A State-of-the-Art Review of Ransomware Attacks on Internet of Things: Trends and Mitigation Strategies

Mobolaji D. Ogunbadejo[1], Oluwatobi A. Ayilara-Adewale[2] Moghaddam Anna[3],
[1]Department of Information System Management, Stanton University, 888 Disneyland Dr #400, Anaheim, California 92802, USA.
[2]Department of Information Technology, Osun State University, P.M.B. 4494, Oke Baale Road, Osogbo, Nigeria.
[3]Department of Information System Management, Stanton University, 888 Disneyland Dr #400, Anaheim, California 92802, USA.
*Email address of the corresponding author: mogunbadejo24@stanton.edu

Abstract

The increase of ransomware targeting the Internet of Things (IoT) is among the most significant challenges in cybersecurity. IoT devices are used extensively in healthcare, manufacturing, and smart structures due to their various functions. Thus, they are attacked because of their known vulnerabilities, such as limited resources, old firmware that has not been updated for years and poor security settings that become attractive targets for today's advanced ransomware attacks. Most importantly, the IoT involves several systems in various technologies, meaning that the controls of one device can compromise several systems, thereby disrupting IoT networks all over the globe. This paper gives an overview and evaluates the trends that characterize IoT ransomware, such as double and triple extortion strategies, a comprehensive state-of-the-art review of the evolution of ransomware, current practices of managing the risks inherent in the IoT system and the key challenges in mitigating ransomware in IoT devices. The paper concluded with recommendations for mitigating ransomware in IoT devices

Keywords: Ransomware, Internet of Things (IoT), Cyber-Attack, Threat Analysis.
DOI: 10.7176/JIEA/15-2-01
Publication date: May 28th 2025

1. Introduction

In the ever-evolving digital age, ransomware attacks, especially on the Internet of Things, have become more prominent and sophisticated; thus, the cyberthreat landscape is evolving. Ransomware is coined from two words, "Ransom and ware", where ransom refers to payment, and ware indicates a malware attack (Rana et al., 2024, Lee et al., 2024) . Ransomware is a type of malware that holds a victim's files hostage by encrypting them or locking access to systems until certain conditions agreed upon by the attacker are met (Keshavarzi and Ghaffary, 2020).

The Internet of Things (IoT) is a fast-growing global network of 'things', be they tangible objects or digital products and services, that are connected and can exchange information over the Internet with minimal or no human interaction (Schoder, 2018, Malik et al., 2021, Chui et al., 2021) . The practical applications of IoT encompass everything from smart home appliances to fitness and health monitoring smart wearables, industrial sensors, and remote health monitoring equipment. In addition, Smart City IoT has revolutionized operational efficiency, as depicted in Figure 1. The Internet of Things (IoT) is one of the most influential trends in business today, connecting billions of devices and sharing data in real time. Nevertheless, the more IoT technology is embraced, the more vulnerable it becomes to cyber threats, especially ransomware attacks (Obaidat et al., 2020, Simaiya et al., 2020, Sun and Jung, 2024) .

IoT is susceptible to many attacks, and one of the most terrifying attacks is the ransomware attack, which has recently become more frequent and evolved in complexity, aiming at IoT infrastructure's key systems and networks (Park et al., 2022). Attackers have targeted IoT devices in recent years since their significance is vital in our day-to-day activities with attack focus on areas such as manufacturing industries, finance, government etc., as shown in Figure 2. The ThreatLabz analyzed about 300,000 blocked attacks on IoT devices with a 400% increase in IoT malware attacks while Botnets remain prevalent in malware attacks with the Mirai and Gafgyt malware families constituting 66% of the attack payloads (ThreatLabz, 2023), this is depicted in Figure 3.

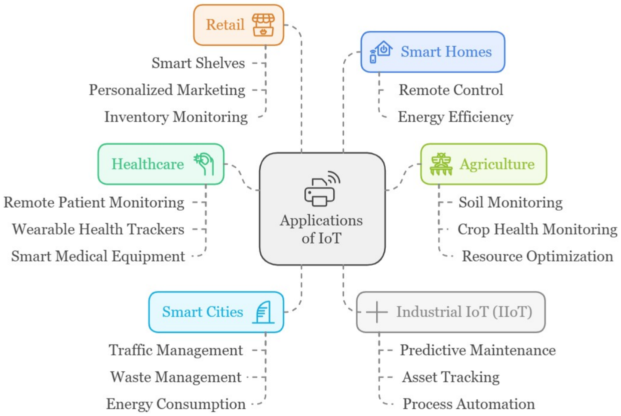

Figure 1: Real-life applications of IoT.

The reason they are easy targets for attackers is that most IoT devices run on lightweight, low-power equipment that lacks sophisticated security functionalities. Moreover, sometimes, they contain old software or firmware that are rarely updated or patched, which makes them easy prey for hackers. Additionally, the number of security measures implemented in different IoT systems is still relatively low (Staddon et al., 2021). Due to the vast connectivity of the Internet and different manufacturers making devices that interconnect with each other on the IoT network, the issue of creating a standardized security framework is challenging. Furthermore, IoT devices are usually installed with default settings such as usernames and weak passwords like admin and open ports, making them an easy target for attackers (Kaur et al., 2023, Ye et al., 2024).

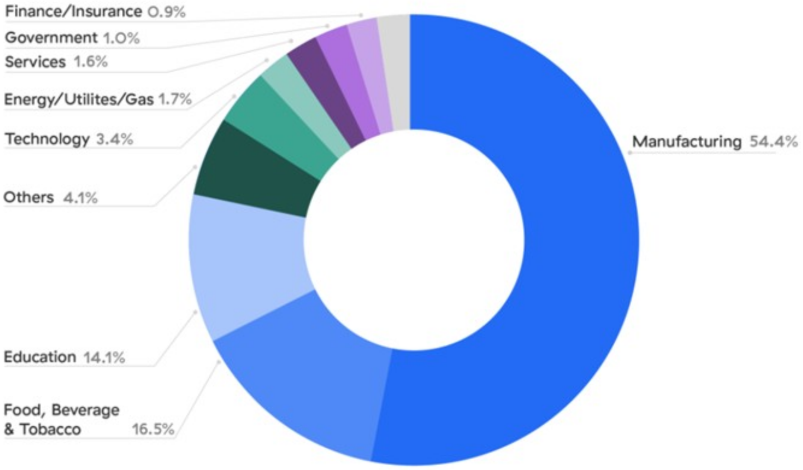

Figure 2: Proportion of Ransomware Attack on Organizations (ThreatLabz, 2023)

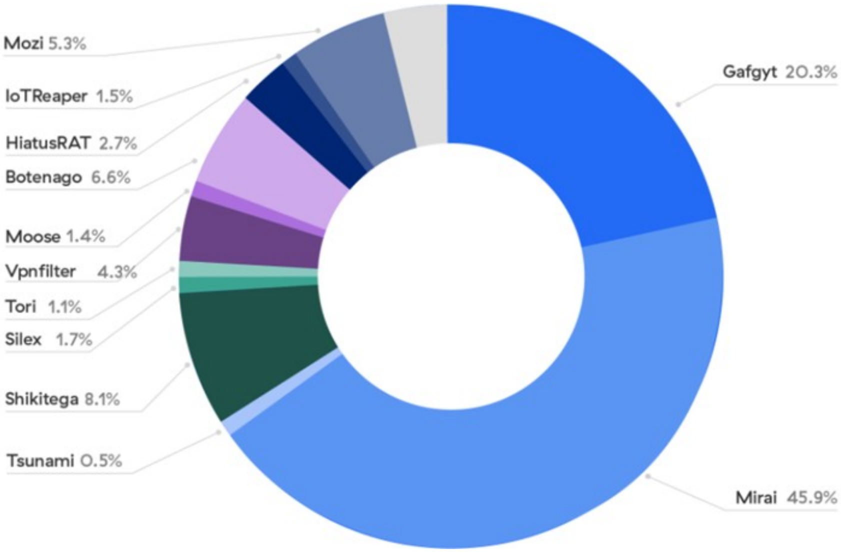

Figure 3: Prevalent Ransomware Attacks on IoT Devices

Ransomware attacks have become more frequent, and the impact is more severe and complex, especially in areas where IoT devices are essential for sensitive processes, such as in finance, healthcare, and infrastructure. Instances of such attacks on healthcare IoT devices can range from imaging systems, infusion pumps, and IoT-enabled pacemakers, which can cause life-threatening circumstances that force and hasten the healthcare provider to pay (Minnaar and Herbig, 2021, Cartwright, 2023), the attack trend is depicted in Figure 4.

This emerging threat requires identifying how ransomware operates on distinct IoT structures and the approaches to mitigate it. This article comprehensively discusses the evolution of ransomware attacks from inception and the landscape of ransomware attacks on IoT. Section 2 introduces the literature review, the detection technique, and current mitigation strategies for IoT ransomware. Section 3 elaborates on the key challenges in mitigating ransomware in IoT devices. The article concluded with a recommendation of the best practices discussed in Section 4, and Section 5 discussed the future direction in mitigating ransomware in IoT.

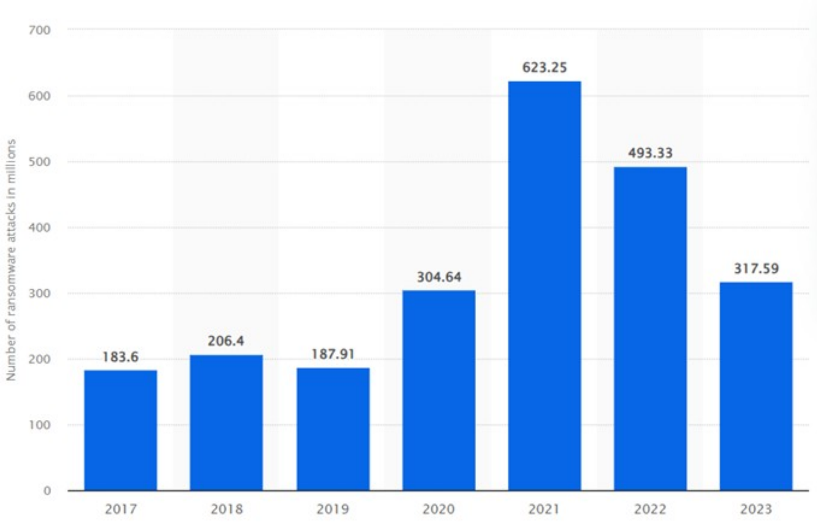

Figure 4: Trend of Ransomware Attacks (SonicWall, 2024)

2. LITERATURE REVIEW

This section discusses a comprehensive state-of-the-art review of the current trends and advancements in ransomware attacks on IoT devices. The section discusses the following: section 2.1 discusses the strategies of ransomware attacks and variants. Section 2.2 provides a detailed analysis of the evolution of ransomware.

Section 2.3 summarizes the findings from the evolution of ransomware. Section 2.4 discusses the categories of ransomware, while section 2.5 elaborates on ransomware detection techniques. Section 2.6 provides the current mitigation strategies for IoT ransomware.

2.1. Ransomware Attack Strategies and Variants

Ransomware attack tactics refer to numerous techniques that an attacker employs in order to gain access into systems, encrypt data and request for ransom. These strategies are dynamic and change over time depending on the technology and ever-increasing security measures. Figure 5 shows the tactical and efficient structure of how modern ransomware attacks are executed. The attack starts with gaining the first foothold. Attackers gain their first unauthorized entry by using techniques such as phishing with malicious attachments or through discovering software flaws. Once inside, attackers conduct network reconnaissance on the network to identify key systems and valuable information. In order to maintain this access, they create persistence by creating a backdoor, scheduled tasks, or rogue accounts. Thereafter, they proceed to the privilege escalation, where they acquire administrator or root-level access to perform high-impact operations. Once higher-level access is obtained, attackers move laterally, shifting through the network to compromise more systems.

Subsequently, they target the recovery processes by performing shadow copy deletions and executing backup destruction ensuring that the victim has no way of recovering from the attack. Prior to the encryption of files, the attackers proceed to data exfiltration and inform victims that they will release the stolen data. After which encryption is done, making significant files inaccessible under strict encryption and leaving a message for ransom to be paid for the decryption key. If ransom is not paid, the attackers move to the next level by posting the stolen data on leak sites, compromising the reputation of the victim organization, or launching Distributed Denial of Service (DDoS) attacks to paralyze the operations, thus the triple extortion technique.

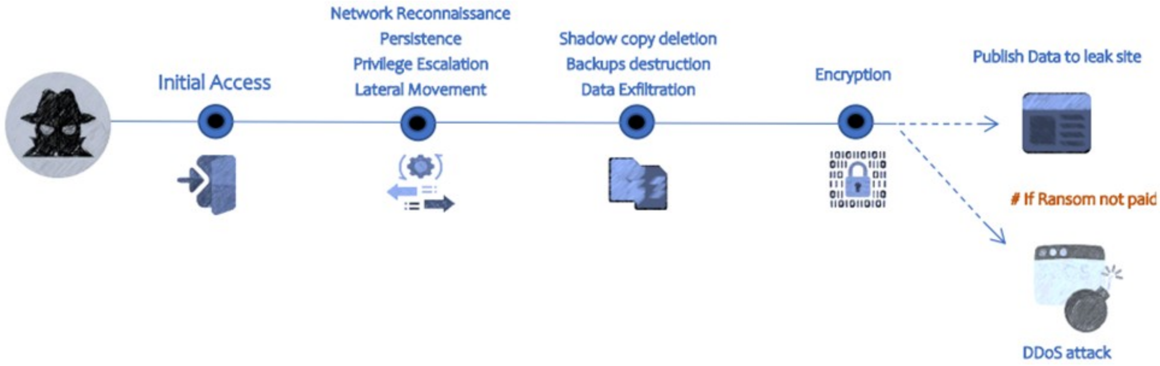

Figure 5: Stages in Advance Ransomware Attack.

Though modern ransomware attacks keep emerging, some variants such as Hive, lockbit, Black Basta, and ALPHV/BlackCat are major threats to large organizations, but Phobos and Makop families mainly focus on small and medium organizations. Gjvu/Stop variants continued to dominate individual attacks in recent years, as shown in Figure 6.

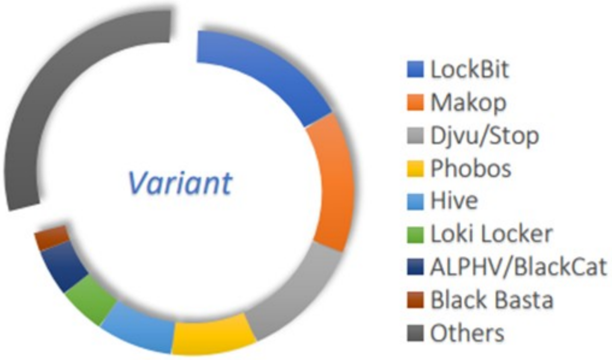

Figure 6: Variants of Major Ransomware Threats.

2.2. The Evolution of Ransomware

Ransomware has evolved over the years after its inception in 1989, from the first recorded attack known as AIDS Trojan to the modern, sophisticated attacks(Razaulla et al., 2023, Nagar, 2024, Jabid et al., 2025). The AIDS Trojan was relatively simple, but the wave of ransomware began through data encryption. Thus, GPCode further developed ransomware by adding RSA encryption by 2004, which started using cryptographic techniques (Wani and Revathi, 2020). In 2012, Reveton used social engineering techniques to trick users by pretending to be law enforcement and demanding that they pay fines (Young et al., 2020). In contrast, in 2013, CryptoLocker advanced ransomware payment by introducing anonymous payments such as Bitcoin, making tracking the payment almost impossible (Jabid et al., 2025, Ahmed, 2024) . These early phases built a basis for more advanced and sophisticated attacks.

The mid-2010s marked another level of evolution in the ransomware threat, both in the choice of platforms to attack and the techniques. SynoLocker was launched in 2014 to lock network-attached storage (NAS), while Sypeng introduced ransomware to portable platforms (Ko and Kim, 2022). In 2015, TeslaCrypt targeted game files, and Encoder introduced Ransomware-as-a-Service (RaaS), which allows non-technical cybercriminals to launch attacks (Niveditha et al., 2024). The first known ransomware designed for macOS, was KeRanger which emerged in 2016, showing that the ransomware has become platform-independent software (McIntosh et al., 2021, Oz et al., 2022). WannaCry in 2017 used a Windows flaw to disrupt organizations worldwide, showing that ransomware could affect anyone, anywhere(Prevezianou, 2021, Hyslip and Burruss, 2023).

As of 2018, ransomware attacks have become more specific and systemic (Al-Rimy et al., 2018); noteworthy examples include GrandCrab, which targeted the RaaS model, and Ryuk, which extorted large amounts of money from organizations. Similarly, in 2020, during COVID-19, NetWalker exploited healthcare vulnerabilities, which was a global disaster(Baig et al., 2023, Zhang et al., 2024). High-profile attacks such as DarkSide on Colonial Pipeline by 2021 make it clear that ransomware is a dangerous threat to the infrastructure . Modern strains like LockBit 3.0 and BlackCat came with new features like bug bounty and cross-platform attacks, indicating how advanced ransomware has evolved. In 2023, ransomware was more sophisticated and stealthier, as in the case of Royal, who used social engineering techniques, and Rorschach had the fastest encryption speed(Liu et al., 2023). The growth of AI and the increasing focus on targeting IoT devices indicate the progression of ransomware attacks. These attacks include emerging trends such as double extortion, data theft, Ransomware-as-a-Service, which remain prevalent. This highlights the paramount importance of effective patching and cybersecurity innovation in combating these persistent threats. The evolution and trend of ransomware is discussed in Table 1.

Table 1: Comprehensive Overview of Ransomware Evolution and Trends

S/N	Ref	Year	Ransomware	Attack mode	Attack Mechanism (mode of attack)	Platform
1	(Nagar, 2024)	1989	AIDS Trojan	Encryption of file name	Infected floppy disk	MS-DOS
2	(Zimba et al., 2019)	1996	Cryptoviral extortion	public key cryptography	infected floppy disks and email	Microsoft Windows
3	(Alzahrani et al., 2020)	2005	Trojan PGPcoder	Encryption of file	Spam email attachment	Microsoft Windows
4	(Jabid et al., 2025)	2005	Archievus	Encryption of specific files (My document)	Social engineering	Microsoft Windows
5	(Othman and Zolkipli, 2021)	2006	Trojan.CryZip	Encryption and compression of files into password-protected ZIP archives	malicious downloads or phishing	Microsoft Windows
6	(Upadhyay et	2008	Gpcode.AK	Encryption of files	Phishing	Microsoft

	al., 2025)					Windows
7	(Bhardwaj, 2017)	2008-2009	Fake AV (Antivirus)	Scareware displaying fake virus infection alerts	Social engineering via malicious pop-ups, drive-by downloads, or email attachments	Microsoft Windows
8	(Sultan et al., 2018)	2011	Unnamed Trojan	locking files or encryption	Social engineering (malicious email attachments or compromised websites)	Microsoft Windows
9	(Sheen and Gayathri, 2022)	2012	Locker ransomware	Locking access to the system or files	exploit kits, phishing, and infected downloads.	Microsoft Windows
10	(Sharma and Shanker, 2022)	2012	Reveton	Locking the system with fake law enforcement warnings	Drive-by downloads via malicious websites or exploit kits	Microsoft Windows
11	(Kara, 2024)	2013	CryptoLocker	File encryption encompasses a message with an encryption key that is required to unlock the file on the affected computer.	It is distributed using infected files in email attachments, including an invoice or a fake ZIP file, and via exploit kits on hacked websites.	Microsoft Windows
12	(McElhinney and Curran, 2020)	2014	CryptoDefense	File locking with a ransom notification message for the owners.	It is transferred through email attachments to users and through the use of exploit kits by social engineering.	Microsoft Windows
13	(Cen et al., 2024)	2014	CryptoWall	File encryption with ransom notes presented in text format, HTML, and as the desktop background image	Spread through phishing emails, infected documents or drive-by downloads, exploit kits and malicious advertisements (malvertising).	Microsoft Windows
14	(Ko and Kim, 2022)	2014	Sypeng	Collecting people's sensitive data and ransom demand display.	Distributed through malicious apps on the Google Play Store, targeting users via social engineering tactics.	Android devices.

15	(Niveditha et al., 2024)	2014	CTB-Locker	File encryption with a countdown timer for ransom payment is displayed on the victim's system.	It is spread through spoofing emails with .zip files or linked images and files through the exploit kits.	Microsoft Windows
16	(Mohammad, 2020)	2015	TeslaCrypt	Encryption of games files and then demand ransom for their decryption.	Phishing emails, infected documents or downloads	Microsoft Windows
17	(Raheem et al., 2021)	2015	DMA Locker	Encrypt files with ransom notes that are placed on the user's screens.	It was first spread via remote desktop protocol compromise, exploit kits, and email attachments.	Microsoft Windows
18	(Yamany et al., 2022)	2015	Linux.Encoder	File encryption specific to web servers and the corresponding directories.	Intrusion of weaknesses via web applications such as Magento for accessing and encrypting files on a server.	Linux systems.
19	(Keshavarzi and Ghaffary, 2020)	2016	AnonPop	Displaying ransom notes claiming to be from "Anonymous" and demanding bitcoin payment.	Spread via phishing emails and malicious attachments.	Microsoft Windows
20	(Anugerah et al., 2024)	2016	Jigsaw	File encryption, where files are erased randomly until ransom is paid. One of the peculiarities is that each time the victim attempts to shut the ransom note or delay payment, the ransom amount rises.	Shared through malicious attachments, exploit kits, and fake software updates.	Microsoft Windows
21	(Aggarwal, 2023)	2016	KeRanger	Encryption of files with ransom messages	Initially spread via a trojanized version of a legitimate application (Transmission, a Mac torrent client). The ransomware encrypted files and demanded payment in Bitcoin.	MacOS systems
22	(Ren et al., 2020)	2016	Petya	Encrypting the Master File Table (MFT) of the hard drive, making the system wholly	Spread through email scams, often in attachment form or through a link to a	Microsoft Windows

				inaccessible and demanding ransom	malicious page. Other versions were propagated via the EternalBlue exploit as well.	
23	(Raheem et al., 2021)	2016	VenusLocker	Encryption of files mainly focuses on the specific extension, which is then accompanied by a ransom in Bitcoin.	Distributed through phishing emails with links or downloading files.	Microsoft Windows
24	(Young et al., 2020)	2016	ZCryptor	File encryption and self-replication between systems using removable media and network shares.	It spread through malicious email attachments, fake software installers, and macro-enabled documents. It encrypted files and behaved like a worm, which directly spread to other related devices.	Microsoft Windows
25	(Kim et al., 2022)	2016	CryptXXX	Encryption of files and stealing important credentials to demand payment in Bitcoin.	Distributed by exploit kits like Angler and email attachments.	Microsoft Windows
26	(Alotaibi and Vassilakis, 2021)	2017	Bad Rabbit	File encryption and prevention of any further access to the system ransom information on the screen.	It spreads through a malware attack on infected Websites using a fake Adobe Flash player update.	Microsoft Windows
27	(Kim and Lee, 2020)	2017	Erebus	File encryption of local files and web servers.	Being spread through infected websites and phishing emails	Linux and Microsoft Windows
28	(Hyslip and Burruss, 2023)	2017	WannaCry	File encryption incorporated a worm-like propagation mechanism in the networks.	Attacked the unpatched Windows systems, exploiting the EternalBlue vulnerability in the Server Message Block (SMB) protocol.	Microsoft Windows
29	(Mos and Chowdhury, 2020)	2017	NotPetya	The ransomware encrypted the Master File Table (MFT) and put a ransom note.	Spread through software updates and took advantage of the EternalBlue vulnerability	Microsoft Windows

30	(Seymour, 2022)	2018	GandCrab and Ryuk	Encrypted files with a request for payment in cryptocurrency.	GandCrab was spread through exploit kits, phishing emails and malicious attachments. Ryuk: Spread through phishing Email and RDP (Remote Desktop Protocol) brute force attack.	Microsoft Windows
31	(Routray et al., 2023)	2018	SamSam	Encryption of files with demands for payment, a type which commonly targets important assets.	Essentially transmitted through successful attacks carried out through phishing and weak or exposed credentials belonging to the RDP	Microsoft Windows
32	(Ploszek et al., 2021)	2018	Katyusha	Encrypted files along with the demand of the ransom.	Acting through email attachments and exploit packs. Katyusha encrypted files on infected systems with a ransom note requiring Bitcoin to unlock files.	Microsoft Windows
33	(Tuunainen, 2021)	2019	PwndLocker	Encrypted files and data stealing with a ransom note.	Spread through phishing emails, malicious attachments, or compromised remote access tools (such as RDP).	Microsoft Windows
34	(Seth et al., 2022)	2019	LockerGoga	Encrypted files with a random request.	Distributed through phishing emails or through the RDP brute force attack.	Microsoft Windows
35	(August et al., 2022)	2019	Dharma	File encryption with the ransom.	Transmitted through phishing emails containing infected attachments or using RDP vulnerability.	Microsoft Windows
36	(Baig et al.,	2020	NetWalker	File encryption with	NetWalker ransomware	Microsoft

	2023)			double extortion.	is spread through phishing emails with attachments or exploiting the network's vulnerabilities.	Windows
37	(Beaman et al., 2021)	2020	Nefilim	File encryption together with double extortion.	Nefilim is spread by infected RDP credentials or through the vulnerabilities in the victim's network.	Microsoft Windows
38	(Gajjar et al., 2024)	2020	v2020	File encryption with a ransom demand.	Spread through phishing emails and vulnerabilities of the RDP services.	Microsoft Windows
39	(Kerns et al., 2022)	2020	Maze	File encryption is accompanied by double extortion.	Spread through phishing mail, exploit kits, or gaining unauthorized access to RDP.	Microsoft Windows
40	(Umar et al., 2021)	2020	REvil (Sodinokibi)	File encryption with double extortion.	It spreads through phishing emails, malicious attachments, exploit kits, and infected RDP connections.	Windows operating systems
41	(Gómez Hernández et al., 2023)	2020	Tycoon	Encryption of files with specific attacks.	Spread through compromised RDP connections.	Linux systems and Microsoft Windows
42	(Beerman et al., 2023)	2021	Darkside	File encryption combined with data exfiltration	Phishing, unpatched software, and brute-force RDP compromises.	Windows-based systems, Linux servers
43	(Moran Stritch et al., 2021)	2021	Conti	File encryption with double extortion.	Phishing emails, malicious attachments, and unpatched software.	Windows operating systems.
44	(Westbrook, 2021)	2021	PhoenixLocker	Encryption of files with a ransom demand.	Weak credentials, phishing and RDP vulnerabilities	Windows operating system

45	(Mogage and Lucanu, 2024)	2021	Avaddon	Encryption of file with data exfiltration	Exploitation of compromised or weak credentials,	Windows operating systems.
46	(Aguilar Antonio, 2024)	2021	BlackByte	Encrypts files on compromised systems	unpatched vulnerabilities or misconfigured systems.	Windows and Linux systems
47	(Denham and Thompson, 2023)	2021	Hive/L0cked	Encryption and Data exfiltration	exploit kits and phishing emails	Windows-based systems
48	(Nicho et al., 2023)	2021	BlackCat	File encryption with double extortion	Phishing or exploitation of weak security measures	Windows, Linux, and VMware ESXi systems
49	(Eliando and Warsito, 2023)	2022	LockBit 3.0	Data encryption and data leak	software vulnerabilities, RDP vulnerabilities, phishing,	Windows-based systems, Linux servers
50	(Ko and Kim, 2022)	2023	ALPHV Blackcat	Data theft, leak and encryption	phishing emails, exploiting vulnerabilities in RDP and remote services.	Windows-based systems, Linux, VMware ESXi
51	(Kim et al., 2024)	2023	Rhysida	Data leak, theft and encryption.	phishing emails, exploiting vulnerabilities, or using RDP, brute force attacks	Windows operating systems, cloud environments, Linux servers.
52	(Kim et al., 2024)	2023	Rorschach	Encryption of files with a ransom note.	Exposed RDP servers, phishing, or software vulnerabilities	Windows-based systems

Table 1 discusses ransomware's evolution, from its first notable incidence in 1969 to its present advancements. It highlights features such as attack mode, attack mechanisms and the targeted platforms. Some key observations have been seen from Table 1, such as the initial ransomware from 1989 to 1995, the primary target of which was MS-DOS systems, which used file name encryption and were distributed through infected floppy disks. The next ransomware introduced Cryptoviral extortion in 1996, which uses public key cryptography to spread ransomware via email and infected floppy disks. The emergence of email as an attack vector started in 2000 and ran through 2005, and it used social engineering and spam email attachments for distribution.

The rise of sophisticated methods started from 2006 to 2011 when the attack approach diversified with strategies such as using scareware (Fake Av) and compressing files into password-secured ZIPs (Trojan.CryZip) (Table 1). Target-specific attacks and exploit kits emerged from 2012 to 2015, targeting Linux and exploring vulnerabilities through compromised websites and phishing. By 2016, there was platform diversity where targeted attacks were on MacOS and Android, while double extortion and worm-like propagation started in 2017-2018. Complexity and threat scope increased as advanced double extortion techniques were introduced, targeting both enterprise environments and individuals where VMware EZXi and Linux became regular targets.

The modern ransomware movement uses multi-platform attacks such as Windows, Linux, cloud computing, and VMware ESXi using sophisticated approaches such as brute force RDP vulnerabilities, data leaks and advanced phishing. Similarly, it was observed that ransomware was easily distributed through exploit vulnerabilities, compromised credentials, malicious emails, phishing, brute force and downloads, as indicated in Figure 7. Most of the platforms that were attacked were the Microsoft Windows system.

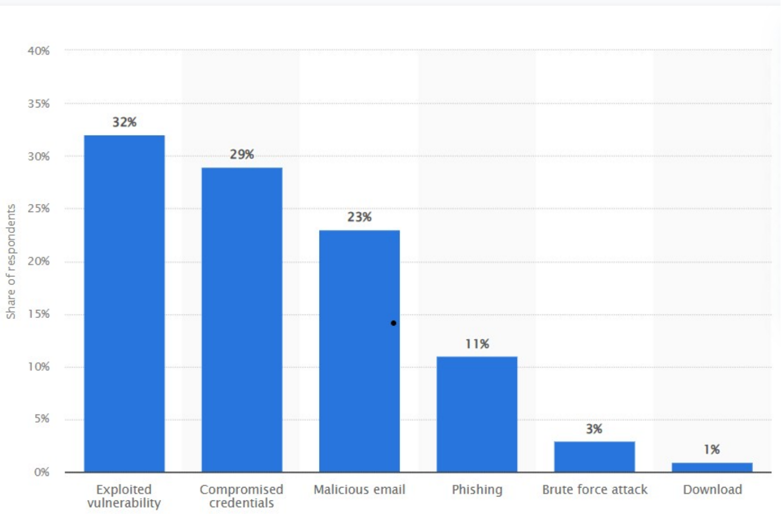

Figure 7: Sources of Ransomware in Organizations Globally (Sophos, 2024)

2.3. Categories of Ransomware

Ransomware has significantly evolved over the years and has been categorized based on its distinct characteristics and mode of operations. It is essential to understand these as categorized into the following: Locker Ransomware, Crypto-Ransomware, Ransomware–as–a–Service, Double Extortion Ransomware, Triple Extortion Ransomware, Scareware Ransomware, Mobile Ransomware, Wiper Ransomware, Cloud Ransomware, and IoT-specific Ransomware.

Locker ransomware is known for locking out users from their operating system or devices without encryption of files until a ransom is paid; an example of such is the Police-themed ransomware (Srinivasan et al., 2023) , while Crypto-ransomware will encrypt the users file and make them inaccessible until a ransom is paid to have the decryption key, instances of such is the Wannacry and Cryptolocker (Hyslip and Burruss, 2023, Kara, 2024). Similarly, Ransomware-as-a-Service is a lease or sold-as-a-service to cyber criminals which do not require technical knowledge to deploy attacks, such as Darkside and GandCrab (Seymour, 2022, Beerman et al., 2023) . Still, in the case of double extortion, it will encrypt all files and threaten to disclose the stolen data; a typical example is Maze (Kerns et al., 2022). The triple extortion technique targets third parties for extortion, while Scareware ransomware adopts fake warnings to scare victims into paying, such as antivirus pop-ups.

Mobile ransomware locks the screen or sometimes encrypts the files, and an instance is the Sypeng (Ko and Kim, 2022) and Wiper ransomware automatically deletes the victim's data; an example is Notpetya (Mos and Chowdhury, 2020). Cloud ransomware's principal target is the cloud system by exploiting the vulnerabilities and demanding ransom, while IoT-Specific ransomware aim is the vulnerabilities of IoT devices to steal their data, such as the BrickerBot (Brierley et al., 2020).

2.4. Ransomware Detection Techniques

The ransomware detection technique is a method that recognizes and counters malicious software that encrypts a victim's data in exchange for a ransom. These techniques include signature, machine learning, honeypot, endpoint detection and response. The signature-based technique compares and analyzes the files or processes against a database consisting of a list of known ransomware signature characteristics for detection. The advantage of this technique is the speed and reliability for recognized ransomware strains, but the demerit of this technique is that it is ineffective for new or polymorphic ransomware. Similarly, the machine learning detection approach uses algorithms to train the key features (static or dynamic) obtained from the ransomware activities or files; the merit of this technique is the high adaptation to new ransomware strains. However, this requires suitable datasets for training and substantial computational resources.

The honeypot detection technique uses decoy files or systems to lure ransomware and track its activities. This technique helped in giving intuition into the ransomware infection and pattern mechanisms; the disadvantage is that the system will be attacked first, which means it is reactive rather than proactive. Endpoint detection and response uses automated responses and continuous monitoring to detect and alleviate ransomware on the endpoints. The advantage of this approach is the real-time detection and quick response capabilities, but it needs cutting-edge configuration and management.

2.5. Current Mitigation Strategies for IoT Ransomware

Averting ransomware attacks on IoT devices and systems is difficult because the features of IoT devices' functionality and conception are based on constrained resources, diverse IoT environments, and connectivity. However, IoT gadgets are inseparable from modern infrastructure because their vulnerabilities make them an attractive target for ransomware. Several mitigation strategies have been designed to combat these threats, from merging network security improvements to device protection mechanisms and system architectural principles. Some effective techniques to address ransomware risks in IoT devices include device hardening, regular firmware updates and patch management, network security, Zero Trust architecture, enhanced endpoint detection and response (EDR), recovery plans and backup.

Device hardening is one of the security measures that can be integrated into the processes that take part in the IoT devices' conception phase to protect them against ransomware (Carrillo-Mondéjar et al., 2022). These include system boot processes that deny unauthorized firmware to run, secured encrypted messages to protect data while in transit and enhanced authentication to deny unauthorized access. Incorporating security in IoT from the design level would reduce the existence and exposure of such gadgets to threats. Similarly, network segmentation is another approach to secure IoT devices where the devices are isolated from infected systems to prevent further ransomware spread (Carrillo-Mondéjar et al., 2022). Deploying techniques such as intrusion detection systems (IDS) and firewalls designed specifically for IoT environments will allow real-time detection and monitoring, improving overall security.

In addition, patch management and regular firmware updates will address the vulnerabilities that ransomware can exploit. Also, endpoint detection and response (EDR) solutions are now more sophisticated, incorporating artificial intelligence and machine learning algorithms to detect and prevent anomaly behaviors that indicate ransomware (Kaur and Tiwari, 2021). When analyzing behavioral patterns, these systems can identify threats in real-time, enabling organizations to fight off attackers using the best strategies. Another effective technique to secure IoT devices is the zero-trust model that uses the principle of never trust, always verify technique. This approach strongly relies on identification, authorization, least-privilege access control and consistent monitoring which will reduce unauthorized access or ransomware within the IoT networks.

3. Key Challenges in Mitigating Ransomware in IoT Devices

The advancement of IoT devices in different sectors has provided a massive advantage, raising unique issues regarding protecting devices from ransom attacks. These challenges are inherent with IoT device limitations, diverse IoT ecosystems, and human factors precipitating vulnerabilities. In the context of IoT device limitation, the security of IoT devices depends on the kind of hardware and software built into the device. Since these are constrained devices, they cannot adopt complex technologies. Their limited capacity in processing power and memory means that it is challenging to implement key features like encryption, intrusion detection, or malware detection in real time (Al-Sharekh and Al-Shqeerat, 2019). For example, low-cost sensors often used in smart homes do not have the means to perform complex security protocols.

Further, multiple IoT manufacturers do not release firmware updates as frequently as needed, which results in the susceptibility of devices; this is especially dangerous for older IoT networks that function in industrial settings and can become targets for ransomware due to outdated software and susceptibility to malware. Moreover, IoT devices allow connection with default or basic and sometimes insufficient credentials, which are rarely changed (Angrishi, 2017). These default configurations are quickly manipulated by attackers using automated tools, thereby raising vulnerability even higher. Similarly, with Internet connections in every aspect of our daily lives, the IoT environment is quite heterogeneous regarding devices, manufacturers, operating systems, interfaces, and communication protocols.

These factors foster an environment that offers considerable predispositions to a model of security that is not standardized. Thus, most IoT devices have implementation specific to their vendors and do not follow universal standards, which can cause heterogeneity in security solutions (Fortino et al., 2018). For instance, a smart factory might have incorporated devices from several manufacturers with different security technologies, making it challenging to develop a coherent security framework for an entire smart factory. Security in IoT is influenced by several parameters, the most important of which is user behavior, which is unpredictable and uncontrollable. While using or managing the device, users and administrators often do not even bother to set their passwords to something stronger than the default 'password' or enable two-factor authentication. For instance, employees using genre devices at work may link unsecured personal devices to the IoT environment, offering attackers a way in.

Moreover, there is no adequate knowledge about the threat to security in IoT Internet of Things (IoT). Most users cannot distinguish between a genuine link or an attempt by an attacker to carry out an illegitimate operation that may jeopardize the devices and networks. In addition, IoT devices are usually resource-limited, and some organizations do not promptly maintain them once installed (Xie et al., 2022). This approach increasingly exposes devices to greater risks, as updates and security patches are not installed systematically, making them vulnerable to exploitation.

In mitigating ransomware attacks in IoT devices, the challenges must be addressed through standardization, technological innovation, and user awareness. Understanding these challenges is the key step towards developing robust IoT security architecture to tackle the ever-growing ransomware attacks.

4. Conclusion and Recommendations

Ransomware attacks on IoT devices show the importance of adopting even higher levels of cybersecurity as more devices become connected. This review has identified trends such as the increasing attack surface due to the IoT expansion, double and triple extortion tactics, and cybercriminals' exploitation of IoT weaknesses. These attacks severely affect the targeting infrastructure, healthcare, and IoT-dependent industries, resulting in extreme operational disruption, damages, and monetary and safety concerns.

Hence, to overcome these challenges, a multilayered approach to mitigating these issues is called for. This is done through device hardening with inbuilt security, segmenting and continuously monitoring the networks, backing up, and having recovery procedures in place. Techniques like zero-trust architectural models, AI-based threat identification, and user awareness are important in securing IoT devices from ransomware threats. Continuous research, innovation, and collaboration in different sectors are essential to stay abreast of the rapidly emerging ransomware landscape. Developing global standards with shared threat intelligence and cutting-edge solutions will enhance the IoT ecosystem and prevent the unrelenting and increasing ransomware threat.

5. Future Directions

The future of ransomware mitigation in IoT involves the application of modern technologies and aligning partners globally. The use of blockchain technology in improving IoT security is auspicious due to its capability to record data in a decentralized and tamper-proof manner, appending a unique identity to everything and making communications between devices more secure. The choice of blockchain-based solutions can minimize various risks connected with IoT systems reliability, especially for ransomware attacks, due to the possibility of transparent and secure identity management.

Artificial intelligence and machine learning are equally essential components of future defense. These technologies help in real-time threat detection of anomalies in data from IoT and analysis of patterns. AI is capable of learning continually to predict and work against new threats, which, as a result, makes it a sound defense barrier against ransomware. Further, post-quantum cryptography will be key with the increase in the popularity of quantum computing. Implementing quantum-resistant algorithms to IoT systems means that the systems are defendable against future computational attacks. Mitigating ransomware in an IoT environment requires global collaboration and a unified standard policy to combat this evolving ransomware threat.

References

AGGARWAL, M. Ransomware Attack: An Evolving Targeted Threat. 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023. IEEE, 1-7.

AGUILAR ANTONIO, J. M. 2024. Ransomware Gangs and Hacktivists: Cyber Threats to Governments in Latin America.

AHMED, M. 2024. *Ransomware Evolution*, CRC Press.

AL-RIMY, B. A. S., MAAROF, M. A. & SHAID, S. Z. M. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security,* 74**,** 144-166.

AL-SHAREKH, S. I. & AL-SHQEERAT, K. H. 2019. Security challenges and limitations in IoT environments. *Int. J. Comput. Sci. Netw. Secur,* 19**,** 193-199.

ALOTAIBI, F. M. & VASSILAKIS, V. G. 2021. Sdn-based detection of self-propagating ransomware: the case of badrabbit. *Ieee Access,* 9**,** 28039-28058.

ALZAHRANI, A., ALSHEHRI, A., ALSHAHRANI, H. & FU, H. 2020. Ransomware in windows and android platforms. *arXiv preprint arXiv:2005.05571*.

ANGRISHI, K. 2017. Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*.

ANUGERAH, C. A., JADIED, E. M. & CAHYANI, N. 2024. An Impact Analysis of Damage Level caused by Malware with Dynamic Analysis Approach. *International Journal on Information and Communication Technology (IJoICT),* 10**,** 90-99.

AUGUST, T., DAO, D. & NICULESCU, M. F. 2022. Economics of ransomware: Risk interdependence and large-scale attacks. *Management Science,* 68**,** 8979-9002.

BAIG, Z., MEKALA, S. H. & ZEADALLY, S. 2023. Ransomware attacks of the COVID-19 pandemic: Novel strains, victims, and threat actors. *IT Professional,* 25**,** 37-44.

BEAMAN, C., BARKWORTH, A., AKANDE, T. D., HAKAK, S. & KHAN, M. K. 2021. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security,* 111**,** 102490.

BEERMAN, J., BERENT, D., FALTER, Z. & BHUNIA, S. A review of colonial pipeline ransomware attack. 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), 2023. IEEE, 8-15.

BHARDWAJ, A. 2017. Ransomware: A rising threat of new age digital extortion. *Online banking security measures and data protection.* IGI Global.

BRIERLEY, C., PONT, J., ARIEF, B., BARNES, D. J. & HERNANDEZ-CASTRO, J. PaperW8: an IoT bricking ransomware proof of concept. Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020. 1-10.

CARRILLO-MONDÉJAR, J., TURTIAINEN, H., COSTIN, A., MARTÍNEZ, J. L. & SUAREZ-TANGIL, G. 2022. Hale-iot: Hardening legacy internet of things devices by retrofitting defensive firmware modifications and implants. *IEEE Internet of Things Journal,* 10**,** 8371-8394.

CARTWRIGHT, A. J. 2023. The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing,* 37**,** 1123-1132.

CEN, M., JIANG, F., QIN, X., JIANG, Q. & DOSS, R. 2024. Ransomware early detection: A survey. *Computer Networks,* 239**,** 110138.

CHUI, M., COLLINS, M. & PATEL, M. 2021. The Internet of Things: Catching up to an accelerating opportunity.

DENHAM, B. & THOMPSON, D. R. Analysis of Decoy Strategies for Detecting Ransomware. 2023 IEEE Conference on Communications and Network Security (CNS), 2023. IEEE, 1-6.

ELIANDO, E. & WARSITO, A. B. 2023. LockBit Black Ransomware On Reverse Shell: Analysis of Infection. *CogITo Smart Journal,* 9**,** 228-240.

FORTINO, G., SAVAGLIO, C., PALAU, C. E., DE PUGA, J. S., GANZHA, M., PAPRZYCKI, M., MONTESINOS, M., LIOTTA, A. & LLOP, M. 2018. Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach. *Integration, interconnection, and interoperability of IoT systems***,** 199-232.

GAJJAR, A., KASHYAP, P., AYSU, A., FRANZON, P., CHOI, Y., CHENG, C., PEDRETTI, G. & IGNOWSKI, J. 2024. RD-FAXID: Ransomware Detection with FPGA-Accelerated XGBoost. *ACM Transactions on Reconfigurable Technology and Systems*.

GÓMEZ HERNÁNDEZ, J. A., GARCÍA TEODORO, P., MAGÁN CARRIÓN, R. & RODRÍGUEZ GÓMEZ, R. 2023. Crypto-ransomware: A revision of the state of the art, advances and challenges. *Electronics,* 12**,** 4494.

HYSLIP, T. S. & BURRUSS, G. W. 2023. Ransomware. *Handbook on Crime and Technology.* Edward Elgar Publishing.

JABID, T., MASUM, S., SHAMS, R. A., CHOWDHURY, A., ISLAM, M. M., FERDAUS, M. H., ALI, M. S. & ISLAM, M. 2025. A Brief History of Ransomware. *Ransomware Evolution.* CRC Press.

KARA, İ. 2024. Analyzing TorrentLocker Ransomware Attacks: A Real Case Study. *Sakarya University Journal of Science,* 28**,** 774-781.

KAUR, B., DADKHAH, S., SHOELEH, F., NETO, E. C. P., XIONG, P., IQBAL, S., LAMONTAGNE, P., RAY, S. & GHORBANI, A. A. 2023. Internet of things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things,* 22**,** 100780.

KAUR, H. & TIWARI, R. Endpoint detection and response using machine learning. Journal of Physics: Conference Series, 2021. IOP Publishing, 012013.

KERNS, Q., PAYNE, B. & ABEGAZ, T. Double-extortion ransomware: A technical analysis of maze ransomware. Proceedings of the Future Technologies Conference (FTC) 2021, Volume 3, 2022. Springer, 82-94.

KESHAVARZI, M. & GHAFFARY, H. R. 2020. I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review,* 36**,** 100233.

KIM, D. & LEE, J. 2020. Blacklist vs. whitelist-based ransomware solutions. *IEEE Consumer Electronics Magazine,* 9**,** 22-28.

KIM, G., KANG, S., BAEK, S., KIM, K. & KIM, J. 2024. A Method for Decrypting Data Infected with Rhysida Ransomware. *arXiv preprint arXiv:2402.06440*.

KIM, G. Y., PAIK, J.-Y., KIM, Y. & CHO, E.-S. 2022. Byte frequency based indicators for crypto-ransomware detection from empirical analysis. *Journal of Computer Science and Technology,* 37**,** 423-442.

KO, M.-H. & KIM, D. 2022. Trends in Mobile Ransomware and Incident Response from a Digital Forensics Perspective.

LEE, J., YUN, J. & LEE, K. 2024. A Study on Countermeasures against Neutralizing Technology: Encoding Algorithm-Based Ransomware Detection Methods Using Machine Learning. *Electronics,* 13**,** 1030.

LIU, C., LI, B., ZHAO, J., FENG, W., LIU, X. & LI, C. 2023. A2-CLM: Few-Shot Malware Detection Based on Adversarial Heterogeneous Graph Augmentation. *IEEE Transactions on Information Forensics and Security*.

MALIK, P. K., SHARMA, R., SINGH, R., GEHLOT, A., SATAPATHY, S. C., ALNUMAY, W. S., PELUSI, D., GHOSH, U. & NAYAK, J. 2021. Industrial Internet of Things and its applications in industry 4.0: State of the art. *Computer Communications,* 166**,** 125-139.

MCELHINNEY, D. & CURRAN, K. 2020. The Rise of Ransomware Aided by Vulnerable IoT Devices. *Security and Organization within IoT and Smart Cities.* CRC Press.

MCINTOSH, T., KAYES, A., CHEN, Y.-P. P., NG, A. & WATTERS, P. 2021. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR),* 54**,** 1-36.

MINNAAR, A. & HERBIG, F. J. 2021. Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology,* 34**,** 155-185.

MOGAGE, A. & LUCANU, D. 2024. Towards Logical Specification and Checking of Evasive Malware.

MOHAMMAD, A. H. 2020. Analysis of ransomware on windows platform. *International Journal of Computer Science and Network Security,* 20**,** 21-27.

MORAN STRITCH, M., WINTERBURN, M. & HOUGHTON, F. 2021. The Conti ransomware attac k on healthcare in Ireland: Exploring the impacts of a cybersecurity breach from a nursing perspective. *Canadian Journal of Nursing Informatics,* 16.

MOS, M. A. & CHOWDHURY, M. M. The growing influence of ransomware. 2020 IEEE International Conference on Electro Information Technology (EIT), 2020. IEEE, 643-647.

NAGAR, G. 2024. The evolution of ransomware: tactics, techniques, and mitigation strategies. *International Journal of Scientific Research and Management (IJSRM),* 12**,** 1282-1298.

NICHO, M., YADAV, R. & SINGH, D. 2023. Analyzing WhisperGate and BlackCat Malware: Methodology and Threat Perspective. *International Journal of Advanced Computer Science and Applications,* 14.

NIVEDITHA, V. S., KUNWAR, R. S. & KUMAR, K. 2024. Ransomware attacks on IoT devices. *Advanced Techniques and Applications of Cybersecurity and Forensics.* Chapman and Hall/CRC.

OBAIDAT, M. A., OBEIDAT, S., HOLST, J., AL HAYAJNEH, A. & BROWN, J. 2020. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers,* 9**,** 44.

OTHMAN, K. A. K. & ZOLKIPLI, M. F. 2021. Survey on Technique to Prevent Ransomware Attack. *Borneo International Journal eISSN 2636-9826,* 4**,** 12-18.

OZ, H., ARIS, A., LEVI, A. & ULUAGAC, A. S. 2022. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR),* 54**,** 1-37.

PARK, J. H., SINGH, S. K., SALIM, M. M., AZZAOUI, A. E. & PARK, J. H. 2022. Ransomware-based cyber attacks: A comprehensive survey. *Journal of Internet Technology,* 23**,** 1557-1564.

PLOSZEK, R., ŠVEC, P. & DEBNÁR, P. 2021. Analysis of encryption schemes in modern ransomware. *Rad Hrvatske akademije znanosti i umjetnosti. Matematičke znanosti***,** 1-13.

PREVEZIANOU, M. F. 2021. Wannacry as a creeping crisis. *Understanding the Creeping Crisis.* Springer International Publishing Cham.

RAHEEM, A., RAHEEM, R., CHEN, T. M. & ALKHAYYAT, A. Estimation of ransomware payments in bitcoin ecosystem. 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2021. IEEE, 1667-1674.

RANA, M. U., SHAH, M. A., ALNAEEM, M. A. & MAPLE, C. 2024. Ransomware Attacks in Cyber-Physical Systems: Countermeasure of Attack Vectors Through Automated Web Defenses. *IEEE Access*.

RAZAULLA, S., FACHKHA, C., MARKARIAN, C., GAWANMEH, A., MANSOOR, W., FUNG, B. C. & ASSI, C. 2023. The age of ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access,* 11**,** 40698-40723.

REN, A., LIANG, C., HYUG, I., BROH, S. & JHANJHI, N. 2020. A three-level ransomware detection and prevention mechanism. *EAI Endorsed Transactions on Energy Web,* 7.

ROUTRAY, S., PRUSTI, D. & RATH, S. K. Ransomware attack detection by applying machine learning techniques. Machine Intelligence Techniques for Data Analysis and Signal Processing: Proceedings of the 4th International Conference MISP 2022, Volume 1, 2023. Springer, 765-776.

SCHODER, D. 2018. Introduction to the Internet of Things. *Internet of things A to Z: technologies and applications***,** 1-50.

SETH, R., SHARAFF, A., CHATTERJEE, J. M. & JHANJHI, N. 2022. Ransomware Attack: Threats & Different Detection Technique. *Information Security Handbook.* CRC Press.

SEYMOUR, W. 2022. Examining Trends and Experiences of the Last Four Years of Socially Engineered Ransomware Attacks.

SHARMA, N. & SHANKER, R. Analysis of ransomware attack and their countermeasures: A review. 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022. IEEE, 1877-1883.

SHEEN, S. & GAYATHRI, S. Early Detection of Android Locker Ransomware Through Foreground Activity Analysis. Proceedings of Third International Conference on Communication, Computing and Electronics Systems: ICCCES 2021, 2022. Springer, 921-932.

SIMAIYA, S., LILHORE, U. K., SHARMA, S. K., GUPTA, K. & BAGGAN, V. 2020. Blockchain: A new technology to enhance data security and privacy in Internet of things. *Journal of Computational and Theoretical Nanoscience,* 17**,** 2552-2556.

SONICWALL. 2024. *Annual Number of Ransomware Attempts Worldwide from 2017 to 2023* [Online]. Available: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/ [Accessed January 04 2025].

SOPHOS. 2024. *Root causes of ransomware attacks in organizations worldwide as of February 2024* [Online]. Available: https://www.statista.com/statistics/1410445/cause-ransomware-attacks-global/ [Accessed January 04 2025].

SRINIVASAN, D., RS, S. K. & NAVALADI, V. N. Analysis of Cyber Threats and Security Auditing. 2023 Fourth International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), 2023. IEEE, 1-5.

STADDON, E., LOSCRI, V. & MITTON, N. 2021. Attack categorisation for IoT applications in critical infrastructures, a survey. *applied sciences,* 11**,** 7228.

SULTAN, H., KHALIQUE, A., ALAM, S. I. & TANWEER, S. 2018. A SURVEY ON RANSOMEWARE: EVOLUTION, GROWTH, AND IMPACT. *International Journal of Advanced Research in Computer Science,* 9.

SUN, Y. & JUNG, H. 2024. Machine Learning (ML) Modeling, IoT, and Optimizing Organizational Operations through Integrated Strategies: The Role of Technology and Human Resource Management. *Sustainability,* 16**,** 6751.

THREATLABZ. 2023. *Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report* [Online]. Available: https://info.zscaler.com/resources-industry-reports-threatlabz-2023-enterprise-ioT-ot-threat-report [Accessed 10th January 2025].

TUUNAINEN, T. 2021. White Hat hacking: system and application security focusing on its fundamentals, malware and Wi-Fi vulnerability.

UMAR, R., RIADI, I. & KUSUMA, R. S. 2021. Mitigating sodinokibi ransomware attack on cloud network using software-defined networking (SDN). *International Journal of Safety and Security Engineering,* 11**,** 239-246.

UPADHYAY, A. K., DUBEY, P., GANDHI, S. & JAIN, S. 2025. State‐of‐the‐Art in Ransomware Analysis and Detection. *Emerging Threats and Countermeasures in Cybersecurity*, 111-135.

WANI, A. & REVATHI, S. 2020. Ransomware protection in loT using software defined networking. *Int. J. Electr. Comput. Eng,* 10, 3166-3175.

WESTBROOK, A. D. 2021. A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets and Defending National Security. *NYUJL & Bus.,* 18, 391.

XIE, Y., GUO, Y., MI, Z., YANG, Y. & OBAIDAT, M. S. 2022. Edge-assisted real-time instance segmentation for resource-limited iot devices. *IEEE Internet of Things Journal,* 10, 473-485.

YAMANY, B., ELSAYED, M. S., JURCUT, A. D., ABDELBAKI, N. & AZER, M. A. 2022. A new scheme for ransomware classification and clustering using static features. *Electronics,* 11, 3307.

YE, J., DE CARNAVALET, X. D. C., ZHAO, L., ZHANG, M., WU, L. & ZHANG, W. Exposed by Default: A Security Analysis of Home Router Default Settings. Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, 2024. 63-79.

YOUNG, C., MCARDLE, R., LE-KHAC, N.-A. & CHOO, K.-K. R. 2020. Forensic investigation of ransomware activities—Part 1. *Cyber and Digital Forensic Investigations: A Law Enforcement Practitioner's Perspective*, 51-77.

ZHANG, H., ZHAO, L., YU, A., CAI, L. & MENG, D. 2024. Ranker: Early Ransomware Detection through Kernel-level Behavioral Analysis. *IEEE Transactions on Information Forensics and Security*.

ZIMBA, A., WANG, Z., CHEN, H. & MULENGA, M. 2019. Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks. *KSII Transactions on Internet and Information Systems (TIIS),* 13, 3258-3279.