SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Enhancing Cybersecurity: Ransomware Detection - A Proof of Concept Study

Tamara Nusairat[1], Madihah Mohd Saudi[2,*], Azuan Ahmad[2], Muji Setiyo[3]

[1] Faculty of Science and Engineering (FSE), Department of Computer Science and Engineering (CSE), Irbid National University, Road International Road 35, Irbid, Jordan
[2] Cyber Security and Systems (CSS) Research Unit, Faculty of Science and Technology (FST), University Sains Islam Malaysia (USIM),71800 Nilai, Negeri Sembilan, Malaysia
[3] Center of Energy for Society and Industry (CESI), Universitas Muhammadiyah Magelang, Jl. Bambang Sugeng km.05 Mertoyudan Magelang, 56172, Indonesia

ABSTRACT

Presently, our digital landscape faces a pervasive onslaught of diverse cyber threats, encompassing distributed denial of service (DDoS), phishing, ransomware, and smishing, all orchestrated with malicious intent. Counteracting these malicious incursions poses a formidable challenge, particularly in devising efficacious detection solutions. Ransomware incidents are on the ascent, particularly within critical sectors such as healthcare, finance, and telecommunications. Consequently, this paper introduces a proof of concept (POC) aimed at detecting ransomware activities targeting Internet of Medical Things (IoMT) devices. The primary objective of this paper revolves around the identification and evaluation of factors correlating with ransomware attacks on IoMT and then developing a ransomware detector. The experimental framework involves the utilization of a simulated environment mirroring real-world IoMT devices and networks. The methodology integrates diverse approaches, encompassing data collection from IoMT devices, analysis of ransomware behaviour through the study of encryption patterns, and anomaly detection. The POC assesses the efficacy of these methodologies in detecting and responding to ransomware threats, with the experimentation conducted through hybrid analysis within a controlled laboratory setting. The dataset consists of 13 families with a total malware of 9251 taken from GitHub. For POC, a total of 3459 ransomware dataset samples have been selected. As a result of the experiment, thirteen (13) distinct features have been identified as trigger factors for ransomware attacks. These features are obtained by capturing of the processes initiated by the ransomware samples using a process monitor (procmon). A temporal pattern of the processes which include the file system, API, and access based on their frequency of occurrence were used to develop a ransomware detection model. The proposed approach achieved an accuracy of 99.2% and an error rate of 0.8 %, when evaluated on temporal pattern dataset and by using an enhanced artificial neural network (EANN).

Keywords:

Ransomware attacks; Hybrid analysis; IoMT; Ransomware detection

* *Corresponding author.*
E-mail address: madihah@usim.edu.my

https://doi.org/10.37934/araset.54.2.252268

1. Introduction

In the rapidly evolving landscape of technology, the integration of the Internet of Things (IoT) within the realm of medical devices has ushered in transformative possibilities for healthcare. However, this advancement is not without its challenges, as the intersection of medical technology and the digital realm introduces new vectors of vulnerability. These vulnerabilities are taken as an advantage by malware to wreak havoc on the entire Internet of Medical Things (IoMT) ecosystem.

Malware is the main term encompassing a variety of harmful software versions, such as viruses, ransomware, and spyware. The virus is often distributed by email as a link or file. Specifically, ransomware is a virus that infects users by encrypting data and restricting lawful access to user data. The irrevocable nature of a ransomware attack distinguishes it from other types of malwares. Once encryption is completed, the only method to decode the user files is to utilize the decryption key. To decrypt the data, attackers demand payment in an untraceable currency, such as Bitcoin introduced by Comito *et al.,* [3]. At the forefront of these threats lies the insidious ransomware attacks, a menace that holds the potential to disrupt not just data and services, but also patient well-being. Ransomware attacks can infiltrate systems, encrypt critical data, and demand ransom for its release.

In the context of the Internet of Medical Things (IoMT), where devices are interconnected to improve patient care, the consequences of successful ransomware attacks are alarming. As life-saving medical equipment becomes digitally linked, the vulnerability of such systems to malicious actors becomes a main concern. Looking at the complex landscape of cyber threats within the healthcare sector, specifically focusing on the challenges posed by ransomware attacks targeting the IoMT, the demonstration and evaluation of different approaches is very important. In response to this growing risk, increasing investments in cyber security capabilities have been explored as a means for reducing cyber-attacks and encouraging the use of technologies to cut the menace [1]. For optimal exploration of these capabilities, the determination of proof of concept (POC) of various approaches for detecting ransomware attacks within the IoMT ecosystem emerges as a crucial defence strategy. In the context of the IoMT ecosystem, a POC aims to provide evidence that a particular detection method or solution can work effectively. This paper evaluates different potential features that serve as the sources of ransomware attacks. Hence, the objective of this paper is to identify features of ransomware samples that can attack an IoMT ecosystem and then build a ransomware detector with features using an enhanced artificial neural network.

The analysis was conducted using a hybrid analysis and other processes including MD5, execution, initial access, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, collection, control and command, impact, and network communication. It involves the collection of datasets which are thoroughly cleaned through the pre-processed approach and then analysed in a VMware which creates a secured and isolated space of experiment. Introducing the ransomware samples into a virtual server one after the other, allowing real-time monitoring and analysis of its actions. As a result, this paper identified thirteen (13) related features that triggered ransomware attacks. These features are based on vulnerability analysis, potential attack routes, and the effects of a successful security breach against the security devices.

The paper is organized as follows: section 1 is an introduction, section 2 discusses background, section 3 consists of methodology, section 4 presents results and discussion, and section 5 contains conclusion.

2. Background

There are a few considerations in developing a ransomware detection mechanism, especially for the IoMT ecosystem. This includes an understanding of the ransomware and IoMT architecture. In the rapidly evolving landscape of the Internet of Medical Things (IoMT), ransomware attacks in IoMT environments pose a great danger, they can exploit critical vulnerable devices, disrupt healthcare fed, and jeopardize patient safety. These malicious software variants can exploit IoMT networks through various vectors, such as unsecured devices, vulnerable software, or phishing attacks on healthcare staff. Once inside, ransomware encrypts patient data or takes control of essential medical equipment, holding them hostage until a ransom is paid. The consequences of such attacks can be devastating, not only in terms of financial losses but also in compromising the integrity and confidentiality of patient information. As the IoMT ecosystem continues to expand, safeguarding against ransomware and other malware threats becomes an imperative task for healthcare providers, demanding robust cybersecurity measures, regular updates, and staff training to mitigate the risks and ensure the continued safety and reliability of medical systems. Ransomware types (locker and crypto) occupy a significant place in malware families. Many institutions and organizations have been exposed to ransomware threats, resulting in significant financial and reputation loss. Ransomware encrypts files on the target computer using robust cryptographic algorithms by Ilker *et al.*, [4]. The locker type prevents the computer's OS and applications from running. It even opens the computer to prevent the user from performing routine operations. In contrast, the other type encrypts the files in the computer's disk through the functions of the computer's OS by Weckstén *et al.,* [5]. The most common attack vectors used in ransomware attacks are spam and phishing e-mails using social engineering techniques by Mimura *et al.,* [6]. Ransomware attacks have shown no signs of slowing down in 2023. A new report from the Malwarebytes Threat Intelligence team shows 1,900 total ransomware attacks within just four countries the United States of America (USA), Germany, France, and the United Kingdom in one year. Attackers often employ advanced encryption techniques to secure communication between infected systems and command and control (C&C) servers. By using strong encryption algorithms and secure communication protocols, they can make it difficult for security tools to intercept or analyses the traffic. Recent research on this topic highlights the increasing use of encryption in cyberattacks was written by Symantec in 2022. Literature has shown characteristics of the most important ransomware samples as shown in Table 1.

Table 1
Types and characteristics of the most important ransomware samples

Reference	Name	Method of Infection	Date	Payload	Encryption Algorithm
Alotaibi *et al.,* [7]	Bad Rabbit	It appears as an Adobe Flash Player update patch	September 2017	Spread over internal and external networks via SMB service	AES algorithm
Aishwarya *et al.,* [8]	Clop	It infected email attachments	February of 2019	XGBoost outperforms all other machine-learning algorithms	N/A (not available)
Kyurkchiev *et al.,* [9]	Crypto locker	Opening spam e-mails	September 5, 2013	Scanning the network devices, modifying the names of the files and folders, and encrypting files	RSA asymmetric
Beşiktaş *et al.,* [10]	Crypto Wall	Hidden Tear malware	November 2013	Trojan horse to encrypt files on a	RC4

				compromised computer	
Kara *et al.,* [11]	Cerber	Bleeping Computer	First half of 2015	Encrypted with the ". cerber" extension and pop-ups are shown in HTML format	AES-256 and RSA
Almashhadani *et al.,* [12]	Locky	Macros in a Word document	February 2016	After the victim activates macros, the macro will start downloading executable file of Locky	DGA algorithm
Trautman *et al.,* [13]	WannaCry/ Wanna	Microsoft's Server Message Block (SMB) protocol	May 12 2017	Exploit vector named Eternal Blue	N/A (not available)
Chen *et al.,* [14]	Cuba ransomware group	It infects email attachments (macros), torrent websites, malicious ads.	August 2022	Cuba (files are also appended with a unique ID and cyber criminals' email address).	RSA algorithm
Aidan *et al.,* [15]	Petya	Encrypt the Master File	April 2016	Causes a full blue screen of death crash by overwriting the Master Boot Record (MBR)	N/A (not available)
Raulin *et al.,* [16]	Look bit	Data encryption to render victim data inaccessible and threats to release stolen data on designated leak sites	January 2023 to June 2023	Block user access to computer systems	N/A (not available)
Nicho *et al.,* [17]	BlackCat	The payload was launched via *dllhost.exe*	January 2023 to June 2023	Deletes backups to prevent recovery	N/A (not available)
Sarowa *et al.,* [18]	Clop	It steals passwords, banking details, and other sensitive data once infected, potentially jeopardizing individual and business security	January 2023 to June 2023	Encrypts data, renaming each file by appending the. clop extension to encrypted files.	N/A (not available)

Ransomware attacks have been successful primarily because of poor cyber awareness practices. Researchers have proposed a few advanced techniques for ransomware avoidance. However, they are limited to specific environments and strands of ransomware and hence do not qualify as a one-for-all solution. Ransomware attacks follow a specific pattern that can be observed in each family and variant of ransomware by Al-Rimy *et al.,* [19].

The IoMT infrastructure involves several types of online communications technologies such as Wi-Fi technology, GPS and RFID connection of the IoMT devices and sensors to the cloud platforms have become possible sources of security breaches as presented by Hireche *et al.,* [20]. By linking medical gadgets, tools, and other healthcare-related systems to the Internet, IoMT has changed the healthcare business differently. However, as with any system that connects to the Internet, security vulnerabilities have arisen. Paul *et al.*, [21] and Strielkowski *et al.*, [22] believe that the healthcare security business alone will be worth $8.7 billion in the United States. One of the IoMT's primary goals is to achieve minimum human involvement throughout healthcare operations and regular patient visits. Sensor automation and smart machine approaches are employed for this purpose. The

goal of an intrusive device implanted in the human body or a non-invasive device attached to the skin is to collect sufficient information about a patient. This type of medical treatment reduces physicians' time to interact with the patient's diagnosis and reduces the frequency of hospital visits was introduced by Tomiko *et al.,* [23]. In addition, IoMT can lower patient expenses while increasing the efficiency of healthcare providers. Despite the benefits of the IoMT discussed, adopting IoMT is still attended with every new set of obstacles such as security and privacy because of the general opinion that medical data are overly sensitive and invasive. Huang *et al.,* [24] proposed the concept of patients frequently objecting to the sharing of medical or health-related information. The problem is that since IoMT includes and welcomes all sorts of devices and apps in the setup, it also makes it more open to various security and privacy assaults. The security breach includes a malicious device or gadget managed by an unknown party causing a possible breach of patient information privacy. The accurate data may result in accurate diagnoses and the adverse of this notion could endanger the lives of targeted individuals. Hackers might exploit the IoMT environment to access essential healthcare information, which could be used as a physical threat to the victims and may cost lives by Tawalbeh *et al.,* [25]. Additionally, healthcare workers may be falsely accused of conducting incorrect treatments or falsifying data, among other things. As the use of IoMT expands, the security and networks must be strengthened. To mitigate the dangers and assaults to which IoMT infrastructures are vulnerable, new lightweight and robust techniques must be devised. The primary aim of this review is to identify and evaluate the corresponding factors that triggered the ransomware attacks against IoMT.

Ransomware attacks against the IoMT leverage specific features within the IoMT architecture to achieve their malicious objectives. Although the characteristics may differ between attacks, several identified features have commonly triggered ransomware attacks on the IoMT. These features include vulnerabilities in software, such as outdated or unpatched systems, insecure communication protocols that facilitate unauthorized access, weak authentication and authorization mechanisms that enable attackers to gain control, inadequate network segmentation and isolation that allow for rapid spread of the malware, insufficient data backup and recovery mechanisms that make it challenging to restore encrypted data, lack of security awareness and training among healthcare professionals, absence of intrusion detection and prevention systems. Understanding and addressing these identified features are crucial to enhancing the security posture of the IoMT and mitigating the risks posed by ransomware attacks.

For this paper, an experiment was conducted in a controlled lab environment to assess vulnerabilities, potential attack routes, and the consequences of security breaches on the IoMT with a total of 9251 malware taken from a GitHub. For POC, a total of 3459 ransomware dataset samples have been selected. The details procedures for the experiment, which is part of the proof of concept (POC) can be referred to in section 3.4.

Based on the POC conducted, thirteen (13) features were extracted from the analysis. These features cover various stages and aspects of cyberattacks, offering valuable insights into IoMT security. These include initial access, persistence, execution, defence evasion, credential access, discovery, impact, command and control, privilege escalation, lateral movement, collection, network communication, and MD5 analysis. The POC was conducted as a part of the whole analysis of the ransomware dataset. It is beneficial as a baseline analysis and to understand these features in mitigating ransomware attacks against IoMT. Furthermore, POC is significant to determine whether the proposed analysis and features extracted are feasible before continuing a bigger dataset and further analysis.

The features of ransomware, intricately woven into the fabric of its malicious design, often stem from a meticulous vulnerability analysis. Cybercriminals strategically exploit weaknesses in software,

authentication mechanisms, and human behaviour to orchestrate ransomware attacks. These vulnerabilities serve as entry points, allowing ransomware to infiltrate systems and encrypt valuable data. From software vulnerabilities that remain unpatched to weak authentication practices and deceptive phishing emails, ransomware features are intimately linked to identifying and capitalizing on security gaps. Consequently, understanding and addressing these vulnerabilities through proactive cybersecurity measures are essential in defending against the devastating consequences of ransomware attacks.

In the healthcare industry, it is plausible that the importance of the IoMT whose ultimate purpose is to gather and transmit health information such as ECG, weight, blood pressure and sugar levels. Such data may be shared with an approved individual, who may be a physician, a participating health company, an insurance provider, or an external contractor regardless of their time, location, and device. However, the issue is not as simple as presented because IoMT faces various emerging cyber-attacks and threats. New malware attacks are created daily and launched on IoMT. These attacks range from denial of service (DoS), router attack, sensor attack, repay attack, fingerprint, and time-based spoofing to more recent malware attacks such as Miari, Emoted, Gamut and ransomware in IoMT written by Mushtaq *et al.,* [26]. The healthcare sector faces an evolving and increasingly sophisticated ransomware threat landscape, as evidenced by recent studies by Smith *et al.,* [27]. These threats specifically target IoMT devices, including critical equipment like medical sensors, infusion pumps, and interconnected healthcare records. Healthcare-related ransomware attacks have surged, underscoring the urgent need for mitigation strategies introduced by Brown *et al.,* [28]. Numerous vulnerabilities in IoMT architectures have been identified as ransomware entry points. These vulnerabilities range from insecure device configurations by Gupta *et al.,* [29] to deficient network segmentation by Chen *et al.,* [11] and inadequate encryption of patient data presented by Lee *et al.,* [30]. Additionally, the absence of standardized security protocols for IoMT devices presents a significant challenge by Johnson *et al.,* [31]. To address these threats, researchers have proposed a range of mitigation strategies aimed at bolstering the security of IoMT architectures. These strategies encompass device hardening by Roberts *et al.,* [32], network segmentation by Wang *et al.,* [33], threat intelligence sharing presented by Miller *et al.,* [34], and the adoption of blockchain technology to ensure data integrity by Clark *et al.,* [35]. In conclusion, the convergence of ransomware and IoMT architectures poses a critical challenge for healthcare organizations. This literature review sheds light on the dynamic threat landscape, vulnerabilities, and mitigation approaches in the context of ransomware attacks on IoMT devices. As the healthcare sector continues to embrace IoMT technologies, the development of robust security measures, standards, and protocols is imperative to safeguard patient data and uphold the integrity of medical services.

Recently, Ransomware classification has become a common area of research because of its implication on individual and corporate organizations. Ransomware detection systems have been widely classified using different algorithms, most especially neural networks. Agrawal *et al*., [36] proposed the use of neural cells to integrate ARI (Attended Recent Inputs) learning mechanism which uses LSTM (Long Short-Term Memory) networks. It was used to analyse ransomware executables. They classify the input sequences with ransomware as “1” and the benign as “0”. They used sequences of data obtained from benign and ransomware PE files setup on the user’s computer which contains the Windows operating system. It was shown based on their result that the accuracy of the ARI-LSTM surpasses that of the LSTM. Houria *et al.,* [37] also compared the performance of Artificial Neural Network (ANN) and Bayesian Network (BN) on a proposed ransomware dataset, it demonstrated that ANN performs better than the BN.

3. Methodology

In this section, we describe the hardware setup for creating a virtual environment to determine the potential features that cause ransomware attacks. The virtual environment is required when extracting features from any malware because of its infectious nature, especially for dynamic (behavioural) and static analysis. A virtual environment is usually created on an operating system using a virtual machine (VM). VM creates an alienated environment similar to that of a normal operating system on IoMT devices which can curb the infection ability of live malware attacking the actual or original machine. The VM can be easily discarded after identifying the malware features. In performing this exercise, some hardware and software selection are required.

3.1 Feature Data Collection

The experiment involved a step-by-step process carried out in a controlled laboratory setting, utilizing open-source tools (VMware), Cuckoo Sandbox, and Ubuntu (Linux operating system). To begin with, a ransomware dataset was collected for analysis from GitHub. The dataset underwent pre-processing and transformation to ensure accurate and reliable results. A controlled lab environment was then created using VMWare, providing a secure and isolated space for the experiment. The tools for analysis were installed within this environment to enable a comprehensive analysis of the ransomware's behaviour. The next step involved injecting the ransomware dataset into a virtual server, allowing for real-time monitoring and analysis of its actions. Through the use of hybrid analysis, different features were exhibited by different samples of the ransomware which give a valuable insight into the behaviour and potential sources of ransomware attacks.

First, a dataset comprising known ransomware samples is collected and pre-processed to extract relevant features. The methodology for executing the work is reproduced in the flowchart shown in Figure 2.

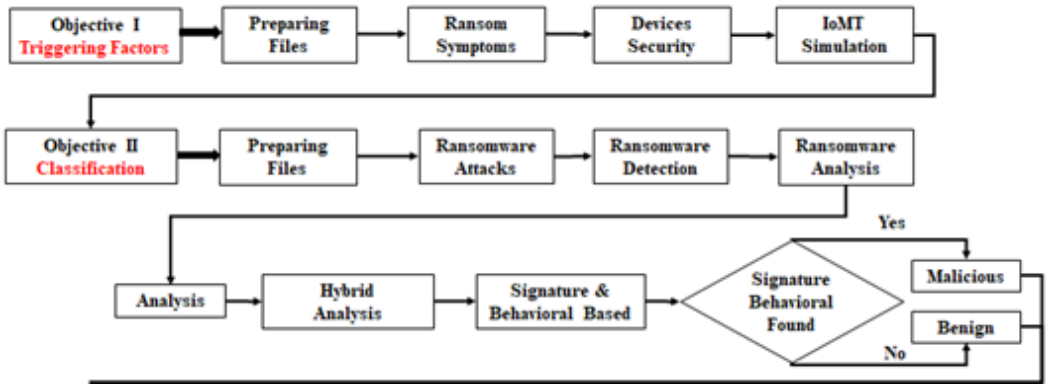


Fig. 2. Flowchart of the methodology

Malicious attackers either listen to the message being delivered to discover information (see Figure 3), also known as passive eavesdropping, which was carried out by Kim *et al.,* [38].

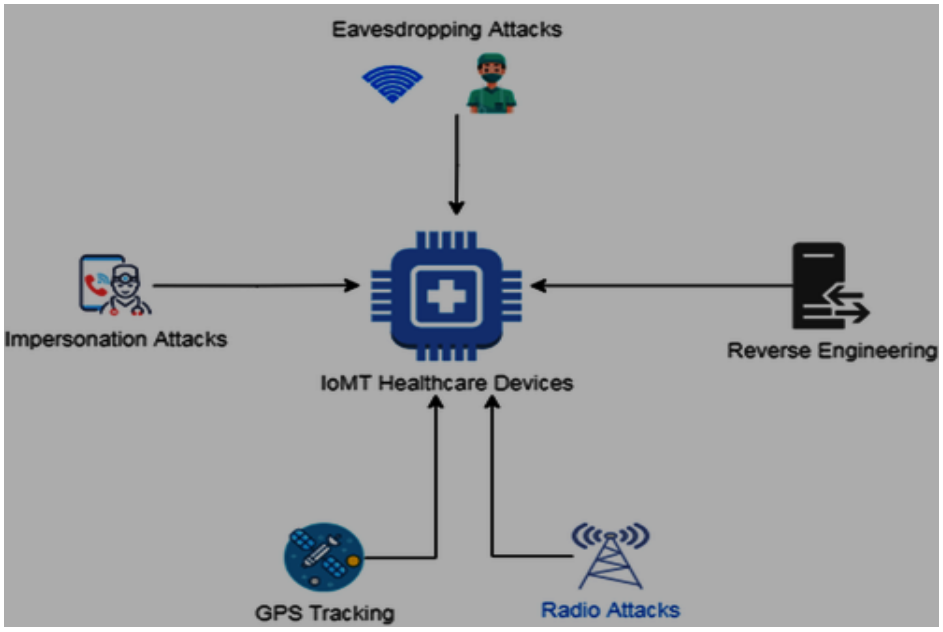


Fig. **3**. Attacks on IoMT by Hasan *et al.,* [39]

3.2 Data Pattern Extraction

The first step in ransomware feature identification involves a meticulous examination of potential features relevant to ransomware detection. Understanding the distinctive characteristics of ransomware attacks is crucial to identify features that encapsulate the essence of malicious behaviour. Static features, encompassing file attributes and characteristics that remain unchanged during execution, and dynamic features, capturing the runtime behaviour of ransomware, will be scrutinized to construct a comprehensive feature set. More attention is paid to file system operation, API calls, registry operation [1-3], as well as other suspicious actions such as file creation, file lock and file encryption.

The main approach used in identifying the ransomware request in file system processes after I/O access requests monitoring is the manner and frequency in which I/O request repetition is generated based on the malicious process instructions. Studies have shown that ransomware samples could be identified based on different process pattern of I/O file system [2], registry key access and API calls. The detection criterion is based on read, write, delete and encrypt or lock activities in I/O sequences for each malware execution process captured. Figure 4 shows different level access patterns for some families of ransomwares studied under this research, for crypto locker and crypto wall families.

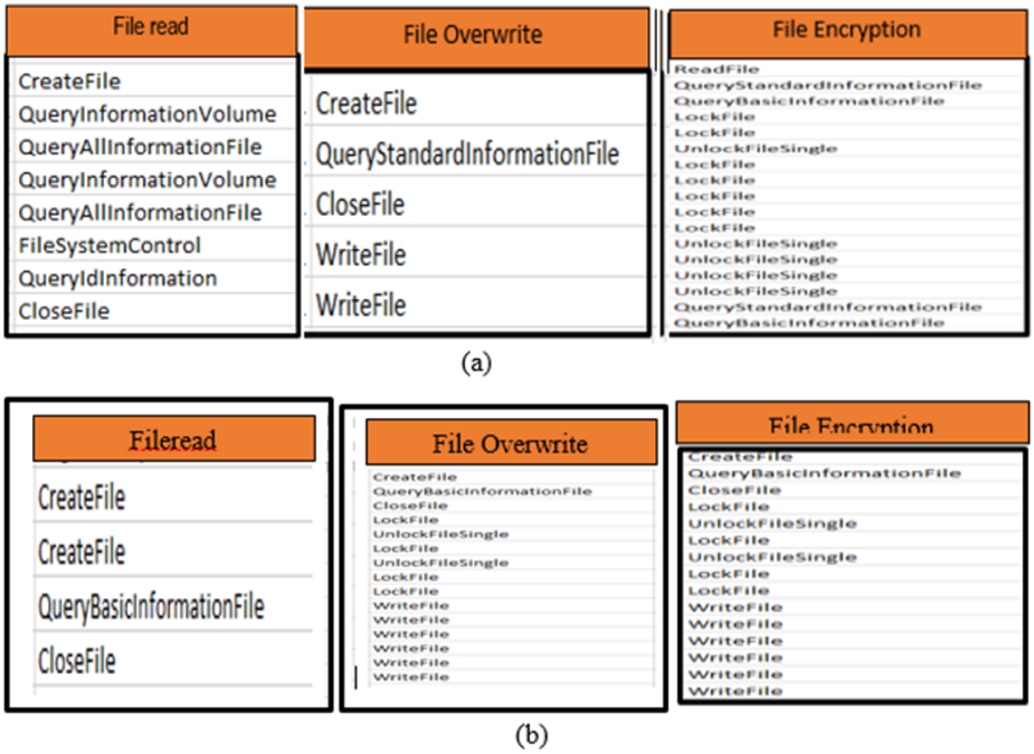


Fig. 4. Input and Output access patterns for (a) Cryptolocker and (b) Cryptowall ransomwares

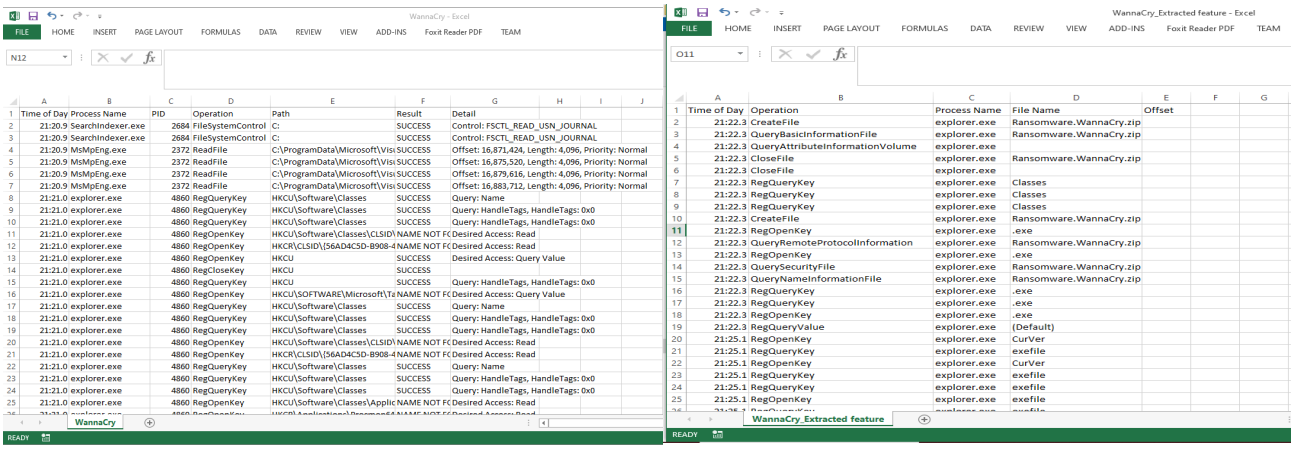
The description of the various attributes of the process monitor operation command is as shown Table 2. The malicious process in a successful ransomware assault often seeks to create, read, encrypt, overwrite, or erase user files at some point during the attack.

Table 2
Datasets attributes and description

S/N	Attributes	Description
1	CreateFile	seeks to create a specified file, if the file already exists in the file path, the function opens it
2	QueryInformationVolume	Queries storage volume information
3	QueryIdInformation	Queries file information ID
4	QueryAllInformationFile	Queries all files for all its information
5	QueryStandardInformationFile	The standard and basic information about the file is queried.
6	LockFile	Locking or encryption of the file
7	WriteFile	Writing a file

3.2.1 Data pre-processing

The dataset is grouped according to process time, process operation, process ID, process name and file path. The required group for training is the process operation, process name and file path. The required groups were extracted from the dataset using a python code. The proposed model's classifier identification capability performs effectively on different pattern combinations, registry, API and file system. Because the process pattern, API, registry access pattern and file system demonstrate the behavioural features of the ransomwares. Figure 5 shows a sample of the dataset and the extracted ones.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
21:20.9	SearchIndexer.exe	2684	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
21:20.9	SearchIndexer.exe	2684	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
21:20.9	MsMpEng.exe	2372	ReadFile	C:\ProgramData\Microsoft\Visi	SUCCESS	Offset: 16,871,424, Length: 4,096, Priority: Normal
21:20.9	MsMpEng.exe	2372	ReadFile	C:\ProgramData\Microsoft\Visi	SUCCESS	Offset: 16,875,520, Length: 4,096, Priority: Normal
21:20.9	MsMpEng.exe	2372	ReadFile	C:\ProgramData\Microsoft\Visi	SUCCESS	Offset: 16,879,616, Length: 4,096, Priority: Normal
21:20.9	MsMpEng.exe	2372	ReadFile	C:\ProgramData\Microsoft\Visi	SUCCESS	Offset: 16,883,712, Length: 4,096, Priority: Normal
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegOpenKey	HKCU\Software\Classes\CLSID\	NAME NOT FC	Desired Access: Read
21:21.0	explorer.exe	4860	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4	NAME NOT FC	Desired Access: Read
21:21.0	explorer.exe	4860	RegOpenKey	HKCU	SUCCESS	Desired Access: Query Value
21:21.0	explorer.exe	4860	RegCloseKey	HKCU	SUCCESS	
21:21.0	explorer.exe	4860	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegOpenKey	HKCU\SOFTWARE\Microsoft\Te	NAME NOT FC	Desired Access: Query Value
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegOpenKey	HKCU\Software\Classes\CLSID\	NAME NOT FC	Desired Access: Read
21:21.0	explorer.exe	4860	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4	NAME NOT FC	Desired Access: Read
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
21:21.0	explorer.exe	4860	RegOpenKey	HKCU\Software\Classes\Applic	NAME NOT FC	Desired Access: Read

Time of Day	Operation	Process Name	File Name	Offset
21:22.3	CreateFile	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	QueryBasicInformationFile	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	QueryAttributeInformationVolume	explorer.exe		
21:22.3	CloseFile	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	CloseFile	explorer.exe		
21:22.3	RegQueryKey	explorer.exe	Classes	
21:22.3	RegQueryKey	explorer.exe	Classes	
21:22.3	RegQueryKey	explorer.exe	Classes	
21:22.3	CreateFile	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	RegOpenKey	explorer.exe	.exe	
21:22.3	QueryRemoteProtocolInformation	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	RegOpenKey	explorer.exe	.exe	
21:22.3	QuerySecurityFile	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	QueryNameInformationFile	explorer.exe	Ransomware.WannaCry.zip	
21:22.3	RegQueryKey	explorer.exe	.exe	
21:22.3	RegQueryKey	explorer.exe	.exe	
21:22.3	RegOpenKey	explorer.exe	.exe	
21:22.3	RegQueryValue	explorer.exe	(Default)	
21:25.1	RegOpenKey	explorer.exe	CurVer	
21:25.1	RegQueryKey	explorer.exe	exefile	
21:25.1	RegOpenKey	explorer.exe	CurVer	
21:25.1	RegQueryKey	explorer.exe	exefile	
21:25.1	RegQueryKey	explorer.exe	exefile	
21:25.1	RegOpenKey	explorer.exe	exefile	

Fig. **5**. Sample of the dataset and the extracted ones

3.2.2 Feature extraction techniques

The extraction strategies used to distil relevant information from the process operation patterns stored in the CSV file generated by process monitor (Procmon), preparing the data for subsequent filter-based feature selection. The choice of specific strategies is made to align with the characteristics of the ransomware detection problem and the insights sought from the process operation patterns for each ransomware family. This is implemented because each family of ransomware have peculiar process operation pattern. The feature extraction strategies used for this research employed hybrid of sequence analysis approach where the sequential nature of system calls within each ransomware family process are captured and file access patterns. This is used to create sequences of N consecutive system calls, API calls, and registry access to analyse their occurrence patterns and then build matrices representing the transition probabilities between different system call types. The later explore patterns related to the order and frequency of file accesses to analyse the process operations for each family of the ransomware. The same process is implemented for the ransomware dataset as shown in Figure 6. A python code program is used to extract the patterns in relation to their order and frequency of file access.

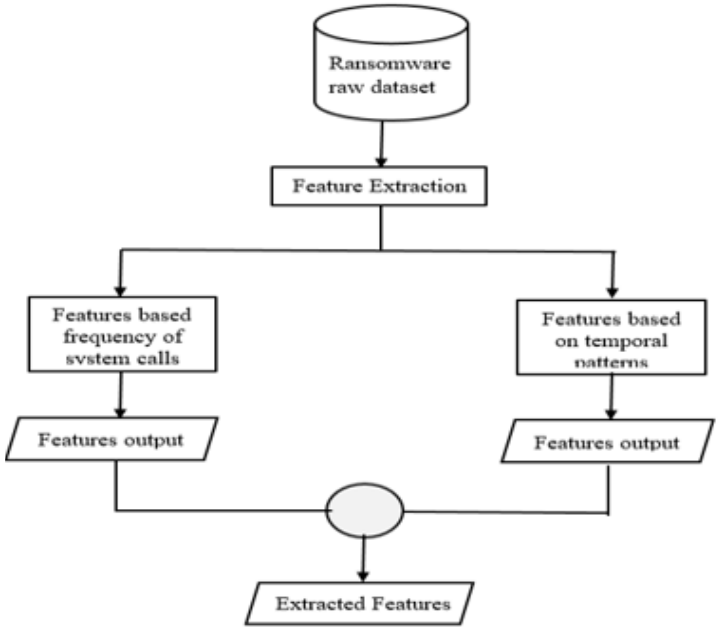


Fig. **6.** Feature extraction process from the raw ransomware

3.3 Enhanced Weight Initialization

Weight initialization is a critical aspect of training Artificial Neural Networks (ANNs). Proper initialization helps in faster convergence, better generalization, and mitigates issues like vanishing or exploding gradients during training. If all the neurons in a layer start with the same weights e.g. setting all weights to zero, they will compute the same output during backpropagation, leading to symmetric weight updates. This can hinder the learning process. During backpropagation, gradients are used to update weights. If the initial weights are too small, gradients can vanish, making learning slow. If they are too large, gradients can explode, leading to instability during training. For an enhanced weight initialization, different weight initialization methods are applied based on the activation functions of the layers. For the first hidden layer with ReLU activation, He weight initialization was used and it is described as Eq. (1).

$$W \sim \mathrm{N}\left(0, \frac{2}{\text{number of input units}}\right) \quad (1)$$

Where the weights are initialized from a Gaussian distribution with mean 0 and variance $\frac{2}{\text{number of input units}}$. It is stated in the code as:

model.add (layers. Dense (128, input_dim=input_dim, activation='relu', kernel_initializer = he_normal ()))

The second hidden layer with *tanh* activation and the output layer with *sigmoid* activation are initialized with Glorot weight initialization and it is given as in Eq. (2):

$$W \sim \mathrm{N}\left(0, \frac{2}{\text{number of input units} + \text{number of output units}}\right) \quad (2)$$

In the code, the second hidden layer and the output layer were initialized using Glorot initialization as:

model.add (layers. Dense (64, activation='tanh', kernel_initializer=glorot_normal ()))
model.add (layers. Dense (1, activation='sigmoid', kernel_initializer=glorot_normal ()))

This produces a more stable training due to appropriate initialization for each layer, it prevents problems of vanishing/exploding gradients which give room for a faster convergence. However, a more complex processing will be required because of different initialization methods for different layers.

3.4 Experimental Procedure

The dataset samples were acquired from GitHub, with a focus on ransomware detection. It comprises 13 families, totalling 9521 samples, with a 37% ransomware percentage. For POC, a total of 3459 ransomware dataset samples have been selected.

The dataset is arranged as X and Y, where the features (X) and labels (y) are arranged X and y should be NumPy arrays or pandas Data Frames. For a two classes problem (binary), the output of the neural network is a probability denoted as P ($y = 1$). The cross-entropy loss L is expressed as in Eq. (3):

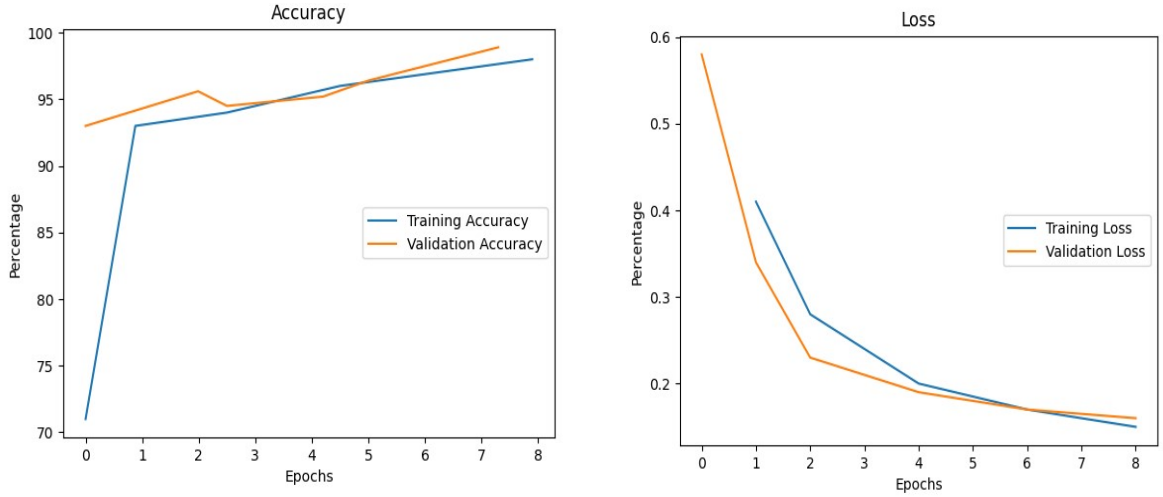
$$L(y, \hat{y}) = -[y.\log(\hat{y}) + (1 - y).\log(1 - \hat{y})] \quad (3)$$

where y is the true class label, and $\hat{y}$ predicted probability of belonging to class 1. For binary cross-entropy loss, If $y = 1$, the loss is $-\log(\hat{y})$. This term penalizes the model more if the predicted probability $(\hat{y})$ for class 1 is low but If $y = 0$, the loss is $-\log(1 - \hat{y})$. This term penalizes the model more if the predicted probability for class 1 is high when it should be low.

The dataset is splitted into training and testing sets at 80% to 20% respectively. The input features were normalized using StandardScaler and the accuracy of the model is evaluated using confusion matrices. The neural network model is built using the build model function with He initialization for the first layers with ReLU activation and Glorot (Xavier) initialization for the hidden layers with tanh and the output layer with sigmoid activation. The epochs for the dataset were set to ten for testing purposes after fine-tuning the hyper parameters.

4. Results and Discussion

In the context of neural networks, the cross-entropy loss is often used in binary or multiclass classification tasks. In this research work, the dataset is generated for binary two classes cross entropy. The model's validation and training accuracies for binary cross entropy evaluation are shown in Figure 7 with an acceptable low loss observed for the training and validation.



(a) The model's training and validation accuracy (b) The model's training and validation loss

Fig. 7. The model's training accuracy, validation accuracy, and loss for two classes (binary) evaluations

A decrease in loss is observed for the training and validation evaluation due to kernel minimization. The operation datasets patterns obtained for the ransomware were converted to binary output using a python code that choses a binary output one for operations caused by the PE file of the ransomware and binary zero for operations caused otherwise. It is observed that the accuracy of the testing process and the generated loss for pattern datasets is steady for higher number of epochs as shown in Figure 8. Furthermore, fine-tuning the hyper parameter values enriches the performance of detecting algorithm. Using feature based on frequency of the system and the temporal pattern of the operations produce a distinct pattern for each ransomware which is learn by separable convolution layers to obtain distinct texture-like characteristics to separate benign and ransomware pattern with just a few training repetitions. Therefore, the algorithm is highly effective in detecting ransomware attacks.

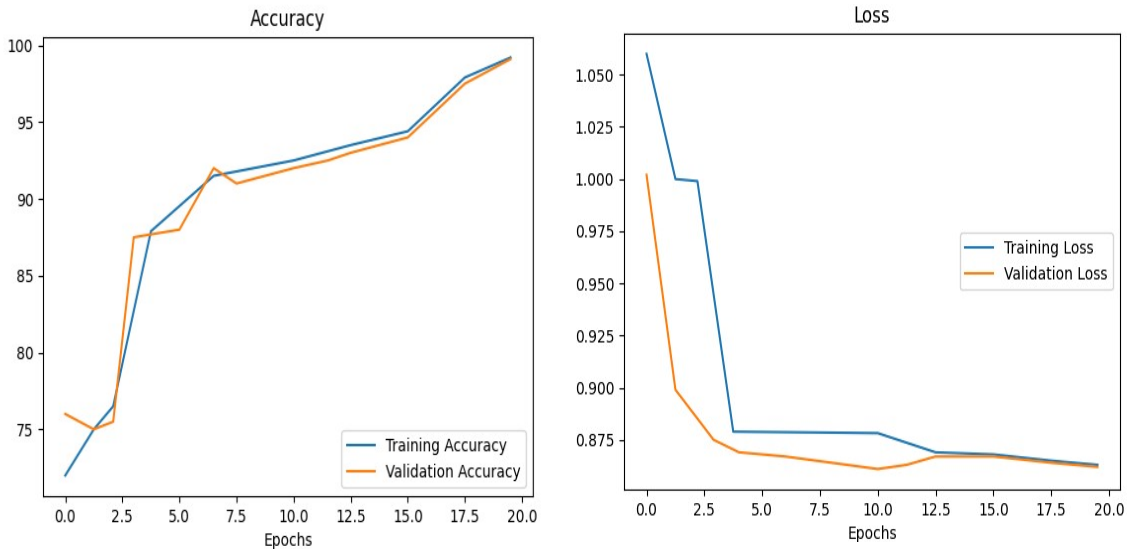


Fig. 8. The model's training and validation accuracy, and losses for higher number of epochs

The hyperparameters settings varies from one deep learning algorithms to another to obtain the best configuration. The best configurations are achieved based on fine-tuning the parameters. The final configuration and optimizing variables used to suggest the best for the temporal pattern models are configured as: the lowest size of batch quantity is 15, the dropout rate is 0.5, learning rate schedule variables is set to "piecewise" learning rate at 0.0001, and Adam optimizer is selected for the training as it generally performs well across various tasks. The highest epoch's numbers set is set to twenty. Using the binary cross entropy and the temporal pattern extracted features for the trained model, the training accuracy and loss performance compared with other models of algorithms are shown in Table 3.

Table 3
Comparison of RGB and grayscale dataset in binary classification on various models

Models	Accuracy (%)	Loss (%)
Proposed Approach	99.2	0.8
CNN Algorithm	97.1	2.9
KNN	97.7	2.3
SVM	96.9	3.1

However, the metrics of the training and evaluations are monitored using the precision, recall, and F1-score for a more comprehensive evaluation as shown in Table 4 which demonstrated the effectiveness of the temporal pattern extracted dataset on deep learning algorithms.

Table 4
Performance evaluation of the proposed model on temporal pattern dataset

Accuracy (%)	Error Rate (%)	Precision (%)	Recall (%)	F-1 Score (%)
99.2	0.8	90	99	98

5. Conclusion

This research proposed a dataset obtained through temporal pattern and frequency of system calls extraction from ransomware-initiated processes to train a deep learning ransomware detector

model using an enhanced artificial neural network. The proposed enhance ANN (EANN) model used different weight initialization methods applied based on the activation functions of the layers (i.e He with ReLU activation for the first hidden layer, tanh activation for the second hidden layer and sigmoid activation with the output layer). This produces more stable training, reduces vanishing/exploding gradients for faster convergence and better performance. The proposed approach achieved an accuracy of 99.2% and error rate of 0.8%. It performed better than other models evaluated on the same datasets. The extracted features obtained demonstrate the true nature of ransomwares when active IoMT devices. This gives the proposed algorithm a better performance when compared with other models of different algorithms.

The possibilities of the proposed ransomware detector to recognize or detect newly released ransomwares is very high because the extracted features used in training the model are based on patterns and frequencies of occurrence of different processes which are not tagged to images unlike other approaches that are proposed by other approaches. The enhanced artificial neural network (EANN) provides a more stable training process with faster convergence. The enhanced weight initialization is more tailored to the characteristics of the neural network architecture, leading to improved training performance. The Adam optimizer used in the proposed EANN can be changed with heuristic optimization methods such as differential evolution, particle swamp optimization and Grasshopper optimization which may improve the performance of the trained model.

Acknowledgement
This research was funded by the Ministry of Higher Education (MOHE) of Malaysia under the Fundamental Research Grant Scheme (FRGS/1/2022/ICT07/USIM/02/1).

References

[1] Pigola, Angélica, Priscila Rezende Da Costa, Marcos Ferasso, and Luís Fabio Cavalcanti da Silva. "Enhancing cybersecurity capability investments: Evidence from an experiment." *Technology in Society* 76 (2024): 102449. https://doi.org/10.1016/j.techsoc.2023.102449

[2] Aidan, Jagmeet Singh, and Urvashi Garg. "Advanced Petya ransomware and mitigation strategies." In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 23-28. IEEE, 2018. https://doi.org/10.1109/ICSCCC.2018.8703323

[3] Comito, Carmela, Agostino Forestiero, and Clara Pizzuti. "Word embedding based clustering to detect topics in social media." In *IEEE/WIC/ACM International Conference on Web Intelligence*, pp. 192-199. 2019. https://doi.org/10.1145/3350546.3352518

[4] Ilker, K. A. R. A., and Murat Aydos. "Cyber fraud: Detection and analysis of the crypto-ransomware." In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0764-0769. IEEE, 2020.

[5] Weckstén, Mattias, Jan Frick, Andreas Sjöström, and Eric Järpe. "A novel method for recovery from Crypto Ransomware infections." In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1354-1358. IEEE, 2016. https://doi.org/10.1109/CompComm.2016.7924925

[6] Mimura, Yuiko, Toshio Tsuchiya, Kaho Moriyama, Kanna Murata, and Sana Takasuka. "UX design for mobile application of E-Commerce site by using Kansei interface." In *Advances in Industrial Design: Proceedings of the AHFE 2020 Virtual Conferences on Design for Inclusion, Affective and Pleasurable Design, Interdisciplinary Practice in Industrial Design, Kansei Engineering, and Human Factors for Apparel and Textile Engineering, July 16–20, 2020, USA*, pp. 641-647. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-51194-4_84

[7] Alotaibi, Fahad M., and Vassilios G. Vassilakis. "Sdn-based detection of self-propagating ransomware: the case of badrabbit." *Ieee Access* 9 (2021): 28039-28058. https://doi.org/10.1109/ACCESS.2021.3058897

[8] Aiswarya, E. S., Adheena Maria Benny, and Leena Vishnu Namboothiri. "CLOP Ransomware Analysis Using Machine Learning Approach." In *Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021*, pp. 593-600. Springer Singapore, 2022. https://doi.org/10.1007/978-981-16-3728-5_45

[9] Kyurkchiev, Nikolay. "Selected Topics in Mathematical Modeling: Some New Trends." *Dedicated to Academician Blagovest Sendov (1932-2020), LAP Lambert Academic Publishing* (2020).

[10] Beşiktaş, Cihangir, Didem Gözüpek, Aydın Ulaş, and Erhan Lokman. "Secure virtual network embedding with flexible bandwidth-based revenue maximization." *Computer Networks* 121 (2017): 89-99. https://doi.org/10.1016/j.comnet.2017.04.020

[11] Kara, Ilker, and Murat Aydos. "Static and dynamic analysis of third generation cerber ransomware." In *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, pp. 12-17. IEEE, 2018. https://doi.org/10.1109/IBIGDELFT.2018.8625353

[12] Almashhadani, Ahmad O., Mustafa Kaiiali, Sakir Sezer, and Philip O'Kane. "A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware." *IEEE access* 7 (2019): 47053-47067. https://doi.org/10.1109/ACCESS.2019.2907485

[13] Trautman, Lawrence J., and Peter C. Ormerod. "Wannacry, ransomware, and the emerging threat to corporations." *Tenn. L. Rev.* 86 (2018): 503. https://doi.org/10.2139/ssrn.3238293

[14] Chen, You-Shyang, Jerome Chih-Lung Chou, Yu-Sheng Lin, Ying-Hsun Hung, and Xuan-Han Chen. "Identification of SMEs in the Critical Factors of an IS Backup System Using a Three-Stage Advanced Hybrid MDM–AHP Model." *Sustainability* 15, no. 4 (2023): 3516. https://doi.org/10.3390/su15043516

[15] Aidan, Jagmeet Singh, and Urvashi Garg. "Advanced Petya ransomware and mitigation strategies." In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 23-28. IEEE, 2018. https://doi.org/10.1109/ICSCCC.2018.8703323

[16] Raulin, Vincent, Pierre-François Gimenez, Yufei Han, and Valérie Viet Triem Tong. "BAGUETTE: Hunting for Evidence of Malicious Behavior in Dynamic Analysis Reports." In *20th International conference on security and cryptography SECRYPT 2023*. 2023. https://doi.org/10.5220/0012086400003555

[17] Nicho, Mathew, Rajesh Yadav, and Digvijay Singh. "Analyzing WhisperGate and BlackCat Malware: Methodology and Threat Perspective." *International Journal of Advanced Computer Science and Applications* 14, no. 4 (2023). https://doi.org/10.14569/IJACSA.2023.0140456

[18] Sarowa, Sandeep, Bhisham Bhanot, Vijay Kumar, and Munish Kumar. "Analysis of Attack Patterns and Cyber Threats in Healthcare Sector." In *2023 International Conference on Device Intelligence, Computing and Communication Technologies,(DICCT)*, pp. 160-165. IEEE, 2023. https://doi.org/10.1109/DICCT56244.2023.10110141

[19] Al-Rimy, Bander Ali Saleh, Mohd Aizaini Maarof, Mamoun Alazab, Syed Zainudeen Mohd Shaid, Fuad A. Ghaleb, Abdulmohsen Almalawi, Abdullah Marish Ali, and Tawfik Al-Hadhrami. "Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection." *Future Generation Computer Systems* 115 (2021): 641-658. https://doi.org/10.1016/j.future.2020.10.002

[20] Hireche, Rachida, Houssem Mansouri, and Al-Sakib Khan Pathan. "Security and privacy management in Internet of Medical Things (IoMT): a synthesis." *Journal of Cybersecurity and Privacy* 2, no. 3 (2022): 640-661. https://doi.org/10.3390/jcp2030033

[21] Paul, Metty, Leandros Maglaras, Mohamed Amine Ferrag, and Iman Almomani. "Digitization of healthcare sector: A study on privacy and security concerns." *ICT Express* 9, no. 4 (2023): 571-588. https://doi.org/10.1016/j.icte.2023.02.007

[22] Strielkowski, Wadim, Tatiana Kulagovskaya, Galina Panaedova, Luboš Smutka, Stanislava Kontsevaya, and Dalia Štreimikienė. "Post-soviet economics in the context of international trade: opportunities and threats from mutual cooperation." *Economic research-Ekonomska istraživanja* 36, no. 1 (2023): 2021-2044. https://doi.org/10.1080/1331677X.2022.2094444

[23] Tomaiko, Emrie, and Michael S. Zawaneh. "Cybersecurity threats to cardiac implantable devices: room for improvement." *Current Opinion in Cardiology* 36, no. 1 (2021): 1-4. https://doi.org/10.1097/HCO.0000000000000815

[24] Huang, Daniel Q., Hashem B. El-Serag, and Rohit Loomba. "Global epidemiology of NAFLD-related HCC: trends, predictions, risk factors and prevention." *Nature reviews Gastroenterology & hepatology* 18, no. 4 (2021): 223-238. https://doi.org/10.1038/s41575-020-00381-6

[25] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and security: Challenges and solutions." *Applied Sciences* 10, no. 12 (2020): 4102. https://doi.org/10.3390/app10124102

[26] Mushtaq, Mudassar, Munam Ali Shah, and Azhar Ghafoor. "The internet of medical things (iomt): Security threats and issues affecting digital economy." (2021): 137-142. https://doi.org/10.1049/icp.2021.2420

[27] Smith, Leigh, Sara M. Karaba, Joe Amoah, George Jones, Robin K. Avery, Kathryn Dzintars, Taylor Helsel, Sara E. Cosgrove, and Valeria Fabre. "Hospital-acquired infections among adult patients admitted for coronavirus disease 2019 (COVID-19)." *Infection Control & Hospital Epidemiology* 43, no. 8 (2022): 1054-1057. https://doi.org/10.1017/ice.2021.148

[28] Brown, Lori, J. Shoshanna Ehrlich, and Nicole M. Guidotti-Hernández. "No Refuge (es) Here: Jane Doe and the Contested Right to 'Abortion on Demand'." *Feminist Legal Studies* 32, no. 1 (2024): 27-49. https://doi.org/10.1007/s10691-022-09502-9

[29] Gupta, Akash, Shazia Mumtaz, Cheng-Hsuan Li, Irshad Hussain, and Vincent M. Rotello. "Combatting antibiotic-resistant bacteria using nanomaterials." *Chemical Society Reviews* 48, no. 2 (2019): 415-427. https://doi.org/10.1039/C7CS00748E

[30] Lee, Seungjin, Azween Abdullah, Nz Jhanjhi, and Sh Kok. "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning." *PeerJ Computer Science* 7 (2021): e350. https://doi.org/10.7717/peerj-cs.350

[31] Armstrong, Stuart, Kaj Sotala, and Seán S. Ó hÉigeartaigh. "The errors, insights and lessons of famous AI predictions–and what they mean for the future." *Journal of Experimental & Theoretical Artificial Intelligence* 26, no. 3 (2014): 317-342. https://doi.org/10.1080/0952813X.2014.895105

[32] Roberts, Lara N., Martin B. Whyte, Loizos Georgiou, Gerard Giron, Julia Czuprynska, Catherine Rea, Bipin Vadher, Raj K. Patel, Emma Gee, and Roopen Arya. "Postdischarge venous thromboembolism following hospital admission with COVID-19." *Blood, The Journal of the American Society of Hematology* 136, no. 11 (2020): 1347-1350. https://doi.org/10.1182/blood.2020008086

[33] Wang, Chengdi, Zhoufeng Wang, Guangyu Wang, Johnson Yiu-Nam Lau, Kang Zhang, and Weimin Li. "COVID-19 in early 2021: current status and looking forward." *Signal Transduction and Targeted Therapy* 6, no. 1 (2021): 1-14. https://doi.org/10.1038/s41392-021-00527-1

[34] Miller, Kimberly D., Leticia Nogueira, Angela B. Mariotto, Julia H. Rowland, K. Robin Yabroff, Catherine M. Alfano, Ahmedin Jemal, Joan L. Kramer, and Rebecca L. Siegel. "Cancer treatment and survivorship statistics, 2019." *CA: a cancer journal for clinicians* 69, no. 5 (2019): 363-385. https://doi.org/10.3322/caac.21565

[35] Clark, John Bates. *Essentials of economic theory: as applied to modern problems of industry and public policy*. Good Press, 2019.

[36] Madani, Houria, Noura Ouerdi, Ahmed Boumesaoud, and Abdelmalek Azizi. "Study on the different types of neural networks to improve the classification of ransomwares." In *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020) 12*, pp. 790-798. Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-73689-7_75

[37] Agrawal, Rakshit, Jack W. Stokes, Karthik Selvaraj, and Mady Marinescu. "Attention in recurrent neural networks for ransomware detection." In *ICASSP 2019-2019 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, pp. 3222-3226. IEEE, 2019. https://doi.org/10.1109/ICASSP.2019.8682899

[38] Ashfaq, Zarlish, Abdur Rafay, Rafia Mumtaz, Syed Mohammad Hassan Zaidi, Hadia Saleem, Syed Ali Raza Zaidi, Sadaf Mumtaz, and Ayesha Haque. "A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem." *Ain Shams Engineering Journal* 13, no. 4 (2022): 101660. https://doi.org/10.1016/j.asej.2021.101660

[39] Hasan, Mohammad Kamrul, Taher M. Ghazal, Rashid A. Saeed, Bishwajeet Pandey, Hardik Gohel, Ala'A. Eshmawi, Sayed Abdel-Khalek, and Hula Mahmoud Alkhassawneh. "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things." *IET communications* 16, no. 5 (2022): 421-432. https://doi.org/10.1049/cmu2.12301

[40] Palla, Tarun Ganesh, and Shahab Tayeb. "Intelligent Mirai malware detection for IoT nodes." *Electronics* 10, no. 11 (2021): 1241. https://doi.org/10.3390/electronics10111241

[41] Perwej, Yusuf, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, and Anurag Kumar Jaiswal. "A systematic literature review on the cyber security." *International Journal of scientific research and management* 9, no. 12 (2021): 669-710. https://doi.org/10.18535/ijsrm/v9i12.ec04

[42] Moussaileb, Routa, Nora Cuppens, Jean-Louis Lanet, and Hélène Le Bouder. "A survey on windows-based ransomware taxonomy and detection mechanisms." *ACM Computing Surveys (CSUR)* 54, no. 6 (2021): 1-36. https://doi.org/10.1145/3453153

[43] Sikorski, Michael, and Andrew Honig. *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press, 2012.

[44] Tailor, Jinal P., and Ashish D. Patel. "A comprehensive survey: ransomware attacks prevention, monitoring and damage control." *Int. J. Res. Sci. Innov* 4, no. 15 (2017): 116-121.

[45] Savenko, Oleg, Andrii Nicheporuk, Ivan Hurman, and Sergii Lysenko. "Dynamic Signature-based Malware Detection Technique Based on API Call Tracing." In *ICTERI workshops*, pp. 633-643. 2019.

[46] Urooj, Umara, Mohd Aizaini Bin Maarof, and Bander Ali Saleh Al-rimy. "A proposed adaptive pre-encryption crypto-ransomware early detection model." In *2021 3rd International Cyber Resilience Conference (CRC)*, pp. 1-6. IEEE, 2021. https://doi.org/10.1109/CRC50527.2021.9392548

[47] Gioulekas, Fotios, Evangelos Stamatiadis, Athanasios Tzikas, Konstantinos Gounaris, Anna Georgiadou, Ariadni Michalitsi-Psarrou, Georgios Doukas *et al.,* "A cybersecurity culture survey targeting healthcare critical infrastructures." In *Healthcare*, vol. 10, no. 2, p. 327. MDPI, 2022. https://doi.org/10.3390/healthcare10020327

[48] Soni, Preeti, Jitesh Pradhan, Arup Kumar Pal, and SK Hafizul Islam. "Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system." *IEEE Transactions on Industrial Informatics* 19, no. 1 (2022): 830-840. https://doi.org/10.1109/TII.2022.3179429

[49] Turk, Žiga, Borja García de Soto, Bharadwaj RK Mantha, Abel Maciel, and Alexandru Georgescu. "A systemic framework for addressing cybersecurity in construction." *Automation in Construction* 133 (2022): 103988. https://doi.org/10.1016/j.autcon.2021.103988

[50] Liaqat, Shahzana, Adnan Akhunzada, Fatema Sabeen Shaikh, Athanasios Giannetsos, and Mian Ahmad Jan. "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)." *Computer Communications* 160 (2020): 697-705. https://doi.org/10.1016/j.comcom.2020.07.006

[51] Karmakar, Kallol Krishna, Vijay Varadharajan, Uday Tupakula, Surya Nepal, and Chandra Thapa. "Towards a security enhanced virtualised network infrastructure for internet of medical things (IoMT)." In *2020 6th IEEE conference on network softwarization (NetSoft)*, pp. 257-261. IEEE, 2020. https://doi.org/10.1109/NetSoft48620.2020.9165387

[52] Yaacoub, Jean-Paul A., Mohamad Noura, Hassan N. Noura, Ola Salman, Elias Yaacoub, Raphaël Couturier, and Ali Chehab. "Securing internet of medical things systems: Limitations, issues and recommendations." *Future Generation Computer Systems* 105 (2020): 581-606. https://doi.org/10.1016/j.future.2019.12.028

[53] Papaioannou, Maria, Marina Karageorgou, Georgios Mantas, Victor Sucasas, Ismael Essop, Jonathan Rodriguez, and Dimitrios Lymberopoulos. "A survey on security threats and countermeasures in internet of medical things (IoMT)." *Transactions on Emerging Telecommunications Technologies* 33, no. 6 (2022): e4049. https://doi.org/10.1002/ett.4049

[54] Hussien, Hassan Mansur, Sharifah Md Yasin, Nur Izura Udzir, Mohd Izuan Hafez Ninggal, and Sadeq Salman. "Blockchain technology in the healthcare industry: Trends and opportunities." *Journal of Industrial Information Integration* 22 (2021): 100217. https://doi.org/10.1016/j.jii.2021.100217

[55] Kim, Meejoung, Eenjun Hwang, and Jeong-Nyeo Kim. "Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas." *Wireless Networks* 23 (2017): 355-369. https://doi.org/10.1007/s11276-015-1160-4

[56] Nassar, Amin H., Elio Adib, and David J. Kwiatkowski. "Distribution of KRAS G12C somatic mutations across race, sex, and cancer type." *New England Journal of Medicine* 384, no. 2 (2021): 185-187. https://doi.org/10.1056/NEJMc2030638

[57] Lelli, Diana, Stefano Tolone, Giovanni Pulignano, Maria Denitza Tinti, Donatella Del Sindaco, Giulia Dipasquale Mazzilli, Raffaele Antonelli Incalzi, and Claudio Pedone. "Nutritional status is associated with physical function and disability in older adults with chronic heart failure." *European Journal of Internal Medicine* 74 (2020): 73-78. https://doi.org/10.1016/j.ejim.2019.12.007

[58] Lopez-Rojas, Jeffrey, Christopher A. de Solis, Felix Leroy, Eric R. Kandel, and Steven A. Siegelbaum. "A direct lateral entorhinal cortex to hippocampal CA2 circuit conveys social information required for social memory." *BioRxiv* (2021): 2021-04. https://doi.org/10.1101/2021.04.15.440048

[59] Hussien, Hassan Mansur, Sharifah Md Yasin, Nur Izura Udzir, Mohd Izuan Hafez Ninggal, and Sadeq Salman. "Blockchain technology in the healthcare industry: Trends and opportunities." *Journal of Industrial Information Integration* 22 (2021): 100217. https://doi.org/10.1016/j.jii.2021.100217