Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/121135

Cryptovirology Ransomware: A Review of Dissemination and Mitigation Techniques

Muhammad Imran Sarwar [1,*], *Louai A. Maghrabi* [2], *Kashif Nisar* [1] *and Imran Khan* [3]

[1]Department of Computer Science & IT, The Superior University, Lahore, Lahore-54500, Pakistan
[2]Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia
[3]School of Computer Science and Informatics, Cardiff University, Cardiff CF10 3AT, United Kingdom

Received: 2 Sep. 2023, Revised: 22 Oct. 2023, Accepted: 26 Oct. 2023
Published online: 1 Nov. 2023

Abstract: Digital assets are generally regarded as one of the most valuable assets for an organization. When they are captured for ransom purposes, a serious problem arises, and ransomware is responsible for this. When ransomware gets onto a computer or other electronic device, the data on it is encrypted, made inaccessible, or taken away until a ransom is paid. The culprits behind these activities release and disseminate new and sophisticated variants of illicit wealth and notorious practices. Hardware and antivirus software that detect intrusions are not a permanent solution, as hackers can bypass them easily. After ransomware has been executed on an electronic device, it is extremely difficult or nearly impossible to recover the data, and now is the time to draw attention to this threat. In this study, various aspects of ransomware's propagation, encryption, and mitigation techniques are discussed. We have also used the RanSim simulator to detect malware in a system, and details of the experiment are presented in the later sections. The methodology used for this study can be classified as exploratory research to explore the recent literature on the topic. This study contributes by highlighting recent trends in ransomware, their consequences, and prevention and mitigation techniques.

Keywords: RanSim, Ransomware, Ransomware Threats and Mitigation, System Implications of Ransomware, Trusted Computing.

1 Introduction

Cryptovirology software, known as ransomware, aims to either disclose the victim's private information or permanently lock access to the files unless a ransom is paid. Advanced-version malware uses a method termed cryptoviral extortion, whereas simple ransomware may lock the system without deleting any files [1]. The files are encrypted, rendering them inaccessible, and a ransom demand is made in order to unlock them. They are often designed to spread over a network, target the file servers and databases, and halt the entire process. It is a growing threat that results in billions of dollars of losses while significantly harming businesses and government institutions [2]. Hundreds of thousands of pieces of ransomware have been developed, and this number is increasing, for the sole purpose of carrying out criminal and illegal activities [3]. These programs are malware that supports the development of illicit activities. Criminals use malware to control computers and steal personal data and confidential information. As the use of malware to commit crimes has increased, digital forensic investigators are being forced to conduct malware analyses using tools only available from antivirus manufacturers and safety research organizations [4]. Since 2005, the ransomware mafia has grown into a very powerful cyber giant, and since 2012, there has been a huge increase in attacks. By 2013, with the growth of the Internet of Things (IoT), these attacks had spread into every aspect of life, including home and building automation [5]. Now, in 2023, a new model is emerging that works on top of SaaS (Software as a Service) called RaaS (Ransomware as a Service) [6], and we are expecting an increase in the number and cost of ransomware attacks in future years. It highlights the importance of raising awareness among researchers about the severity of this issue.

The evolution of ransomware is a few decades old. The world first heard of ransomware in 1980, when payments were being sent via snail mail [7]. Now, it has become the most notorious kind of virus, causing financial damage to everyone, from individuals to large corporations and the public sector [8]. The amount of loss is increasing year after year, and

* Corresponding author e-mail: info@imranchishty.com

as a result, special consideration is being given to protecting the data from ransomware. Ransomware creators demand ransoms in cryptocurrency [9], usually Bitcoin, due to its anonymity. Figure 1 shows the evolution of ransomware.

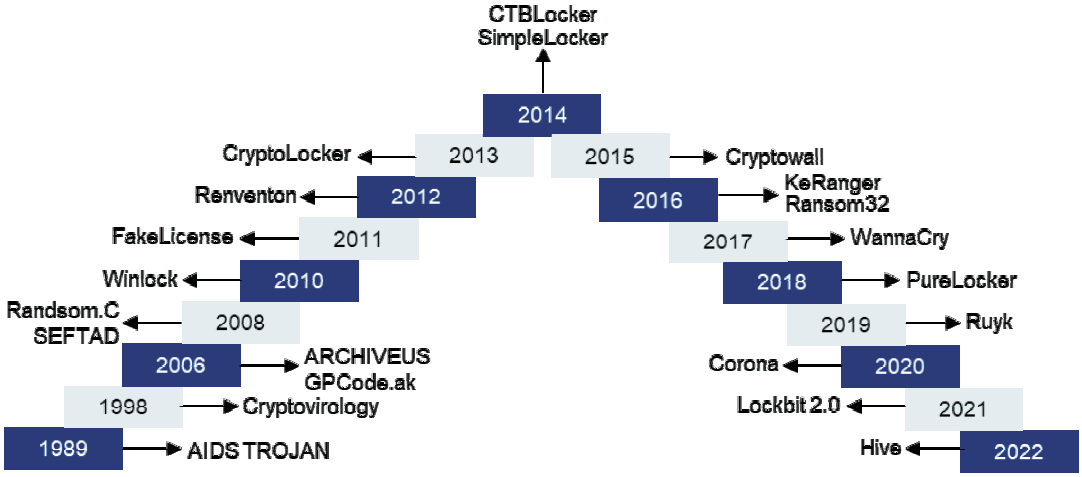

Figure 1: Ransomware evolution between 1989 and 2022 [10]

Ransomware attacks have become a challenge for people, businesses, and public sector [11]. These attacks can result in billions of dollars of losses and render data unusable or seized for ransom. Ransomware began its attacks using Locker Ransomware. This type of ransomware locks all files on the victim's computer, and prevents them from being able to access them without the ransom being paid. However, over time, its functionality has changed, and it has changed into the most dangerous and vicious crypto-ransomware which encrypts all files in the system with a strong encryption technique such as Advanced Encryption Standards (AES), which is nearly impossible to break or decrypt [12]. Ransomware is mainly divided into two types according to their functionality: 1) Crypto and 2) Locker, as shown in Figure 2.

Figure 2: Types of ransomware

1.1 Crypto-Ransomware

Ransomware uses encryption techniques to encrypt the victims' data. Ransomware primarily uses two different types of encryption, namely selective encryption and indiscriminate encryption [13]. Indiscriminate encryption is a technique that allows the attacker to delete the original files and replace them with the encrypted files. TorrentLocker is an example of this kind of crypto-ransomware. The attackers use an application programming interface (API) for this purpose, known as Windows secure deletion. In selective encryption, selected files are deleted from the system instead of encrypting all files, and sometimes attackers modify the master boot record (MBR). The CryptoWall family belongs to the crypto-type variant.

1.2 Locker-Ransomware

This type of ransomware infects the system without encrypting the data. Locker ransomware locks the system files and other resources such as the mouse and keyboard. Locker ransomware is also used to lock, modify, or encrypt the MBR of the Windows OS. Flocker is an example of Locker ransomware [14]. It is available in approximately 7000 variants with developers continually adding new variants. Flocker typically targets Android devices such as smartphones and televisions. Locker-type ransomware targets devices in a specific geographic location. If it finds the device in the targeted location, it activates itself; otherwise, it becomes deactivated automatically. Flocker works very intelligently. It requests admin privileges from the device, and if they are not granted, it immediately freezes the screen and contacts the Command and Control (C&C) server, which delivers an apk file with the filename misspelled.apk. The C&C server collects information, typically including contacts, phone numbers, and location, and encrypts it with an AES key that is essentially impossible to crack or decrypt.

1.3 Dissemination and Mitigation Techniques

According to [15], paying a ransom is not a guarantee of data recovery. It also motivates criminals to target more victims and provides an incentive for others to engage in illicit behavior. Ransomware or crypto-ransomware can use different encryption models, such as symmetric, asymmetric, and hybrid encryption, to encrypt and disseminate the data and also increase the difficulty level of decryption [15]. This variant of ransomware is more lethal than the traditional variants. The attackers typically demand a ransom in Bitcoin in order to remain anonymous during the payment process. If a victim pays the ransom, the hacker will lead them to data decryption; subject to the honesty of the attacker. Figure 3 illustrates how the ransomware attack is made, how the files and data are encrypted, how attackers demand the ransom for decryption keys, and what happens after the ransom is paid [16].

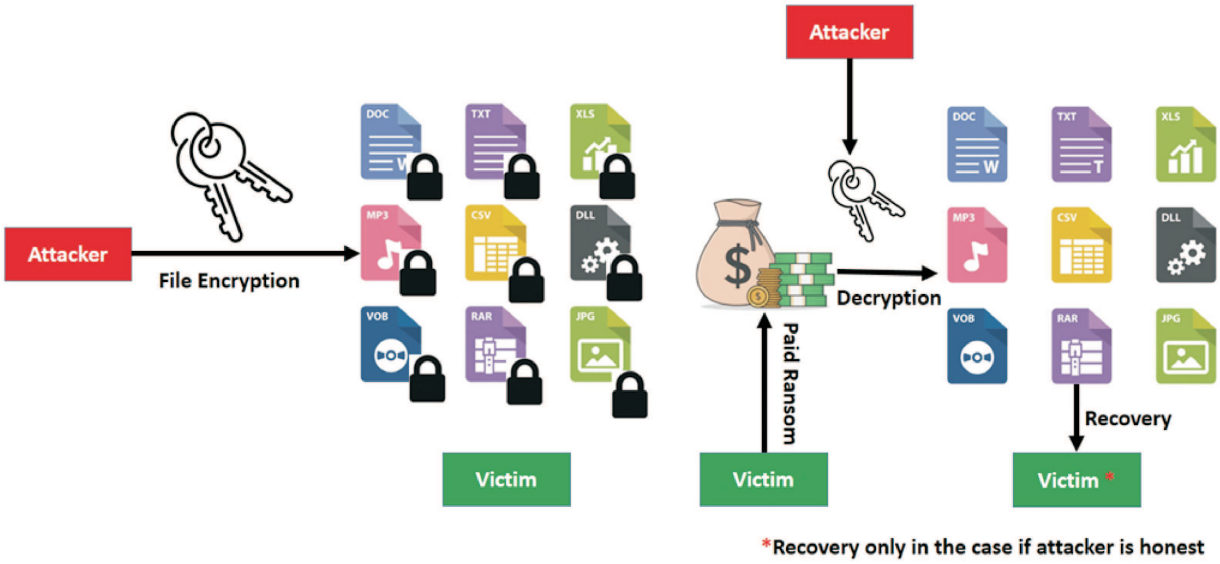

Figure 3: Basics of a ransomware attack

Offering a free version of the software is another typical approach to ransomware infection, and it can include cracked games or software, free games, or fake apps promoted as a way to cheat in online games or bypass a website's barriers. Hackers can get past any firewall or email filter by preying on the user in this way [14]. An example of a ransomware assault that took advantage of the popularity of the game Minecraft by offering a mod to gamers. When the user installs software on his device, the malware also installs in the background and executes according to the instructions or through the C&C server. Hackers take advantage of communication network flaws as the point of initialization through the communication channel to the data or resources being accessed, and the vulnerabilities are

visible. Remote desktop protocol (RDP) sessions enable users to log in and control Windows machines remotely. Many companies enable Internet traffic via a firewall, allowing users to use their computers remotely, and RDP uses the 3389 port, which is specific for communication [9]. Hackers are more able to target these vulnerable systems and use them to spread malware over a network. When weak passwords are used or account lockout protections are also not activated, RDP is abused as a result of an unpatched vulnerability or a weak password [14].

Drive-by downloads happen when a computer is infected by using an old browser or software plug-in or by downloading an app that is not appropriate for it from a third party [7]. Hackers always try to find defects in the software that can help them with malicious code execution. Most of the time, software makers find vulnerabilities quickly and fix them quickly, but software users are always vulnerable to them for a period of time. The Exploit Kit (EK) is used to analyze the affected website for known vulnerabilities.

The most common way for ransomware to spread is through email attachments that look like suspicious files. Attackers send a file with different extensions to mask the precise file type that they deliver. If a phishing email is sent with an attachment or with a downloadable link and the recipient does not check the validity of the attachment or link, they are likely to be infected with ransomware. This is the most common way to infect a user's computer with ransomware [17]. The Spam Intelligence Database of the Australian Communications and Media Authority gave a ten per cent data sample of 25.76 million spam emails for scanning, and it was discovered that roughly one out of every ten emails had been infected with malware [10].

The WannaCry ransomware has a two-part mechanism [18]. Firstly, it is available on network devices such as an iPn in a worm-like manner and gathers lists of local and global IP addresses. It then exploits the MS17-010 vulnerability in Microsoft's OS at port 445 and infects any unpatched computers. Secondly, it has embedded RSA keys for encryption and takes the necessary steps to decrypt the malicious DLL files that represent a component for encrypting data. The author also discovered that WannaCry communicates with a C&C server and uses embedded onion addresses to download the Tor browser through a secure channel on port 443 and the standard Tor ports 900 and 9050. The results of this survey can help us come up with a good plan to stop WannaCry and other families that behave similarly. In another research work, the authors discussed the propagation techniques of ransomware including WannaCry, Petya, and CrySis/Dharma over the network [19].

The experiments were carried out in a virtual environment for safety reasons. The WannaCry ransomware's functionality on the network was examined using two samples [20]. The first sample contained the ransomware's raw payload, and the other was an adaptation of the first sample with added network functionality and propagation behavior [21]. The second sample was allowed to run in the prepared virtual machine (VM) and was given access to the virtual network within VMware. The incoming and outgoing network activities were monitored closely with Wireshark. The findings showed that when the WannaCry sample is run, it tries to scan the entire local network and other hosts to infect them [22]. Once a remote host is discovered on the network, evidence suggests that the WannaCry sample attempts to infect the host by exploiting an EternalBlue vulnerability in the Windows Super Mystère B.2 (SMB2) protocol, allowing it to spread to other hosts on the network [23].

In order to make a comparison, the network activity of Petya was examined. The results reveal that Petya exhibits similar behavior, but upon finding a host to infect, it begins to exchange substantial TCP and SMB2 traffic with the identified vulnerable host to propagate Petya's payload from one system to the next [24]. To ensure that no additional hosts are infected, the secondary infected host continues to search the network until the system shutdowns or restarts, and during this activity, a fake CHKDSK process appears and, it overwrites the master file table (MFT) in background [25].

Wireshark analysis of incoming and outgoing network traffic for CrySiS/Dharma [26] did not reveal any clear patterns. However, Immunity Debugger [27] static analysis showed many references to WebDav in the form of davcLnt and other names. This indicates that the sample may want to infect not only the whole network but also other servers on the network. Possibly, it could also mean that it intended to get more files from the network. However, the activity on the network was found because CrySiS was able to encrypt the contents of a mapped network location. This shows that it can get into other systems on the network without necessarily infecting them. Ransomware can cause a serious threat to the entire organization, and multiple studies have focused on various mitigation techniques [28].

A plan called the HoneyFiles Structure (HFS) is described as a way to catch ransomware once it starts encrypting files [29]. HFS is deployed throughout the target environment to capture the ransomware. HFS uses FIFO-style files, which means that once the ransomware begins reading the file, it is blocked. In addition, the authors claim that HFS is capable of automatically launching anti-infection countermeasures. Furthermore, because it does not require any prior training or knowledge, the approach can be used to combat zero-day ransomware attacks [30]. The approach was created for Unix platforms and used the R-Locker tool on the Linux platform. It was tested by running various ransomware samples in a controlled environment. R-Locker captured the ransomware sample and blocked it to prevent it from spreading further, as well as meeting operations requirements from R1 to R5, i.e., efficiency, low resource consumption, plainness, and transparency [31]. When compared to other detection tools, R-Locker demonstrates the best performance, and the author claims in conclusion that this method can also be very useful in a real environment. The authors also discussed the workings of the same methodology for Windows and Android OS, and this will form part of future work [32].

Jigsaw is ransomware that was first discovered in late 2016 [33][34]. The original name of the program was BitcoinBlackmailer, but it was renamed Jigsaw when the encrypted image appeared [35]. Attackers propagate it using spam emails, and that is the most common infection vector because they trick the recipient into installing harmful software. Infected files are encrypted, and a 150 USD Bitcoin payment is demanded. It also gradually deletes encrypted files until the victim makes a ransom payment [36].

Over time, ransomware is getting more dangerous, and companies and security organizations are working constantly to reduce or minimize its effects. Some tools and antiviruses such as RanSim [37], Kaspersky, and McAfee can help against ransomware. The No More Ransom website is a joint effort to combat ransomware by the Dutch National High-Tech Crime Unit and Europol's European Cybercrime Centre [38]. In recent years, a hybrid blend of symmetric and asymmetric encryption techniques has been used in ransomware. It is really a time-consuming and hectic activity to reverse the ransomware encryption and also requires intensive resources. However, reverse engineering and crypto-analysis can significantly help mitigate a ransomware attack after it has been executed [39].

1.4 Trusted Computing (TC)

TC refers to the concept of designing computer systems that can be trusted to behave as expected, even in the face of various threats and attacks. It can include protecting against malware, unauthorized access, data breaches, and other types of cyber threats. One approach to achieving trusted computing is through the use of hardware-based security features, such as Trusted Platform Modules (TPMs) and secure enclaves. The trusted platform module (TPM) technology protects computers from malware and sophisticated cyberattacks at the hardware level [40]. These features provide a secure, isolated environment for running a sensitive code and storing cryptographic keys and other sensitive data. TC can also involve the use of secure boot processes, digital signatures, and other measures to ensure that software and firmware running on a system are legitimate and have not been tampered with. Figure 4 shows a model of TC.

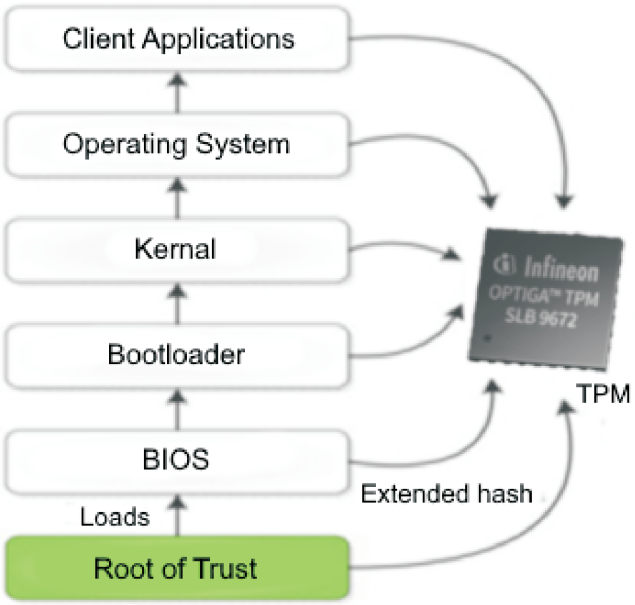

Figure 4: A conceptual view of trusted computing

Mainstream hardware vendors have formed a non-profit consortium called the Trusted Computing Group (TCG) and are focusing on defining open standards for information system security [41]. Their goal is to develop standards and use them in all domains to protect against ransomware attacks by attackers and hackers. The group also wants to make mobile phones, PDAs, and PCs more trustworthy and give their owners a clear view of the platform's software stack. Because TC gives a high level of confidence, solutions based on it have already been built into millions of devices. The TPM has a secure and protected storage area to store secure data and other cryptographic keys [42]. It means that the data inside TPM is protected from malicious manipulation and alteration. Data inside TPM is stored inside data registers known as

platform configuration registers (PCRs). Remote attestation is the process by which platform status (the software loaded into the system) stored within the TPM is reported to external entities for verification and attestation. Due to the attestation and verification nature of TC, it is most appropriate for detecting and preventing ransomware. Hardware-based solutions that use the TPM can help mitigate ransomware and other security issues [43].

1.5 Objectives of the Study

The objective of this study is to fully understand the current state of ransomware with regard to its impact on individuals and businesses, how ransomware is propagated, and what the possible mitigation strategies are to protect against it. This study also intends to review trusted computing, as it is an important consideration in securing electronic devices against these threats.

1.6 Organization of the Paper

The organization of this paper is as follows: Section 2 covers the methodology of this study and how the search for literature was carried out. Various search terms to explore scientific databases for literature, screening, filtering, inclusion, and exclusion criteria are presented in this section. Results and discussion are presented in Section 3. This section mainly covers the implications of ransomware attacks, recovery methods, losses and damages caused by ransomware, dissemination, and encryption methods of ransomware, and also presents some statistical analysis. The paper is concluded in the final section.

2 Methodologies

This study used a qualitative methodology to explore the latest literature on ransomware, its impacts, dissemination, and mitigation techniques. It also highlights the anatomy of ransomware, how it attacks, and discusses possible countermeasures. A structured approach was carried out to search, evaluate, and review the latest and relevant studies. To explore the literature, we searched various scientific databases to identify relevant publications and these included Google Scholar, IEEE, ACM, MDPI, Researchgate, Hindawi, university websites, and different websites from companies that are actively working in the field. Several search terms were used to find the relevant literature, including "ransomware," "latest trends in ransomware," "ransomware propagation and mitigation techniques," "impact of ransomware on the economy," "ransomware attacks on the public sector," "ransomware attacks on the health sector," "ransomware attacks on education," "ransomware attacks on financial companies," "financial losses due to ransomware," and "trusted computing." Initially, 648 studies were retrieved. We included the literature published in reputable journals and conference proceedings in recent years and specifically addressed ransomware dissemination and mitigation techniques. Papers that were out of the scope of this study, duplicates, and published in non-English were excluded. Grey, unpublished literature, and publications from low-quality journals and conference proceedings were also not considered for inclusion. After screening and filtering, there were 37 studies left, which are included in this study.

3 Results and Discussion

Examining the severity of ransomware outbreaks around the world reveals that the most likely cause of ransomware spread is that the criminals concentrate where they see the best chance of financial benefits and where they expect weakness in the systems as per the countries' degrees of ransomware protection.

3.1 Ransomware Obliteration Statistics

Here are some key statistics released in the "Internet Crime Report 2022" and other cybersecurity websites. Details of the top countries victimized by less than 10,000 and more than 10,000 ransomware attacks in 2022, compared to the USA, are presented in Figures 5 and 6, respectively. With 479,181 reported ransomware attacks in 2022, the United States took the lead, and the United Kingdom came in second with 384,291 attacks.

Figure 7 shows the reported complaints and losses over the last five years in the USA. Ransomware also has a huge impact on industry and business. In 2019, ransomware affected about 56% of businesses from various industries. In 2020,

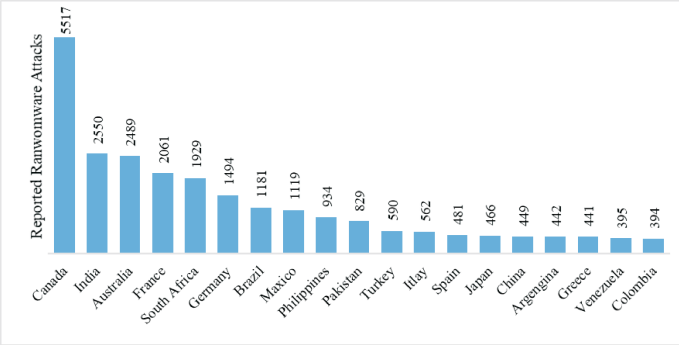

Figure 5: Top victimized countries with less than 10000 ransomware attacks [44]

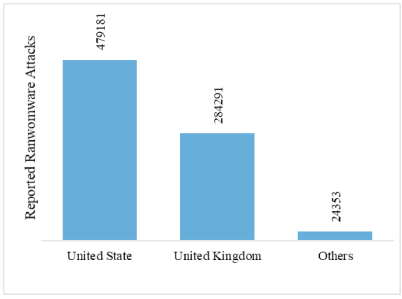

Figure 6: Top victimized countries with more than 10000 ransomware attacks [44]

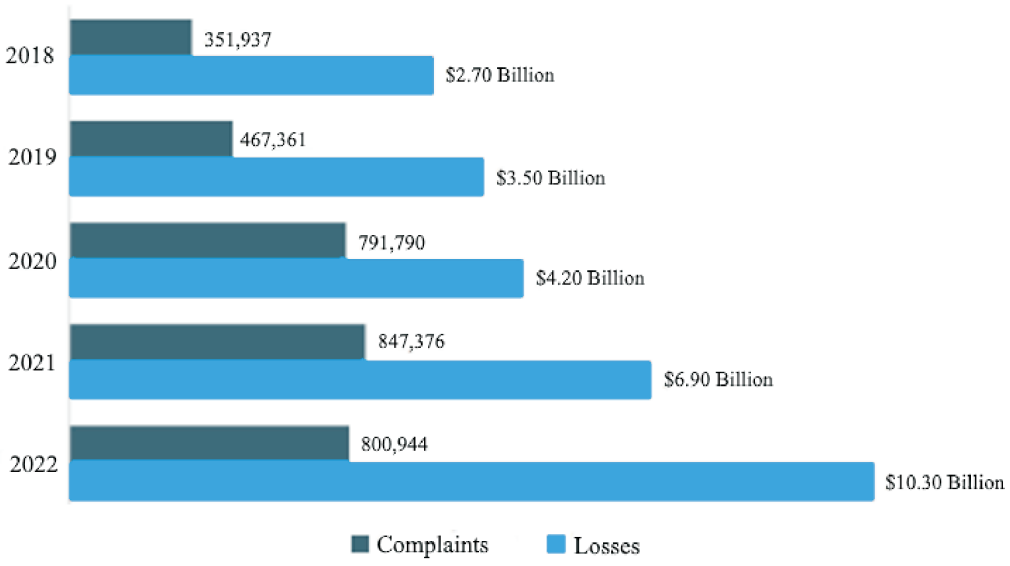

Figure 7: Reported complaints and losses during the last five years in the USA [44]

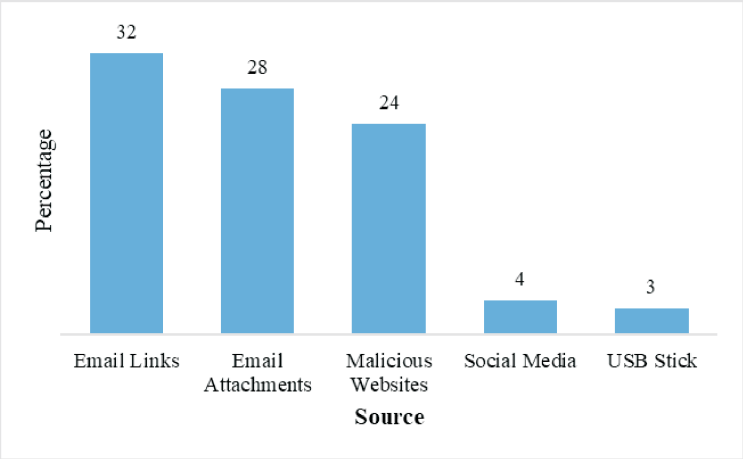

Figure 8: Different methods of ransomware propagation [16]

the healthcare sector reported a large number of ransomware attacks, which are almost 50% of the total number of such attacks, and that was the highest number ever [16]. Ransomware attacks have also wreaked havoc on the public and education sectors, with important and sensitive information about patients and users being the target [45].

It can be observed that the reported ransomware complaints reached a peak in the year 2021 with 847,376 complaints and aggregated losses of $6.90 billion, while businesses, individuals, and the government incurred losses of $10.3 billion due to ransomware attacks in 2022. Ransomware can be disseminated from different sources, mainly by clicking a malicious link that affects 32% of devices, email attachments that affect 28% of devices, and USB flash drives, which are the least likely source of ransomware infection, with only 3%. Further details are provided in Figure 8.

Data breaches due to ransomware attacks on the healthcare, public, and education sectors are summarized in Table 1

The dissemination techniques and encryption methods of popular ransomware are summarized in Table 2.

The implications of ransomware attacks and data recovery methods are presented in Table 3.

RanSim by KnowBe4 [37] is a malware detection simulator that does not use users' files in the system and can be used to detect certain types of malware on a computer running Windows. RanSim is able to perform its function by first imitating the actions of various forms of malware and subsequently determining whether or not the system's security software is able to recognize and thwart those behaviors. It tests 23 different types of infection scenarios and simulates ransomware infections. This can be a helpful way to test the efficacy of security software and ensure that it is able to detect and block potential threats. We also did an experiment with a system, during which we scanned it with RanSim to

Table 1: Data breaches in various sectors

Damages	**Source**
Healthcare Sector	
Nearly 2100 data breaches were recorded in 2009	[46]
Ransomware was to blame for half of all data breaches in the health industry	[47]
Since 2016, ransomware attacks on healthcare professionals in the US cost approximately $157 million	[48]
In 2020, 560 healthcare facilities were hit in 80 separate incidents	[49]
Cybercriminals hacked 9.7 million electronic medical records (EMR) in September 2020 alone	[48]
Public Sector	
In 2020, ransomware assaults on government entities accounted for about 33% of all attacks	[50]
The Florida city paid a $600,000 ransom to recover the compromised files in June 2019	[51]
Training sessions were arranged for nearly 38% of government workers on how to deal with ransomware attacks	[52]
From 2013 to 2018, at least one ransomware attack hit 48 of the 50 states in the US	[53]
Education Sector	
Between 2019 and 2020, ransomware attacks against universities increased by 100%	[54]
There have been nearly 84 ransomware attacks on 1681 higher education institutions since 2020	[54]
Nearly 84 ransomware attacks have hit 1681 higher education institutions since 2020	[49]
In April 2018, a Massachusetts school system paid $10,000 in bitcoin as a ransom	[55]

Table 2: Dissemination and encryption methods of various ransomware

Ransomware	Dissemination Technique	Encryption Method
WannaCry	Exploiting the Windows SMB vulnerability	AES-128 with RSA-2048 public key encryption
Locky	Email phishing campaigns	AES-128 with RSA-2048 public key encryption
Petya/NotPetya	Malicious software updates or email phishing	Overwrites the MBR
CryptoLocker	Email phishing campaigns	AES-256 with RSA-2048 public key encryption
Ryuk	Emotet or Trickbot malware as the initial infection	AES-256 with RSA-4096 public key encryption
Maze	Exploits unpatched software vulnerabilities	ChaCha20 with RSA-2048 public key encryption
Conti	RDP compromise or phishing attacks	AES-256 with RSA-2048 public key encryption
DarkSide	Compromise via phishing, RDP, or other vulnerabilities	AES-256 with RSA-2048 public key encryption

Table 3: System implication and data recovery [16]

Ransomware	System Implications	Data Recovery Methods
WannaCry	It encrypts files and distributes them over the network, causing system crashes	It encrypts around 177 types of files and first creates encrypted files and then deletes the original files. Data can be recovered before it starts deleting the original files. The data is restored without any changes
Locky	It encrypts files and deletes shadow copies; it can turn off security software	No free decryption tool is available. Some decryption methods using third-party software have been developed
Petya/NotPetya	Overwrites the MBR and encrypts files, which can cause system crashes	Restoration of data can be done by replacing MBR/BCD files manually. Data can be recovered without the original filenames
CryptoLocker	It encrypts files and deletes shadow copies; can turn off security software	No free decryption tool is available. Some decryption methods using third-party software have been developed
Ryuk	It encrypts files and deletes shadow copies; can turn off security software	No free decryption tool is available. Some decryption methods using third-party software have been developed
Maze	It encrypts files and exfiltrates data, which can turn off security software	No free decryption tool is available. Some decryption methods using third-party software have been developed
Conti	Encrypts files and exfiltrates data, which can turn off security software	No free decryption tool is available. Some decryption methods using third-party software have been developed
DarkSide	Encrypts files and exfiltrates data, which can turn off security software	No free decryption tool is available. Some decryption methods using third-party software have been developed

look for files that could possibly be infected. We used Windows Sandbox, which is a lightweight virtual environment that allows applications to be run in an isolated mode for the purposes of testing and debugging [56]. This allowed us to create a setting for our test that was secure, isolated, and under our complete control. Figures 9 and 10 present, respectively, the specifics of the encrypted files that the simulator analyzed and a summary of the results of the experiment.

After a ransomware attack, it becomes almost impossible to retrieve the data without the decryption keys, and one cannot get until you pay the ransom. Some forensic tools can be used to get keys from the memory, but in most ransomware, the keys are only in the memory for a very short time during the time the ransomware is running. Phishing emails are one of the most common methods used to distribute ransomware. Training employees on how to identify phishing emails can help prevent them from inadvertently clicking on a link or attachment that contains ransomware. Regularly updating software can help prevent ransomware attacks by patching vulnerabilities that attackers could use to gain access to a network. Implementing Two-Factor Authentication (2FA) can help prevent RDP attacks by requiring users to provide an additional form of authentication before accessing a network. Regularly backing up data can help mitigate the impact of a ransomware attack. If data is backed up regularly, it can be restored without having to pay a ransom. Endpoint protection software, such as antivirus or anti-malware software, can help detect and prevent ransomware attacks by scanning for known signatures or suspicious behavior.

4 Conclusion and Recommendations

The number of ransomware attacks is rising steadily around the world. Continuous attempts have been made to protect against them and learn about their destructive potential. This paper provides an insight into various ransomware and has raised awareness of the growing effects of ransomware as well as the measures to combat it. We have studied some simulators and tools to protect against ransomware. Ransomware is a threat to both corporations and individual users, and it is not easy to find a means of being fully protected against it. However, certain preventive action can be taken to protect vital data and information. We need to follow the golden rule that "prevention is better than cure," and it is very important

	Name	Status	Encrypted Test Files Path	Description
2	Archiver	Executed	C:\KB4\Varsim\DataDir\MainTests\24-Files	Simply archives files using gzip algorithm. This scenario should not be blocked!
3	BlackKingdomVar	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\23-Files	Simulates file related activity of a common version of Black Kingdom ransomware.
4	Collaborator	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\22-Files	Encrypts files similarly to a common version of Critroni. However, it relies on different processes fo
5	CritroniVariant	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\21-Files	Simulates the behavior of a common version of Critroni ransomware.
6	DearCryVariant	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\20-Files	Simulates file related activity of a common version of DearCry ransomware.
7	HollowInjector	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\19-Files	Encrypts files by injecting the encryption code into a legitimate process using process hollowing.
8	Injector	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\18-Files	Encrypts files by injecting the encryption code into a legitimate process using a common approach.
9	InsideCryptor	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\17-Files	Encrypts files using strong encryption and overwrites most of the content of the original files with
10	LockyVariant	NotVulnerabl	C:\KB4\Varsim\DataDir\MainTests\16-Files	Simulates the file activity performed by a popular version of Locky ransomware.
11	MazeVariant	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\15-Files	Simulates file related operations performed by Maze ransomware.
12	Mover	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\14-Files	Encrypts files in a different folder using strong encryption and safely deletes the original files.
13	PaymerVariant	NotVulnerabl	C:\KB4\Varsim\DataDir\MainTests\13-Files	Simulates file related operations performed by DoppelPaymer-like ransomware.
14	ReflectiveInjecto	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\12-Files	Encrypts files by injecting the encryption code into a legitimate process using an advanced approac
15	Remover	Executed	C:\KB4\Varsim\DataDir\MainTests\11-Files	Simply deletes files and does not create any file. This scenario should not be blocked!
16	Replacer	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\10-Files	Replaces the content of the original files. A real ransomware would show a message that fools use
17	RigSimulator	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\9-Files	Simulates a mining rig which uses the machine CPU to mine Monero.
18	RIPlacer	Unexecuted	C:\KB4\Varsim\DataDir\MainTests\8-Files	Attempts to encrypt files in a folder subject to controlled folder access ransomware protection. Thi
19	SlowCryptor	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\7-Files	Simulates the behavior of a ransomware variant that encrypts files slowly, to avoid detection by se
20	Streamer	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\6-Files	Encrypts files and writes data into a single file, using strong encryption, then deletes the original fi
21	StrongCryptor	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\5-Files	Encrypts files using strong encryption and safely deletes the original files.
22	StrongCryptorFas	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\4-Files	Encrypts files using strong encryption and deletes the original files.
23	StrongCryptorNe	Vulnerable	C:\KB4\Varsim\DataDir\MainTests\3-Files	Encrypts files using strong encryption and deletes the original files. It also simulates sending the e

Figure 9: RanSim Simulator - vulnerability scanning report

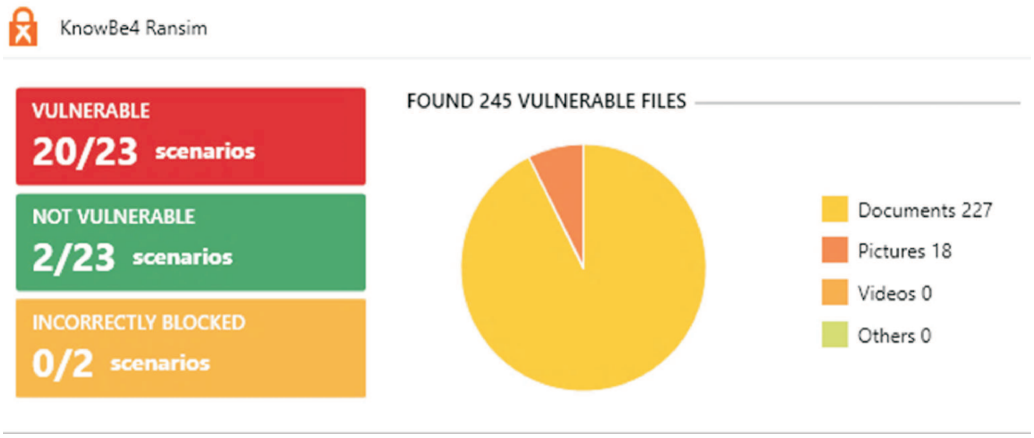

Figure 10: RanSim Simulator – summary of the results

to be careful when opening emails, unknown files, or websites that might be harmful. Antivirus software and firewalls can also be used to secure the systems. However, ransomware evolves at a much faster rate than antivirus software and firewalls. The TPM provides some hope in the battle against this cryptovirology, but billions of devices still remain at risk.

As ransomware attacks continue to evolve, researchers will need to stay on top of the new strains of ransomware that are emerging. It could involve developing new methods for analyzing and detecting ransomware as well as studying the behavior and tactics of ransomware attackers. Since financial gain is frequently the driving force behind ransomware attackers, it is important to conduct research on their business models [57] for both the payment methods they use and the ways in which their victims react to their demands. Researchers could explore new ways to prevent and mitigate the impact of ransomware attacks by developing new security protocols, such as using blockchain technology to secure data or developing new methods for detecting and blocking ransomware in real time. Further, blockchain has proved its potential for data security and immutability and to date, there is no evidence of a security breach or data being compromised [58]. But, as a precautionary measure, there might be a future consideration of this technology against ransomware attacks.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this study as per the journal's policy.

References

[1] Davies, S. R., Macfarlane, R. and Buchanan, W. J. Evaluation of live forensic techniques in ransomware attack mitigation. Forensic Science International: Digital Investigation **33**, 300979 (2020).

[2] Kara, I. and Aydos, M. The rise of ransomware: Forensic analysis for windows based ransomware attacks. Expert Systems with Applications **190**, 116198 (2022).

[3] Lemmou, Y., Lanet, J. and Souidi, E. M. A behavioural in-depth analysis of ransomware infection. IET Information Security [15], 38–58 (2021).

[4] YusirwanS S., Prayudi, Y. and Riadi, I. Implementation of Malware Analysis using Static and Dynamic Analysis Method. International Journal of Computer Applications **117**, 11–15 (2015).

[5] Humayun, M., Jhanjhi, N., Alsayat, A. and Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal **22**, 105–117 (2021).

[6] Adamov, A., Carlsson, A. and Surmacz, T. An Analysis of LockerGoga Ransomware. in 2019 IEEE East-West Design and Test Symposium (EWDTS) 1–5 (IEEE, 2019).

[7] Alqahtani, A. and Sheldon, F. T. A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. Sensors **22**, 1837 (2022).

[8] McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J. and Buchanan, W. J. Ransomware: Analysing the Impact on Windows Active Directory Domain Services. Sensors **22**, 953 (2022).

[9] Chesti, I. A., Humayun, M., Sama, N. U. and Jhanjhi, N. Evolution, Mitigation, and Prevention of Ransomware. in 2020 2nd International Conference on Computer and Information Sciences (ICCIS) 1–6 (IEEE, 2020).

[10] Oz, H., Aris, A., Levi, A. and Uluagac, A. S. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Computing Surveys **54**, 1–37 (2022).

[11] Tang, F. et al. RansomSpector: An introspection-based approach to detect crypto ransomware. Computers & Security **97**, 101997 (2020).

[12] Hernandez-Castro, J., Cartwright, A. and Cartwright, E. An economic analysis of ransomware and its welfare consequences. Royal Society Open Science **7**, 190023 (2020).

[13] Arabo, A., Dijoux, R., Poulain, T. and Chevalier, G. Detecting Ransomware Using Process Behavior Analysis. Procedia Computer Science **168**, 289–296 (2020).

[14] Alzahrani, A., Alshehri, A., Alshahrani, H. and Fu, H. Ransomware in Windows and Android Platforms. (Preprint) [Online] Available: https://arxiv.org/abs/2005.05571 (2020).

[15] FBI, RANSOMWARE SCAMS AND SAFETY. [Online] Available: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

[16] Sobers, R. 81 Ransomware Statistics, Data, Trends and Facts for 2021 — Varonis. [Online] Available: https://www.varonis.com/blog/ransomware-statistics.

[17] Sophos Cybersecurity as a Service. [Online] Available: https://www.sophos.com.

[18] Cicala, F. and Bertino, E. Analysis of Encryption Key Generation in Modern Crypto Ransomware. IEEE Transactions on Dependable and Secure Computing **19** (2020).

[19] Akbanov, M., Vassilakis, V. G. and Logothetis, M. D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Computers & Electrical Engineering **76**, 111–121 (2019).

[20] Bae, S. Il, Lee, G. Bin and Im, E. G. Ransomware detection using machine learning algorithms. Concurrency and Computation: Practice and Experience **32**, (2020).

[21] Wood, A. C. and Eze, T. The Evolution of Ransomware Variants. in Proceedings of the 19th European Conference on Cyber Warfare (ACPI, 2020).

[22] Ndichu, S., McOyowo, S., Okoyo, H. and Wekesa, C. A Remote Access Security Model based on Vulnerability Management. International Journal of Information Technology and Computer Science **12**, 38–51 (2020).

[23] Adhianto, L. et al. HPCTOOLKIT: tools for performance analysis of optimized parallel programs. Concurrency and Computation: Practice and Experience **22**, 685–701 (2010).

[24] Марценюк, В., Дідманідзе, І., Сверстюк, А., Андрущак, І. and Рудь, К. Automated method of building exploites in analysis software testing. COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION **39**, 146–150 (2020).

[25] Fernández Maimó, L. et al. Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. Sensors **19**, 1114 (2019).

[26] Mehra, C., Sharma, A. K. and Sharma, A. Elucidating Ransomware Attacks In Cybersecurity. International Journal of Innovative Technology and Exploring Engineering **9**, 3536–3541 (2019).

[27] Immunity Debugger. [Online] Available: https://www.immunityinc.com/products/debugger.

[28] Gómez-Hernández, J. A., Álvarez-González, L. and García-Teodoro, P. R-Locker: Thwarting ransomware action through a honeyfile-based approach. Computers & Security **73**, 389–398 (2018).

[29] Gu, Z., Saltaformaggio, B., Zhang, X. and Xu, D. Gemini: Guest-transparent honey files via hypervisor-level access redirection. Computers & Security **77**, 737–744 (2018).

[30] Y. Connolly, L. and Wall, D. S. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security **87**, 101568 (2019).

[31] Beaman, C., Barkworth, A., Akande, T. D., Hakak, S. and Khan, M. K. Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security **111**, 102490 (2021).
[32] Uandykova, M. et al. The social and legislative principles of counteracting ransomware crime. Entrepreneurship and Sustainability Issues **8**, 777–798 (2020).
[33] Mcafee. Jigsaw Ransomware. [Online] Available: https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.jigsaw-ransomware.html.
[34] Norton. Jigsaw. [Online] Available: https://us.norton.com/internetsecurity-emerging-threats- jigsaw-ransomware-wants-to-play-a-game-but-not-in-a-good-way.html.
[35] Akcora, C. G., Li, Y., Gel, Y. R. and Kantarcioglu, M. BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain. in Proceedings of the 9th International Joint Conference on Artificial Intelligence 4439–4445 (2020).
[36] Reshmi, T. R. Information security breaches due to ransomware attacks - a systematic literature review. International Journal of Information Management Data Insights **1**, 100013 (2021).
[37] KnowBe4. RanSim - Ransomware Simulator. [Online] Available: https://www.knowbe4.com/ransomware-simulator.
[38] Broadhurst, R. and Trivedi, H. Malware in spam email: Risks and trends in the Australian Spam Intelligence Database. (Australian Institute of Criminology, 2020).
[39] Alshaikh, H., Ramadan, N. and Ahmed, H. Ransomware Prevention and Mitigation Techniques. International Journal of Computer Applications **177**, 31–39 (2020).
[40] Intel. What is Trusted Platform Module (TPM). [Online] Available: https://www.intel.com.
[41] Sailer, R., Zhang, X., Jaeger, T. and Doorn, L. van. Design and Implementation of a TCG-based Integrity Measurement Architecture. in In Proceedings of the 13th USENIX Security Symposium, San Diego, USA, 2004. (2004).
[42] Lu, D. et al. xTSeH: A Trusted Platform Module Sharing Scheme Towards Smart IoT-eHealth Devices. IEEE Journal on Selected Areas in Communications **39**, 370–383 (2021).
[43] Jha, D. N., Lenton, G., Asker, J., Blundell, D. and Wallom, D. Trusted Platform Module-Based Privacy in the Public Cloud: Challenges and Future Perspective. IT Professional **24**, 81–87 (2022).
[44] FBI. Internet Crime Report, 2022. [Online] Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022s_IC3Report.pdf.
[45] Morato, D., Berrueta, E., Magaña, E. and Izal, M. Ransomware early detection by the analysis of file sharing traffic. Journal of Network and Computer Applications **124**, 14–32 (2018).
[46] TechJury. [Online] Available: https://techjury.net.
[47] The US Department of Health and Human Services (HHS). [Online] Available: https://www.hhs.gov.
[48] HIPPA. HIPAA Journal. [Online] Available: https://www.hipaajournal.com.
[49] Emsisoft. [Online] Available: https://www.emsisoft.com.
[50] Security Intelligence – Cybersecurity Analysis and Insight. [Online] Available: https://securityintelligence.com.
[51] CBC News. [Online] Available: https://cbc.canews.
[52] IBM. [Online] Available: https://www.ibm.com.
[53] Bank Information Security News. [Online] Available: https://bankinfosecurity.com.
[54] BlueVoyant. MDR, Supply Chain Defense, Digital Risk Protection. [Online] Available: https://bluevoyant.com.
[55] CyberScoop. [Online] Available: https://cyberscoop.com.
[56] Microsoft. Windows Sandbox. [Online] Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox.
[57] Sarwar, M. I., Nisar, K., Khan, I. and Shehzad, D. Blockchains and Triple-Entry Accounting for B2B Business Models. Ledger **8**, 37–57 (2023).
[58] Sarwar, M. I. et al. Data Vaults for Blockchain-Empowered Accounting Information Systems. IEEE Access **9**, 117306–117324 (2021).