common aspects of informatics instead of the usage of the IoT technology [2]. This situation can let developers who use IoT-A design to develop specific IoT devices for a wider range of usages. Hence, these kinds of IoT devices are designed to be suitable for the transformation of data as well as information usage, which is a major part of IoT technology nowadays. Furthermore, the IoT-A widely encompasses abstract modelling and structuring of IoT business process management, resources, and services from the angles of information and functionality [1]. For instance, cloud servers are implemented for server management but the IoT devices of users are used in domain-specific computers. IoT-A has management mechanisms and security protocols implemented across IoT devices [1]. For example, Hypertext Transfer Protocol Secure (HTTPS) is used to safeguard the data transmission of IoT devices. EXI (Efficient XML Interchange) is implemented for managing the exchange of data on IoT devices. These mechanisms and protocols that are used in IoT-A have greatly benefited the development of IoT technology. Therefore, these excellent features have made the IoT-A a good managing architecture for the development of IoT technology.

Industrial Internet Reference Architecture (IIRA) mainly focuses on the usability of IoT technology for the industry sector and the interoperability among industries [3]. Thus, IIRA can focus more on industry and business use cases. IIRA also has management mechanisms and security protocols like IoT-A implemented across IoT devices. Four important viewpoints that build up the IIRA: Business Viewpoint, Usage Viewpoint, Functional Viewpoint, and Implementation Viewpoint [3]. The Business Viewpoint is defined as the clients and their business perspectives, targets, and benefits [3]. The Usage Viewpoint is the expectation of the IoT technology in the industry to provide the expected market goals and targets. Furthermore, Implementation Viewpoint describes the necessity of implementation of the respective IoT technology for the respective functional usages. Said uses include the communication system, data rates of the system, and other technical features. Lastly, Functional Viewpoint is known for the functional elements along with the connection and interaction among the IoT devices in the ecosystem [3]. This Functional Viewpoint lets the IoT devices connect among themselves to complete the operations and tasks that can help humans. These four essential viewpoints make IIRA greatly used in the industry sector to manage and control IoT technology more efficiently.

Service Oriented Architecture (SOA) combines IoT technology into service-based connectivity that is agile and reusable, focusing on the end-users, Fig. (**2**) [4]. SOA is an architecture that combines large scale private and public IoT systems

CHAPTER 6

Organizational Security Improvement in Preventing Deepfake Ransomware

Janesh Kapoor[1] and **Nor Azlina Abdul Rahman**[2,*]

[1] *School of Computing & Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

[2] *Forensic and Cyber Security Research Centre, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia*

Abstract: Ransomware is one of the most popular threats in the cyber world. There is an emerging technique for integrating artificial intelligence (AI), deep machine learning, and facial mapping for creating fake videos of people doing and saying something that they have not actually done. Deepfake ransomware is an attack where deepfake technology is being used in ransomware campaigns. Anyone can become the victim or target of this attack, however, this research paper focuses on the impact of deepfake ransomware on organisations. It covers potential risks that an organization might face due to deepfake ransomware attacks such as customer trust, organization reputation, and many other impacts. Besides that, this paper also discusses defence techniques that an organization could consider implementing in protecting the organization against deepfake ransomware attacks. Implementing the defence without awareness will not be effective, hence it is highlighted several times in this paper, that awareness is needed amongst the employees and employers to prevent the organisation from deepfake ransomware. Additionally, it also mentions possible risk management, business continuity, and disaster recovery plans that should be considered by the organization whilst handling the situation of deepfake ransomware attacks.

Keywords: Deepfake ransomware, Organizational security, Security awareness, Risk management, Business continuity.

1. INTRODUCTION

With the use of machine learning technology and artificial intelligence integration, deepfakes have been increasingly difficult to capture as an attack, because deepfake videos are seemingly authentic. Attackers use such attacks as ransomware towards organisations [1 - 3]. For instance, an attacker creates deepfake videos of an organization in which the CEO talks about the company

* **Corresponding author Nor Azlina Abdul Rahman:** Forensic and Cyber Security Research Centre, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia; E-mail: nor.azlina@apu.edu.my

Muhammad Ehsan Rana & Manoj Jayabalan (Eds.)

and announces insolvency. The attacker then uses the material to threaten the organization until the ransom is paid. If the ransom is not paid, the attacker may release the material to the media or publish it on social media channels. This research discusses the impact and potential risks to the organization, business continuity, risk management, and disaster recovery measures taken by the organization. Additionally, it covers defense techniques for improving organizational security to prevent deepfake ransomware, as well as information sharing and awareness of deepfake ransomware.

1.1. What is Deepfake?

Deepfakes are defined as computer-generated images, videos, and voices that are made to imitate the biometric characteristics of a person. Characteristic details such as facial expressions, appearances, and voices are manipulated with detail that makes deepfakes believable [4]. The phrase deepfake is a combination of the terms ‘deep learning’ and ‘fake’. Deep learning refers to the arrangement of algorithms that allow the software to learn and make intelligent decisions on its own [5 - 7].

1.2. How Deepfakes are Created?

Deepfakes rely on machine learning, which uses two networks that are fed the same data sets and compared against each other. Deepfakes are created using a machine learning tool called generative adversarial networks (GANs) [8, 9]. Generative adversarial networks consist of two machine learning models, one of which trains itself to create and imitate using massive data sets, whilst the other detects the imitation that was created. This is done until the first model creates an imitation that is unrecognizable to each other [10, 11]. Hence, deepfake videos are manipulated with the use of Artificial Intelligence (AI) and Machine Learning (ML). Contrary to this, ransomware is a form of malware that prevents victims from accessing their personal data unless the ransom is paid [11].

Ransomware refers to a deepfake video with voice mimicking capabilities that appear to be genuine. However, the deepfakes that are made could be of malicious intent and include pornographic videos or a CEO's speech about insolvency to an organisation. Therefore, deepfake tech can be used in ransomware campaigns or *vice versa*.

1.3. Why Deepfakes were Created?

Deepfakes used to be of good intent such as mimicking someone in a funny perspective. The technology of deepfakes is still being used in the film industry for 3d movies, animations and special effects [12]. However, cybercriminals have

turned this technology into malicious ware. As deepfake uses fake content to deceive its viewers, it is used to spread misinformation and other malicious data. In the past, only people with specialised skills were able to create such content. Unfortunately, the ever-rising race in technology and the ease of obtaining such technology have made it easy for anyone to use [13]. The instigation of machine learning and smartphone apps such as ReFace, Face Swap Live, Snapchat, and others has allowed anyone with a smartphone to create deepfakes.

This poses a major threat to any business or organisation, as it can incite panic and misinformation to produce harmful outcomes [14 - 16]. Thus, the deepfake's malicious intentions to organisations are to spread scams or hoaxes, incite pornography, for social engineering manipulation, and to identity theft, and financial fraud. An example of said financial fraud is how voice skins are used to create audio deepfakes that pose as legitimate, and, in turn, prove to be a threat to CEOs of organisations. An example is the case of a chief executive of the firm's German parent company, which demanded a fraudulent transfer of $243,000 [17].

2. DEEPFAKE RANSOMWARE IMPACT AND POTENTIAL RISK TO THE ORGANIZATION

Deepfake ransomware generates negative impacts and potential risks to an organisation. As compared to the traditional threat of fake news, deepfakes are harder to detect, thus, leading people to dismiss genuine footage as fake. As an attacker creates deepfakes of an organisation, competitors may use this to their advantage as consumers lose the trust of the organisation. Furthermore, brand sabotage, blackmails, financial fraud, and others would be incriminating to an organization [18]. Due to the current pandemic of COVID-19, workplaces are conducted virtually. With this digital transition, the increase of video conferencing and other digital tools gives more access to deepfake material to be created more deceivably [19].

The CIA triad, confidentiality, integrity, and availability, of information security, is an organisation's pride to protect. This shows the organisation manages its CIA to gain the trust and loyalty of its customers and stakeholders. Thus, the deepfake ransomware attack scatters the CIA of an organisation's responsibility to its customers and stakeholders, resulting in impacting the organisation [20 - 22]. The impact on an organisation and the potential risk may include:

2.1. Customer's Trust and Confidence

A customer's trust and confidence is an organisation's main priority, and any deepfake ransomware or disinformation would result in the loss of it. Moreover, the irrefutable damage would have the organisation in disarray to gain its integrity

CHAPTER 7

Use of Machine Learning in Credit Card Fraud Detection

Manoj Jayabalan[1*] and **Shiksha**[1]

[1] *School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK*

Abstract: Credit card fraud is a growing concern, and it poses a significant threat as individual information is being misused and causing a substantial monetary loss. Hence, the prevention of credit card fraud is crucial. Credit card fraud detection is used to differentiate the transactions, either as legitimate or fraudulent. Recently, different machine learning techniques have been implemented to detect credit card fraud. However, the main challenge with fraud detection is that the credit card data is highly skewed, with the fraudulent transactions as less as 1% of the total data. This study investigates the performance of the four supervised machine learning algorithms: logistic regression, support vector machine, decision tree, and random forest, along with different sampling techniques to better understand the fraud detection attributes and performance measures associated with it. This review is also concentrated on exploring different works where the model has a better value for all of the performance evaluation metrics: Recall, precision, F1-score, accuracy, MCC, AUC, and area under the precision-recall curve. This will detect credit card fraudulent transactions better and control credit card fraud.

Keywords: Decision tree, Logistic regression, Random undersampling technique, Random forest, Random oversampling technique, Supervised machine learning algorithms, SVM, SMOTE.

1. INTRODUCTION

Organisations dealing with money are the soft targets for fraudulent activities. Fraud is an illegitimate effort to get information from anyone (internal and external threat) who is acquainted with the system and the security measures through various means [1 - 3]. According to Shift Processing, more than 24 billion dollars were lost in 2018 due to credit card fraud [4]. A credit card is a payment card issued by a financial institution to the cardholder to make purchases with

[*] **Corresponding author Manoj Jayabalan:** School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK; E-mail: m.jayabalan@ljmu.ac.uk

ease [5]. The rapid growth of e-commerce has led to a large increase in the use of credit cards, which has become a necessity of financial services [6].

Online usage of credit cards is an easy target for fraudsters, as it does not require the physical presence of the card [7]. As the operation of credit cards is increasing, there is a higher chance of people (other than the cardholder) misusing it for their own interest. This intentional and illegal misuse of someone's card or its information without their knowledge for attaining financial help to cause loss is termed as credit card fraud [6]. The technology that credit card companies utilises to detect fraud cases is known as a fraud detection system (FDS). The main goal of an FDS is to reduce the false alarm rate and maximise accuracy [8]. The FDS should be quick in action, and the credit card should be immediately revoked once the fraud is detected [9].

Numerous studies have shown machine learning algorithms for credit card fraud detection [9 - 14]. The selection of a suitable algorithm is a complex step towards building the model, and it should always be selected according to the required condition. Hence, the purpose is to review the existing studies using different supervised machine learning techniques on the highly skewed dataset. This will help in better detecting the fraudulent transaction as well as controlling the credit card fraud. The rationale to explore the four techniques selected in this paper: logistic regression, support vector machine, decision tree, and random forest is because of their performance values and advantages reported in the different literatures. Moreover, not many papers have compared the result of all four techniques in a single work, so this work focuses mainly on said algorithms, comparing the performance of the classifiers based on accuracy, sensitivity, specificity, precision and AUC.

2. CONTROL LAYERS IN CREDIT CARD FRAUD DETECTION SYSTEM

In the real world, credit card transactions are inspected rapidly using machine learning algorithms to investigate the transactions and to generate the alert for the sceptical records. These alerts are inspected to know whether it is a genuine or a fraud case, after which feedback is provided as a label for that transaction. It is a significant challenge to investigate every instance of sceptical records due to the time and cost factor. Additionally, these transactions will be unlabelled if customers are not reporting for these transactions. It is stated that this problem, coined as verification latency, has been ignored by several researchers, and it has also been assumed that the labelling of each transaction is done continuously for the fraud detection system [12, 13]. Fig. (**1**) represents a formal design of the real-world fraud detection system with its main features [13]. It is observed that layers

1-4 have been implemented automatically, whereas the last layer requires human interference.

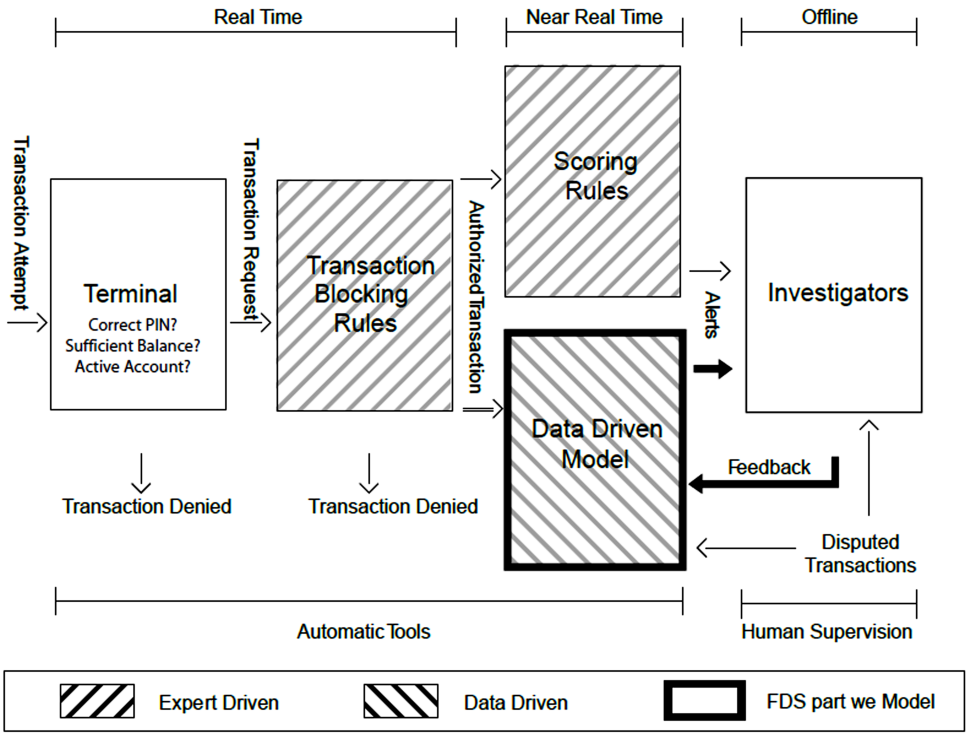

Fig. (1). Control layers used in the fraud detection system [13].

Control layers used in the fraud detection system:

- Terminal: It is the first layer of control for fraud detection and carries out all the required safety measures for all the transaction instances. Such instances include: pin code, card status, number of attempts for accessing credit card, and balance. The response for the online transaction should be in real-time, in milliseconds of time, while the terminal gets details for that particular card from its issuing organisation. If the instances lack any of these details, the transaction is declined. In the case of a successful event, it is passed on to the second layer of control.
- Transaction blocking rules: It is the second layer of control that comes in action after the request is passed from the terminal. These rules are like if-(then)-else conditions, which are used to revoke the fraud transactions. These rules work on

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Muhammad Ehsan Rana

Prof. Muhammad Ehsan Rana did Ph.D. in software engineering. With a career spanning over 20 years, he has excelled in teaching, research, and academic management. Currently, he serves as an associate professor at the Asia Pacific University of Technology & Innovation (APU), Malaysia. He has authored and co-authored more than 100 research articles, conference publications, and book chapters, focusing on areas, such as computer architecture, cloud computing, IoT, and blockchain. His expertise and dedication are evident through his involvement as a reviewer for several prestigious indexed journals and his active participation in organizing IEEE and other international conferences. An advocate for bridging the gap between academia and industry. He has played a crucial role in incorporating industrial collaboration into academic endeavors. Notable collaborations include renowned companies such as, IBM, EMC, Semtech, ARM, Salesforce, CASUGOL, MSTB, MIMOS, among others. Through these collaborations, he has fostered valuable connections and facilitated the integration of real-world industry practices into academic settings.

Manoj Jayabalan

Prof. Manoj Jayabalan is a postdoctoral fellow at Liverpool John Moores University, UK, with over 15 years of experience in academia and industry. He holds a Ph.D. in computing from the Asia Pacific University of Technology & Innovation, Malaysia, MSc. in software engineering from Staffordshire University, UK, and a B.Engg (computer science) from Anna University, India. He is widely recognized for his outstanding contributions in teaching and research. His expertise spans data science, artificial intelligence, machine learning, health informatics, and software engineering. He has published over 50 articles in reputable academic journals, conferences, and books, receiving commendation for his research excellence.