International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Detecting Ransomware Attacks on IoT Platforms Using Multisource Transfer Learning: A Review

***Yazid Ibrahim Isah[1], Badamasi Imam Ya'u[2], Kabiru Musa Ibrahim[3], Abdulmutalib Abdullahi[4] & Ismail Zahraddeen Yakubu[5]***

[1,2,4]*Department of Mathematical Science, Abubakar Tafawa Balewa University, Bauchi*
[3]*Department of Informatiom Management, Abubakar Tafawa Balewa University, Bauchi*
[5]*Department of Computing Technologies, SRM Institute of Science and Technology, Chennai, India*

**ABSTRACT**

The rapid expansion of Internet of Things (IoT) devices has led to increased vulnerability to ransomware attacks, posing significant security challenges. This review paper explores the use of deep transfer learning to enhance ransomware detection on IoT platforms. Traditional security measures often struggle to effectively detect and mitigate ransomware in the heterogeneous and resource-constrained environment of IoT. Deep transfer learning, particularly leveraging Convolutional Neural Networks (CNNs), addresses this challenge by transferring knowledge from pre-trained models to new tasks, improving detection accuracy with limited data. This paper is structured into four sections: Introduction, Related Work, Research Gap, and Conclusion and Future Work, providing a comprehensive overview of the current state of research and identifying potential areas for future investigation. By examining existing literature and highlighting key research gaps, we aim to pave the way for robust and scalable solutions to enhance the security of IoT systems against ransomware threats.

Keywords: Ransomware Detection, IoT Security, Deep Transfer Learning, Convolutional Neural Networks (CNNs) & Cybersecurity.

## 1. INTRODUCTION

Ransomware attacks have emerged as a significant cybersecurity threat, exploiting vulnerabilities in systems and encrypting critical data until a ransom is paid (Teichmann, Boticiu, & Sergi, 2023). Detecting ransomware in real-time across various platforms is challenging due to the rapid evolution of ransomware variants and their ability to evade traditional detection methods (Teichmann et al., 2023). The increased reliance on digital technology has not only improved our lifestyles and businesses but also introduced several security threats. Among these, malware has dramatically grown in prevalence, persistently striking cyberspace and causing damage to individuals and organizations worldwide (Hansen, Larsen, Stevanovic, & Pedersen, 2016).

Ransomware, a type of malware that restricts access to resources on an infected device until a ransom is paid, often in cryptocurrency, has recently penetrated various sectors, including education, healthcare, business, research, and information technology (Möller, 2023). Unlike traditional malware, eradicating ransomware is problematic, and the damage imposed is often irreversible even after removal (Al-rimy, Maarof, & Shaid, 2018). Consequently, cybersecurity has become a crucial concern, attracting researchers and industries to find effective defensive solutions (Pluskal, 2015).

Ransomware has grown in complexity, adversity, and multiplicity, becoming one of the most destructive malware trends (Lang, Connolly, Taylor, & Corner, 2023; Shaukat & Ribeiro, 2018). Cisco's annual security report reveals that ransomware is growing at an annual rate of over 300 percent (King, 2017). Despite its longstanding presence, ransomware variants have evolved, enhancing their proliferation, evasion, and file encryption capabilities, compelling victims to pay ransoms. There are over 200 active ransomware families, including Tescrypt, Crowti, Cerber, and Locky (Lu et al., 2017). Symantec's report indicated a 46% increase in ransomware variants in 2017 (Symantec, 2019).

The earliest known ransomware, AidsInfo, was discovered in 1989. However, the lack of an enabling environment and untraceable payment methods initially rendered ransomware less appealing to cybercriminals (Savage, Coogan, & Lau, 2015). Although early ransomware attacks were rudimentary and had flaws, they set the stage for the sophisticated attacks seen today (Jacob, 2023). The first wave of modern ransomware began in 2005 (Savage et al., 2015), and since then, ransomware has rapidly advanced, with numerous novel families emerging (H. Zhang et al., 2019). The frequency of ransomware attacks has increased fourfold recently, with 4,000 attacks occurring daily and causing an estimated $1 billion in damages in 2016 (Druva, 2017).

Ransomware attacks negatively impact businesses relying on information technology infrastructure (Chiong, 2023). The effects include data damage due to file encryption, downtime caused by system shutdowns, financial costs for incident response, and other security-related challenges, potentially even leading to intellectual property theft and loss of life due to the sudden shutdown of critical healthcare equipment (Andronio, Zanero, & Maggi, 2015; Gómez-Hernández, Álvarez-González, & García-Teodoro, 2018).

Researchers have proposed numerous approaches to detect and defend against ransomware attacks, striving to find lasting solutions (Chen et al., 2017; Cusack, Michel, & Keller, 2018; Daku et al., 2018). However, ransomware continues to evolve, employing various proliferation and evasion methods to circumvent defensive mechanisms (Lamers, Spoerl, Levey, Choudhury, & Ahmed, 2023; Damshenas, Dehghantanha, & Mahmoud, 2013). New protection techniques are essential to detect and prevent ransomware before it causes destruction (Guvçi & Şenol, 2023).

Machine learning algorithms have been proven to solve real-world problems across different domains (Herrera-Silva & Hernández-Álvarez, 2023). Their ability to learn from data and adapt to new situations has made them suitable for ransomware detection. Deep learning techniques, particularly Convolutional Neural Networks (CNNs), have shown promise in detecting complex patterns in data (Gibert, Mateu, & Planes, 2020). However, training deep learning models from scratch requires large amounts of labeled data, which may not be readily available for all platforms and ransomware variants. Transfer learning addresses this challenge by leveraging pre-trained models to improve performance on new tasks with limited data. This paper explores the use of deep transfer learning for enhancing ransomware detection on IoT platforms, aiming to provide a comprehensive overview of current research and identify potential areas for future investigation.

## 2. LITERATURE REVIEW

In this study, we propose a dedicated comprehensive survey on the applications of machine learning defensive solutions to ransomware attacks. The survey is in three perspectives: (1) Technical perspective of the machine learning algorithms found to be applied to detect ransomware attacks. (2) The applications of the machine learning intelligent algorithms in providing solutions to ransomware attacks. (3) Synthesis and analysis of the literature.

### *2.1 Overview of Ransomware: Background, Motivation and Target Platforms*

Ransomware is a devastating cyber threat with global damage costing individuals and organisations enormous forfeiture of assets (Lamers et al., 2023). Ransomware is defined as the malware that denied user access to their devices or denied access to files (Bello et al., 2021). The access to the device or file is allowed after a ransom is paid by the victim. Some common examples of ransomware are as follows: Locky, Cryptolocker, CTB Locker, Cryptowall, Teslacrypt, Winlocker, Torrentlocker, among others. (Verma et al., 2018). Ransomware attacks target various platforms including PCs, mobile devices, IoT devices, wearable devices, and cloud productivity to demand ransomware from individuals and organisations (Al-rimy et al., 2018). Recently, ransomware attacks have drastically increased to encompass IoT devices, mobile platforms including Android, and other internet-enabled devices (Chaudhary, Aujla, Kumar, & Zeadally, 2018; J. Chen et al., 2017; Lachtar, Ibdah, & Bacha, 2019; Muna, den Hartog, & Sitnikova, 2019; Villalba, Orozco, Vivar, Vega, & Kim, 2018). Thus, ransomware has dominated cybercrime reports in 2018, with its threat targeting both individuals and businesses (Berrueta, Morato, Magaña, & Izal, 2019). However, not only individuals are susceptible to ransomware attacks, organisations and business entities are not spired regardless of the proactive countermeasures being practiced.

The motive for ransomware attacks is virtually always monetary. Contrasting other types of malware attacks, ransomware-based attacks usually notified the victim that an exploit has occurred and is given instructions for how to recover from the attack. However, untraceable crypto currencies, like Bitcoin, Monero, etc. are the most widely ransom payment modes required by cybercriminals to hide their identity. Generally, a time limit is assigned for payment, if the deadline exceeds, the ransom demand multiplies or files are damaged or permanently locked. Cybercrime has changed landscape from a world of maverick attackers to a criminal business that generate huge revenue through extortion (Lee, Kim, & Kim, 2019; O'Kane, Sezer, & Carlin, 2018; Su, Liu, Wang, & Wang, 2018). Thus, the time, data loss, and possible intellectual property theft that may be caused on the victim made ransomware attacks irreversible (Digital Guardian, 2019).

Although ransomware extort users and businesses for monetary benefit, however, the malicious program must gain access to the resources before holding it for ransom (Herrera-Silva & Hernández-Álvarez, 2023). This access happens through infection or attack vectors. Email attachments, email links messages, compromised websites and online pop-ups are the most common deception used to distribute ransomware (Kok et al., 2019). In addition, drive-by freeware apps, exploit kits, brute-force authentication credentials, Trojan botnet attacks or social engineering techniques (Bhardwaj, Avasthi, Sastry, & Subrahmanyam, 2016). Therefore, ransomware compromises the availability, confidentiality, and integrity of a victim's system (Javaheri, Hosseinzadeh, & Rahmani, 2018).

In 2005, the notable trend of modern ransomware has grown in full swing (Savage et al., 2015). Various enablers, comprising undetectable payment methods, availability of cryptographic techniques, financial benefit, free development kits, and easy to use ransomware-as-a-service (RaaS) cloud services are the core contributors to the high rate of ransomware attacks (Lang et al., 2023). These enablers promote the advent of new advanced families of ransomware (Shukla, Mondal, & Lodha, 2016).

Moreover, ransomware exploits system flaws such as remote code vulnerability, windows server message block to invade the system (National Vulnerability Databasa, 2017). Many search techniques such as depth-first, file size and file location in the tree hierarchy are often leveraged to trace user-related files in the victim's system (Scaife, Carter, Traynor, & Butler, 2016). Some ransomware families trace recently, access files and encrypt them consecutively. While others render the entire drive inaccessible one time by simply encrypting the master file table. (Ahmadian & Shahriari, 2016). Ransomware usually scrambled specific types of file such as .xls, .doc, .pdf, .jpg, .zip, and other critical business-related file types, like CAD files, database files, and website files (Lu et al., 2017). Ransomware has improved in complexity to hinders reverse engineering techniques by engaging emulation detection, advanced obfuscation, delayed dynamic code loading techniques (Martín, Hernandez-Castro, & Camacho, 2018; Min et al., 2018).

### *2.2 Intelligent Algorithms Applied for detecting ransomware*

The devised taxonomy in Figure 1 depicts the application of intelligent algorithms for the detection of ransomware. The taxonomy categorises the intelligent algorithms into traditional machine learning algorithms and deep learning algorithms. The traditional machine learning algorithms are further classified as either Random Forest (RF), Decision Tree (DT) and other algorithms. The RF shows capability in the detection of ransomware in Windows OS, virtual environment, PC, and Android OS (Bae, Lee, & Im; Cohen & Nissim, 2018; Cusack et al., 2018b; Scalas et al., 2019).

The DT show performance in the detection of ransomware in Windows OS, real-time environment, and network (O. M. K. Alhawi, J. Baldwin, & A. Dehghantanha, 2018; Daku et al., 2018; Wan et al., 2018). Other algorithms include V-detector Negative Selection algorithm with Mutation Optimization and Gradient Tree Boosting algorithm for the detection of ransomware in virtual environment (Lu et al., 2017; Shaukat & Ribeiro, 2018). Random Tree autonomously with Bayes Net algorithm show capability in the detection of ransomware in network environment (Almashhadani et al., 2019).

In addition, Softmax algorithm shows effectiveness in the detection of ransomware in an application (Homayoun et al., 2019). Complex Tree shows competence in detection of ransomware in real-time environment (Verma et al., 2018). Also, iBagging algorithm shows capability in the detection of ransomware in PC (Al-rimy et al., 2019). Lastly, Naïve Bayes shows effectiveness in the detection of ransomware in healthcare system (Fernandez Maimo et al., 2019).

However, deep neural network with batch normalization (DNN-BN) shows effectiveness in the detection of ransomware Industrial Internet of Things (IIoT) (Al-Hawawreh & Sitnikova, 2019). Improved LSTM and SA-CNN show capability in the detection of ransomware in windows environment (Agrawal et al., 2019; B. Zhang et al., 2019). Likewise, deep belief network (DBN) shows competence in the detection of ransomware in Field Programmable Gate Array (FPGA) (Alrawashdeh & Purdy, 2018). Also, Long Short-Term Memory, RanSD and deep learning model show effectiveness in the detection of ransomware in virtual environment (Ashraf et al., 2019; Maniath et al., 2017; Sharmeen et al., 2020). Deep neural network show capability in the detection of ransomware in twitter platform (Vinayakumar et al., 2019). Multi-Layer Perceptron (MLP) show effectiveness in the detection of ransomware in PC (Vinayakumar et al., 2017). LSTM show competence in the detection of ransomware in Android and virtual environments (Bibi et al., 2019; Maniath et al., 2017). Finally, Tree-Shaped Deep Neural Network along with a Quantity Dependent Backpropagation (QDBP) shows effectiveness in the detection of ransomware in network environment (Chen et al., 2017).

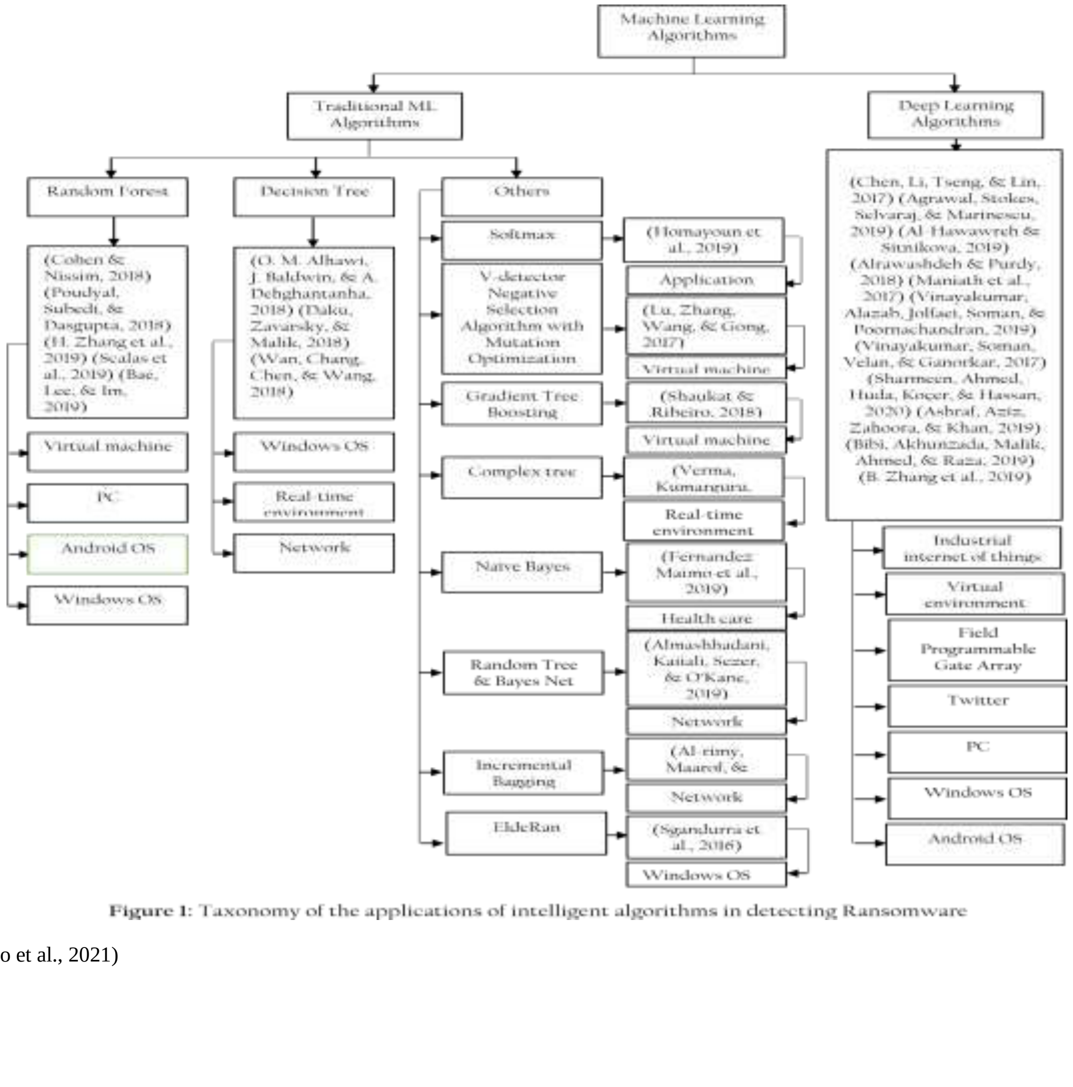
Machine Learning Algorithms
Traditional ML Algorithms
Deep Learning Algorithms
Random Forest
Decision Tree
Others
(Cohen & Nissim, 2018) (Poudyal, Subedi, & Dasgupta, 2018) (H. Zhang et al., 2019) (Scalas et al., 2019) (Bae, Lee, & Im, 2019)
(O. M. Alhawi, J. Baldwin, & A. Dehghantanha, 2018) (Daku, Zavarsky, & Malik, 2018) (Wan, Chang, Chen, & Wang, 2018)
Virtual machine
PC
Android OS
Windows OS
Windows OS
Real-time environment
Network
Softmax
(Homayoun et al., 2019)
Application
V-detector Negative Selection Algorithm with Mutation Optimization
(Lu, Zhang, Wang, & Gong, 2017)
Virtual machine
Gradient Tree Boosting
(Shaukat & Ribeiro, 2018)
Virtual machine
Complex tree
(Verma, Kumaraguru,
Real-time environment
Naive Bayes
(Fernandez Maimo et al., 2019)
Health care
Random Tree & Bayes Net
(Almashhadani, Kaiiali, Sezer, & O'Kane, 2019)
Network
Incremental Bagging
(Al-rimy, Maarof, &
Network
EldeRan
(Sgandurra et al., 2016)
Windows OS
(Chen, Li, Tseng, & Lin, 2017) (Agrawal, Stokes, Selvaraj, & Marinescu, 2019) (Al-Hawawreh & Sitnikova, 2019) (Alrawashdeh & Purdy, 2018) (Maniath et al., 2017) (Vinayakumar, Alazab, Jolfaei, Soman, & Poornachandran, 2019) (Vinayakumar, Soman, Velan, & Ganorkar, 2017) (Sharmeen, Ahmed, Huda, Kocer, & Hassan, 2020) (Ashraf, Aziz, Zahoora, & Khan, 2019) (Bibi, Akhunzada, Malik, Ahmed, & Raza, 2019) (B. Zhang et al., 2019)
Industrial internet of things
Virtual environment
Field Programmable Gate Array
Twitter
PC
Windows OS
Android OS

**Figure 1**: Taxonomy of the applications of intelligent algorithms in detecting Ransomware

Source: (Bello et al., 2021)

### *2.4 Related Work*

This section provides literture that apply deep learning algorithm for the detection of ransomware. For example, (Al-Hawawreh & Sitnikova, 2019) proposed a hybrid model based on Classical Auto-Encoder (CAE), Variational Auto-Encoder (VAE) and Deep Neural Network with Batch Normalization (DNN-BN) to detect ransomware in industrial internet of things (IIoT). The CEA and VEA are simultaneously used to reduce the dimension of data and extract features. The new generated features are used to train and test the proposed classifier (DNN-BN). The DNN-BN performs better than RF, DT, LR, SVM and DNN when train and tested with the same data. The model is trained with less data samples, this can hinder the performance of the model. It does not address the problem of classifying multiple ransomware families.

(Agrawal et al., 2019) proposed an improved Long Short-Term Memory (LSTM) to detect ransomware in Windows environment. Attended recent input cell was incorporated with LSTM to integrate attention learning for ransomware sequences. The ARILSTM performs better than the standard LSTM. Only a known target label and input event sequences are utilized to train the model in end-to-end fashion.

(Alrawashdeh & Purdy, 2018) proposed a four-layer Deep Belief Network (DBN) model based on Restricted Boltzmann Machine (RBM) using Memory-Assisted-Stochastic-Dynamic-Fixed-Point arithmetic to detect ransomware in Field Programmable Gate Array (FPGA). The technique stores random bit-stream in memory to yield efficient cross-correlation for the stochastic computation in FPGA. The DBN is trained by the memory technique for stochastic computation with dynamic fixed-point arithmetic. The memory-based cross-correlation reduction outperforms Hybrid Stochastic Dynamic Fixed-Point (HSDFP) and the dynamic fixed-point methods. The model is not train on large dataset and cannot detect a zero-day ransomware in (FPGA).

(Maniath et al., 2017) proposed a model based on Long-Short Term Memory (LSTM) to detect ransomware behaviour for binary sequence classification of API calls. The method uses dynamic malware analysis of the ransomware to extract the API calls in sequence. The LSTM uses the API sequences generated to classify the samples.  The proposed model performs better than RNN, DBN, Auto-Encoder (AE), RNN and Echo State Networks (ESN). The malware may misbehave to hide its features in the execution environment. It uses dataset with less number of ransomware samples and benign executables.

(Vinayakumar, Alazab, Jolfaei, Soman, & Poornachandran, 2019) proposed a model based on Deep Neural Network (DNN) to classify ransomware tweets to their respective families. The method analyzes tweets from twitter posts to extract optimal features. The extracted features are then passed to the classification algorithm. The results show that the proposed model outperforms SVM, and NB. The paper exclusively considers twitter among numerous social media platforms.

(Vinayakumar, Soman, Velan, & Ganorkar, 2017) proposed a model based on Multi-Layer Perceptron (MLP) to evaluate the effectiveness of shallow and deep networks for detection and classification of ransomware. The method passes the EXE files to the simulated environment and stores the detailed characteristics of ransomware samples in the sandbox logs. API calls are selected as features and passed as input to the MLP and some shallow models for learning to detect and classify ransomware. The results show that MLP outperforms NR, NB, DT, RF, KNN and SVM. The ransomware may not reveal their actual intent in the simulated environment.

(Sharmeen, Ahmed, Huda, Koçer, & Hassan, 2020) proposed a deep learning model for avoiding ransomware threat extortion. The method mines the intrinsic features from the different unlabeled ransomware samples. Then the unsupervised learned model is pooled with supervised classification to build an adaptive detection model. The actual ransomware data is leveraged to validate the framework with dynamic analysis testbed. The results show that the proposed model outperforms SVM, RF, and Multi class classifier. The model is trained with a smaller number of datasets.

(Bibi, Akhunzada, Malik, Ahmed, & Raza, 2019) proposed Long Short-Term Memory (LSTM) model to Android ransomware through multi-factor feature infiltration. The method leverages 8 different machine learning filtration technique to extract essential features. The deep learning-based model is used to detect malicious behaviour of Android applications. The proposed model outperforms with 97.08% detection accuracy. the model only predicts the malware, but there is no comparison made with other algorithms.

(Ashraf et al., 2019) proposed Ransomware Static and Dynamic Analysis (RanSD) for ransomware detection analysis using feature engineering and deep neural networks. The method extracts feature from the collected samples. Then the extracted features are analysed to extract relevant features and sequence for classification. Finally, the effectiveness of the selected features is validated on conventional learning model and deep learning based on transfer learning. The proposed model outperforms with dynamic dataset compared to static dataset. The proposed model only analyses the detection of ransomware using static features and dynamic features.

(B. Zhang et al., 2019) proposes Self-Attention Convolution Neural Network (SACNN) to detect ransomware. The feature vectors were generated from the sequences of N-gram. The self-attention captures valuable information from opcodes. The sequence of N-gram is partitioned. The SA-CNNs is combined with bi-directional selfattention network. The SA-CNN is applied to detect the ransomware and result indicated that the proposed model outperformed KNN, NB and DT algorithms. Advanced packing techniques may not be handled by the static analysis.

(Chen et al., 2017) proposes a TreeShaped Deep Neural Network (TSDNN) with Quantity Dependent Backpropagation (QDBP) algorithm to detect malicious flow including ransomware in a network. The TSDNN model uses behaviour-oriented approach to classify the data in layer-wise manner. Subsequently, the QDBP incorporating the knowledge of the disparity among classes. The results show that the proposed algorithm outperforms the signature-based method in detecting the ransomware. The network behaviour of the malicious samples might not be well-captured within the threshold of six minutes.

(Alam et al., 2021) proposed a Deep Learning based Malware Images Classification and evaluate with AlexNet, VGG-16, ResNet-50, Inceptionv3 model. The trained models allow accurate classification of malware and report a test accuracy of 98.90. however, the performance was limited to single platform

(Rustam, Ashraf, Jurcut, Bashir, & Zikria, 2023) proposed Malware Detection using Image Representation of Malware Data and Transfer Learning and evaluate it using VVG-16 and ResNet-50. With the Bi-model structure, 100% accuracy is obtained for a 25 classes problem. However, the performance was subject to single platform

(Polsani & Jiang, 2023) proposed deep learning and transfer learning and evaluate it with Convolutional Neural (CNN), VGG16, EfficientNet, and Vision Transformers (ViT). The Vision Transformers model achieved the highest accuracy and demonstrated strong classification capabilities across various malware families. However, the study fails to expand the grayscale image analysis to further enhance the model's performance

(Yaseen, Aslam, Farhan, Naeem, & Raza, 2023) proposed a new system for classifying malware into families by transforming malware binaries into grayscale images and applying convolutional neural network. The approach represents a significant advancement in the field of malware classification. However, training the CNN from scratch result in high computational cost and less precision. Hence, these limitations were extensively address in this study. Table 2.1 depict the summary of the applications of deep learning architecture to detect malware detection.

Table 1: The summary of the applications of deep learning architecture to detect ransomware

| Authors | Proposed Method | Evaluation Method | Findings | Limitation |
|---|---|---|---|---|
| (Al-Hawawreh & Sitnikova, 2019) | (DNN-BN) | RF, DT, LR, SVM and DNN | The DNN-BN performs better than RF, DT, LR, SVM and DNN when train and tested with the same data. | The model is trained with less data samples, this can hinder the performance of the model. It does not address the problem of classifying multiple ransomware families. |
| (Agrawal et al., 2019) | ARI-LSTM | LSTM | The ARI-LSTM performs better than the standard LSTM. | Only a known target label and input event sequences are utilized to train the model in end-to-end fashion. |
| (Alrawashdeh & Purdy, 2018) | DBN | HSDFP, DFP, and Memorybased crosscorrelation reduction | The memory-based cross-correlation reduction outperforms (HSDFP) and the dynamic fixed-point methods. | The model is not train on large dataset and cannot detect a zero-day ransomware in (FPGA) |
| (Maniath et al., 2017) | LSTM | RNN, AE, DBN and RNN & ESN | The results show that the LSTM performs better than KNN, SVM, DBN, and RNN | The malware may misbehave to hide its features in the execution environment |
| (Vinayakumar et al., 2019) | DNN | SVM | The results show that the DNN performs better than SVM. | The paper exclusively considers twitter among numerous social media platforms. |
| (Vinayakumar et al., 2017) | MLP | NR, NB, DT, RF, KNN and SVM | The results show that MLP outperforms NR, NB, DT, RF, KNN and SVM | The ransomware may not reveal their actual intent in the simulated environment. |
| (Sharmeen et al., 2020) | Deep learningbased model | SVM, RF, Multi-class classifier | The results show that the proposed model outperforms SVM, RF, and Multi class classifier. | The model is trained with a less number of dataset. |

| | | | | |
|---|---|---|---|---|
| (Bibi et al., 2019) | LSTM | NIL | The proposed model outperforms with 97.08% detection accuracy. | The model only predicts the malware, but there is no comparison made with other algorithms. |
| (Ashraf et al., 2019) | RanSD | SVM, RF, and ResNet-18 | The proposed model outperforms with dynamic dataset compared to static dataset. | The proposed model only analyses the detection of ransomware using static features and dynamic features. |
| (Y.-C. Chen et al., 2017) | TSDN-QDBP | Signature-based method | The results show that the proposed method outperforms the signature-based method. | The network behaviour of the malicious samples might not be well-captured within the threshold of six minutes. |
| (B. Zhang et al., 2019) | SA-CNN | KNN, NB and DT | DT perform better | Advanced packing techniques may not be handled |
| (Xiao, Li, Chen, & Li, 2020) | ML | Single Malware Detection | It was observed that there is improvement of detection rates in those fine-grained classifiers compared to a single classifier | prone to be an expensive task and is limited to small-size of dataset and code coverage |
| (Xiao et al., 2020) | deep convolutional neural networks | SVM, RF and DT | MalFCS can obtain excellent classification better results compare to the state of the art | Model Overfitting issues must be mitigated |
| (Shhadat, Hayajneh, & Al-Sharif, 2020) | Machine Learning | DT, RF and NB | achieved accuracy improvements over all binary.and multi-classifiers. The highest accuracy was achieved by DT is 98.2% for binary classification and 95.8% by RF for multi-class class | Lacks Generalization and have low precision and recall value |
| (Choi, Bae, Lee, Kim, & Kim, 2020) | Attention Base-Deep Learning | CNN and LSTM | this approach yields an accuracy that is approximately 12% and 5% higher than a conventional AI-based detection model using CNN and skip-connected LSTM-based detection model | Lacks Generalization |
| (Alam et al., 2021) | A Deep Learning based Malware Images Classification | AlexNet, VGG-16, ResNet-50, Inceptionv3 model | The trained models allow accurate classification of malware and report a test accuracy of 98.90 | Performance was limited to single platform |
| (Rustam, Ashraf, Jurcut, Bashir, & Zikria, 2023) | Malware Detection using Image Representation of Malware Data and Transfer Learning | VVG-16 and ResNet-50 | With the Bi-model structure, 100% accuracy is obtained for a 25 classes problem | Performance was subject to single platform |

| | | | | |
|---|---|---|---|---|
| (Polsani & Jiang, 2023) | deep learning and transfer learning | Convolutional Neural (CNN), VGG16, EfficientNet, and Vision Transformers (ViT) | the Vision Transformers model achieved the highest accuracy and demonstrated strong<br>classification capabilities across various malware families | Fail to expand the grayscale image analysis to further enhance the model's performance |
| (Yaseen, Aslam, Farhan, Naeem, & Raza, 2023) | a new system for<br>classifying malware into families by transforming<br>malware binaries into grayscale images and applying<br>convolutional neural network | No evaluation algorithm | The approach represents a significant advancement in the field of malware classification | Training from scratch result in high computational cost for the model |

### *2.4 Ransomware attacks dataset*

To put it straight, "*No data, No machine learning*". This section presents the sources and type of the data used in different project to build the machine learning model for detecting ransomware attacks. Table 3 present the summary of the sources and types of the data used in various projects surveyed. The sources of the data can help researchers get ransomware attacks data that are freely available to use for proposing a novel machine learning approach for detecting ransomware attacks, thereby, enhance the development of a robust system for detecting and preventing ransomware attacks.

**Table 2:** Summary of the sources and type of the ransomware data used for Modelling

| Author | Data source | Data Type |
|---|---|---|
| (O. M. Alhawi et al., 2018) | ransomwaretracker.abuse.ch and virustotal.com | Network traffic captures. |
| (Cohen & Nissim, 2018) | Virtual server snapshots | Meta- features created from Volatile memory dumps. |
| (Cusack et al., 2018a) | malwaretraffic-analysis.net | Network traffic signature. |
| (Daku et al., 2018) | virustotal.com. | Behavioral attributes |
| (Homayoun et al., 2019) | Ransomwaretracker.abuse.ch | system calls, sequence of actions taken by an application. |
| (Lu et al., 2017) | virusshare.com. | Application Programming Interface function calls. |
| (Poudyal et al., 2018) | virusShare.com, virustotal.com and https://github.com/ytisf/theZoo. | Assembly instruction set and dlls extracted from binaries. |
| (Shaukat & Ribeiro, 2018) | virusShare.com | Binary code |
| (Verma et al., 2018) | malwr.com, virusShare.com, virustotal.com | Indicator of Compromises. |
| (H. Zhang et al., 2019) | | N-grams extracted from opcode. |
| (Wan et al., 2018) | malwaretrafficanalysis.net and wireshark.org. | Network traffic captures. |
| (Y.-C. Chen et al., 2017) | virustotal.com | Network traffic captures. |
| (Scalas et al., 2019) | http://www.virustotal.com<br>https://github.com/necst/heldroid<br>https://www.sec.cs.tubs.de/~danarp/drebin/<br>and Google Play store | System Application Programming Interface based information. |

| | | |
|---|---|---|
| (Fernandez Maimo et al., 2019) | http://perception.inf.um.es/ICE-datasets/ | Network traffic captures. |
| (Almashhadani et al., 2019)<br>(Al-rimy et al., 2019)<br>(B. Zhang et al., 2019)<br>(Bae et al., 2019) | virusshare.com, malware-trafficanalysis.net and virustotal.com<br>virusshare.com, informer.com and virustotal.com virustotal.com, Windows(R) 10 professional edition.<br>Windows 7 system directories, virustotal.com | Behavioral and the non-behavioral features. Application Programming Interface calls opcode sequence<br>System API invocations sequence |
| Al-Hawawreh & Sitnikova, 2019) | virusShare.com, virustotal.com and software.informer.com | API invocations, registry keys, file operations, file extensions, dropped file extensions, strings and directory operations |
| (Sgandurra et al., 2016) | virusShare.com, virustotal.com and software.informer.com | API invocations, registry keys, file operations, file extensions, dropped file extensions, strings and directory operations |
| (Agrawal et al., 2019) | Microsoft windows operating system | File events: createfile, virtualalloc, virtualalloc, getmodulehandle, and getmodulefilename |
| (Alrawashdeh & Purdy, 2018) | virusShare.com, virustotal.com, software.informer.com | File Extension, Extension Pattern, Encryption Algorithm, Registry Keys Operations, API Stats, Files Operations, Directory Operations, Dropped Files Extensions, Source File, Duration and HTTP Methods |
| (Maniath et al., 2017) | Honeynets, Microsoft Windows, online software repositories | API calls, registry value changes and file operations |
| (Vinayakumar et al., 2019) | Tweeter posts | Tweets |
| (Vinayakumar et al., 2017) | http://www.offensvecomputing.net/, http://contagiodump.blogspot.in/, https://malwr.com/,<br>https://github.com/ytisf/theZoo/, https://virustotal.com/, and https://virusshare.com/. | API invocations |
| (Sharmeen et al., 2020) | virusShare, VirusTotal and Softwareinformer | API calls |
| (Bibi et al., 2019) | Smartphone executable App | API calls |
| (Ashraf et al., 2019) | virusShare, VirusTotal, Windows 7 OS | API calls, Registry operations, File operation, Directory created, Network domains, Drop file extensions, DLL’s, and Strings. |
| (Alam et al., 2021) | Ransomwaretracker.abuse.ch | system calls, sequence of actions taken by an application. |
| (Rustam et al., 2023) | virusshare.com. | Application Programming Interface function calls. |
| (Polsani & Jiang, 2023) | virusShare.com, virustotal.com and https://github.com/ytisf/theZoo. | Assembly instruction set and dlls extracted from binaries. |
| (Yaseen et al., 2023) | virusShare.com | Binary code |

### *2.5 Analysis of the ransom ware detection via intelligent algorithms*

We extracted the information about the various data from the project that revealed their source and types of the data used for their work. However, project that concealed the source of their data are not in Table 2 since the required information to fill the corresponding row is not available.

### *2.5.1 The intelligent algorithms that detect ransomware attacks*

The use of intelligent algorithms for the detection of ransomware have been surveyed as discussed in the preceding sections**.** Different types of intelligent algorithms were applied for the detection and it has shown a remarkable performance. The intelligent algorithms performance in detecting ransomware has proven to be better than the conventional methods of detecting ransomware. This signify that the intelligent algorithms have the potential for enhancing the accuracy of ransomware detection system when deployed in the real world environment. Figure 2 shows the percentage of intelligent algorithms applied to detect ransomware attacks.

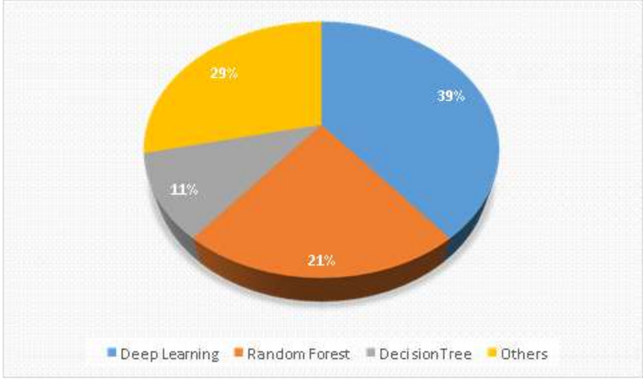

Figure 2: The percentage of intelligent algorithms for the detection of ransomware attacks.

The pie chart shows that 39% of the literatures applied deep learning to detect ransomware activities or classify their families in windows OS, virtual environment, twitter, industrial internet of things, PC, in Field Programmable Gate Array (FPGA) and android environment. Also 21% of the literatures applied RF to detect ransomware activities or classify their families in a virtual machine, PCs, Android OS, or window OS environment. On the other hand, 11% of the literatures applied DT to detect ransomware attacks including their variant in a network, window OS or real-time environment. Finally, 29% applied other types of algorithms to detect ransomware attacks or classify their families in a virtual machine, network, application, windows OS, or real-time environment. It can be deduced from the descriptive statistics that the prominent algorithms that researchers heavily relied on to detect ransomware attacks is the deep learning followed by RF. As it can clearly be seen, deep learning algorithms is the state-of-the-art architecture used to detect ransomware attacks. Though, the idea of applying machine learning algorithms to detect ransomware attacks is still in an infant stage considering the period of time that the literature on the application of machine learning algorithms starts appearing.

### *2.5.2 Domain of applying intelligent algorithms for the detection of ransomware attacks*

Many literatures have proposed different intelligent algorithms for the detection of ransomware in various domain. These domains include

i. Network (Chen et al., 2017; Wan et al., 2018), virtual machine (Ashraf et al., 2019; Cohen & Nissim, 2018; Harikrishnan & Soman, 2018; Lu et al., 2017; Maniath et al., 2017; Sharmeen et al., 2020; Shaukat & Ribeiro, 2018; Verma et al., 2018), PCs (Cusack et al., 2018b; Poudyal et al., 2018; Vinayakumar et al., 2017; H. Zhang et al., 2019), health care (Fernandez Maimo et al., 2019),

ii. Application (Homayoun et al., 2019),

iii. Android (Bibi et al., 2019; Scalas et al., 2019),

iv. real-time environment (Daku et al., 2018),

v. Twitter (Vinayakumar et al., 2017),

vi. industrial internet of things (AlHawawreh & Sitnikova, 2019)

vii. Field Programmable Gate Array (FPGA) (Alrawashdeh & Purdy, 2018) and

viii. Microsoft Windows environment (Agrawal et al., 2019; O. M. K. Alhawi et al., 2018; Bae et al., 2019; Sgandurra, Muñoz-González, Mohsen, & Lupu, 2016).

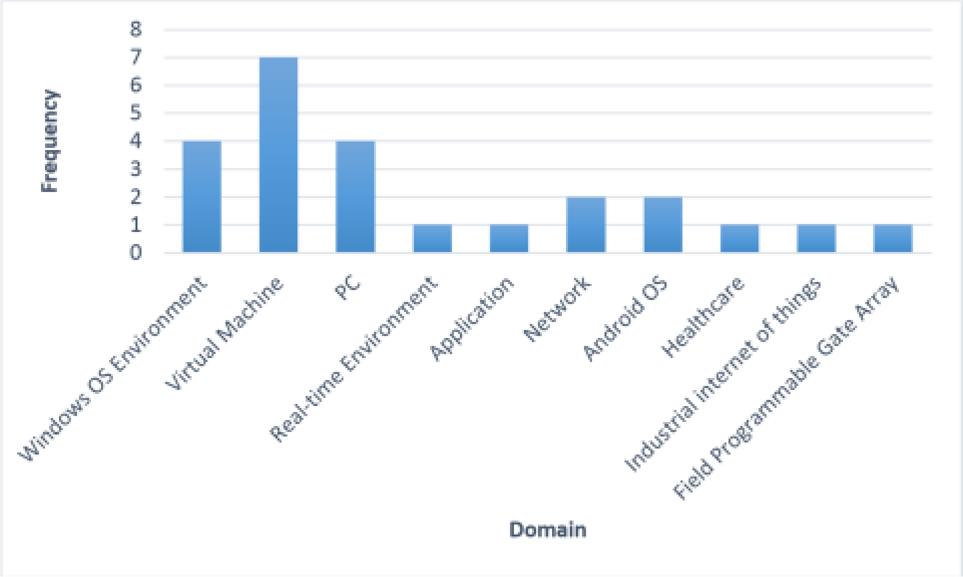

Figure 3: Domain of applying the machine learning algorithm to detect ransomware

Figure 3 depicts the frequency of application domains. The domain that has the highest patronage is virtual environment with 7 applications of machine learning algorithms. Followed by PC and Windows OS each having 4 applications of machine learning algorithms to detect ransomware. Furthermore, network and Android environments each has 2 applications of machine learning to detect ransomware. Finally, health care, application, realtime environment, Field Programmable Gate Array and industrial internet of things environments with one application each.

### *2.6 Research Gap*

From review, we have seen that previous research has explored various techniques for ransomware detection, including signature-based methods, behavior analysis, and machine learning approaches (Al-Hawawreh et al., 2023). However, these methods often struggle with detecting unknown ransomware variants and suffer from high false positive rates. Deep learning models, especially CNNs, have demonstrated effectiveness in feature extraction and pattern recognition, leading to improved ransomware detection performance. Transfer learning has also been widely adopted to leverage pre-trained models and adapt them to specific tasks with limited data. It has been observed from the literature survey that ransomware attacks are of many types, and affect different platforms e.g. network, PC, operating system, virtual machine, among others. Therefore, building a separate classifier from the scratch as currently practice in the literature (e.g. Sharmeen, Ahmed, Huda, Koçer, & Hassan, 2020; Ashraf, Aziz, Zahoora, & Khan, 2019; Bibi, Akhunzada, Malik, Ahmed, & Raza, 2019) (Alam et al., 2021) for ransomware attacks on different platforms is tedious and consume computational resources. To avoid the tedious process of building classifier from the scratch for the different platforms and ransomware attacks, we propose a single model that can detect ransomware attacks on multiple platforms based on deep learning algorithm and transfer learning for detecting ransomware with similar characteristics. This is because the transfer learning allowed a saved trained model to be used to solve a similar problem.

This review highlights the potential of deep transfer learning for detecting ransomware attacks on IoT platforms. By leveraging pre-trained models and adapting them to IoT-specific contexts, deep transfer learning can significantly enhance detection accuracy and efficiency. However, several research gaps need to be addressed to fully realize this potential. Future work should focus on developing comprehensive IoT-specific ransomware datasets that encompass a wide variety of devices and attack scenarios. Additionally, optimizing deep learning models for deployment on resource-constrained IoT devices is crucial. Research should also explore techniques to achieve real-time detection, balancing accuracy with computational efficiency. Further investigation is needed to refine the transfer learning process, ensuring that pre-trained models are effectively adapted to the unique characteristics of IoT environments. By addressing these challenges, the field can move closer to robust and scalable solutions for ransomware detection in IoT, ultimately enhancing the security and resilience of these critical systems.

### *Acknowledgements*

We would like to express our deepest gratitude to our supervisors, Dr. B. I. Yau and Dr. K. I. Musa, whose invaluable guidance, insightful feedback, and unwavering support have been instrumental in the completion of this paper. Your expertise and encouragement have been a source of inspiration throughout this research process. We are profoundly grateful to other researches who grant and provided us academic materials and guides.

### References

Agrawal, R., Stokes, J. W., Selvaraj, K., & Marinescu, M. (2019). *Attention in Recurrent Neural Networks for Ransomware Detection.* Paper presented at the ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).

Ahmadian, M. M., & Shahriari, H. R. (2016). *2entFOX: A framework for high survivable ransomwares detection.* Paper presented at the 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC).

Alam, M., Akram, A., Saeed, T., & Arshad, S. (2021). *Deepmalware: a deep learning based malware images classification.* Paper presented at the 2021 International Conference on Cyber Warfare and Security (ICCWS).

Al-Hawawreh, M., & Sitnikova, E. (2019). *Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment.* Paper presented at the 2019 Military Communications and Information Systems Conference (MilCIS).

Al-Hawawreh, M., Alazab, M., Ferrag, M. A., & Hossain, M. S. (2023). Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. *Journal of Network and Computer Applications*, 103809.

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-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2019). Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. *Future Generation Computer Systems*.

Alhawi, O. M., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. *Cyber Threat Intelligence*, 93-106.

Alhawi, O. M. K., Baldwin, J., & Dehghantanha, A. (2018). Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. *70*, 93-106. doi: 10.1007/978-3-319-73951-9_5

Almashhadani, A. O., Kaiiali, M., Sezer, S., & O'Kane, P. (2019). A Multi-Classifier NetworkBased Crypto Ransomware Detection System: A Case Study of Locky Ransomware. *IEEE Access, 7*, 47053-47067.

Alrawashdeh, K., & Purdy, C. (2018). *Ransomware detection using limited precision deep learning structure in fpga.* Paper presented at the NAECON 2018-IEEE National Aerospace and Electronics Conference.

Andronio, N., Zanero, S., & Maggi, F. (2015). *Heldroid: Dissecting and detecting mobile ransomware.* Paper presented at the International Symposium on Recent Advances in Intrusion Detection.

Ashraf, A., Aziz, A., Zahoora, U., & Khan, A. (2019). Ransomware Analysis using Feature Engineering and Deep Neural Networks. *arXiv preprint arXiv:1910.00286*.

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A Survey and Trends. *Journal of Information Assurance & Security, 6*(2).

Bae, S. I., Lee, G. B., & Im, E. G. Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, e5422.

Bae, S. I., Lee, G. B., & Im, E. G. (2019). Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, e5422.

Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y. u., Jauro, F., Khan, A., . . . Abdulhamid, S. i. M. (2021). Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. *Journal of Ambient Intelligence and Humanized Computing, 12*, 8699-8717.

Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2019). A Survey on Detection Techniques for Cryptographic Ransomware. *IEEE Access, 7*, 144925-144944.

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. (2016). Ransomware digital extortion: a rising new age threat. *Indian Journal of Science and Technology, 9*(14), 1-5.

Bibi, I., Akhunzada, A., Malik, J., Ahmed, G., & Raza, M. (2019). *An Effective Android Ransomware Detection Through Multi-Factor Feature Filtration and Recurrent Neural Network.* Paper presented at the 2019 UK/China Emerging Technologies (UCET).

Breiman, L. (2001). Random forests. *Machine learning, 45*(1), 5-32. Chaudhary, R., Aujla, G. S., Kumar, N., & Zeadally, S. (2018). Lattice based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions. *IEEE Internet of Things Journal*.

Chen, J., Wang, C., Zhao, Z., Chen, K., Du, R., & Ahn, G.-J. (2017). Uncovering the face of android ransomware: Characterization and real-time detection. *IEEE Transactions on Information Forensics and Security, 13*(5), 1286-1300.

Chen, Y.-C., Li, Y.-J., Tseng, A., & Lin, T. (2017). *Deep learning for malicious flow detection.* Paper presented at the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC).

Chiong, G. M. (2023). *The Rise of Ransomware: Motivations, Contributing Factors, and Defenses.* Utica University.

Choi, S., Bae, J., Lee, C., Kim, Y., & Kim, J. (2020). Attention-Based Automated Feature Extraction for Malware Analysis. *Sensors, 20*(10), 2893.

Cohen, A., & Nissim, N. (2018). Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. *Expert Systems with Applications, 102*, 158-178.

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

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security, 79*, 162-189.

Cusack, G., Michel, O., & Keller, E. (2018a). *Machine learning-based detection of ransomware using sdn.* Paper presented at the Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization.

Cusack, G., Michel, O., & Keller, E. (2018b). Machine Learning-Based Detection of Ransomware Using SDN. 1-6. doi: 10.1145/3180465.3180467

Daku, H., Zavarsky, P., & Malik, Y. (2018). *Behavioral-based classification and identification of ransomware variants using machine learning.* Paper presented at the 2018 17thIEEE

International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

Damshenas, M., Dehghantanha, A., & Mahmoud, R. (2013). A survey on malware propagation, analysis, and detection. *International Journal of Cyber-Security and Digital Forensics, 2*(4), 10-30.

Digital Guardian. (2019). A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. Retrieved from

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worstransomware-attacks-all-time

Ding, Z., Shao, M., & Fu, Y. (2016). Incomplete multisource transfer learning. *IEEE transactions*

*on neural networks and learning systems, 29*(2), 310-323.

Druva. (2017). Druva releases annual enterprise ransomware report. from https://www.globenewswire.com/news-release/2017/06/28/1217348/0/en/Druva-Releases-Annual-Enterprise-Ransomware-Report.html

Feizollah, A., Anuar, N. B., Salleh, R., & Wahab, A. W. A. (2015). A review on feature selection in mobile malware detection. *Digital investigation, 13*, 22-37.

Fernandez Maimo, L., Huertas Celdran, A., Perales Gomez, A. L., Clemente, G., Félix, J., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. *Sensors, 19*(5), 1114.

Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications, 153*, 102526.

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

GUVÇİ, F., & ŞENOL, A. (2023). An Improved Protection Approach for Protecting from Ransomware Attacks. *Journal of Data Applications*(1), 69-82.

Han, T., Liu, C., Yang, W., & Jiang, D. (2019). Deep transfer network with joint distribution adaptation: A new intelligent fault diagnosis framework for industry application. *ISA transactions*.

Hansen, S. S., Larsen, T. M. T., Stevanovic, M., & Pedersen, J. M. (2016). *An approach for detection and family classification of malware based on behavioral analysis.* Paper presented at the 2016 International Conference on Computing, Networking and Communications (ICNC).

Harikrishnan, N., & Soman, K. (2018). *Detecting Ransomware using GURLS.* Paper presented at the 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC).

Herrera-Silva, J. A., & Hernández-Álvarez, M. (2023). Dynamic feature dataset for ransomware detection using machine learning algorithms. *Sensors, 23*(3), 1053.

Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., Khayami, R., Choo, K.-K. R., & Newton, D. E. (2019). DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Generation Computer Systems, 90*, 94-104. doi: 10.1016/j.future.2018.07.045

Javaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018). Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. *IEEE Access, 6*, 78321-78332.

Jacob, S. (2023). The Rapid Increase of Ransomware Attacks Over the 21st Century and Mitigation Strategies to Prevent Them from Arising.

Joseph, D. P., & Norman, J. (2020). A Review and Analysis of Ransomware Using Memory Forensics and Its Tools *Smart Intelligent Computing and Applications* (pp. 505-514): Springer.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). *Cutting the gordian knot: A look under the hood of ransomware attacks.* Paper presented at the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

King, D. (2017). Detect and Protect. *ITNOW, 59*(4), 54-55.

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, Threat and Detection Techniques: A Review. *Int. J. Computer Science and Network Security, 19*(2), 136.

Lachtar, N., Ibdah, D., & Bacha, A. (2019). The Case for Native Instructions in the Detection of Mobile Ransomware. *IEEE Letters of the Computer Society*.

Lamers, C., Spoerl, E., Levey, G., Choudhury, N., & Ahmed, M. (2023). Ransomware: A Threat to Cyber Smart Cities *Cybersecurity for Smart Cities: Practices and Challenges* (pp. 185-204): Springer.

Lang, M., Connolly, L., Taylor, P., & Corner, P. J. (2023). The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice, 4*(4), 1-22.

Lee, S., Kim, H. K., & Kim, K. (2019). Ransomware protection using the moving target defense perspective. *Computers & Electrical Engineering, 78*, 288-299.

Li, J., Wu, W., Xue, D., & Gao, P. (2019). Multi-Source Deep Transfer Neural Network Algorithm. *Sensors, 19*(18), 3992.

Lu, T., Zhang, L., Wang, S., & Gong, Q. (2017). *Ransomware detection based on v-detector negative selection algorithm.* Paper presented at the 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC).

Maigida, A. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments, 5*(2), 67-89.

Maniath, S., Ashok, A., Poornachandran, P., Sujadevi, V., Sankar, A. P., & Jan, S. (2017). *Deep learning LSTM based ransomware detection.* Paper presented at the 2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE).

Martín, A., Hernandez-Castro, J., & Camacho, D. (2018). An in-depth study of the Jisut family of Android ransomware. *IEEE Access, 6*, 57205-57218.

Min, D., Park, D., Ahn, J., Walker, R., Lee, J., Park, S., & Kim, Y. (2018). Amoeba: An

Autonomous Backup and Recovery SSD for Ransomware Attack Defense. *IEEE Computer Architecture Letters, 17*(2), 245-248.

Möller, D. P. (2023). Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 273-303): Springer.

Muna, A.-H., den Hartog, F., & Sitnikova, E. (2019). Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things. *IEEE Internet of Things Journal*.

National Vulnerability Databasa. (2017). CVE-2017-0144 Detail. from https://nvd.nist.gov/vuln/detail/CVE-2017-0144

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks, 7*(5), 321-327.

Pan, S. J., Tsang, I. W., Kwok, J. T., & Yang, Q. (2010). Domain adaptation via transfer component analysis. *IEEE Transactions on Neural Networks, 22*(2), 199-210.

Pathak, P., & Nanded, Y. M. (2016). A dangerous trend of cybercrime: ransomware growing challenge. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5*(2), 371-373.

Polsani, H., & Jiang, H. (2023). DeepGray: A Novel Approach to Malware Classification Using Grayscale Images with Deep Learning.

Pluskal, O. (2015). *Behavioural malware detection using efficient SVM implementation.* Paper presented at the Proceedings of the 2015 Conference on research in adaptive and convergent systems.

Poudyal, S., Subedi, K. P., & Dasgupta, D. (2018). *A Framework for Analyzing Ransomware using Machine Learning.* Paper presented at the 2018 IEEE Symposium Series on Computational Intelligence (SSCI).

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10.

Ryan, M. (2020). *The ransomware revolution: how emerging encryption technologies created a prodigious cyber threat.* UNSW Sydney.

Sabharwal, S., & Sharma, S. (2020). Ransomware Attack: India Issues Red Alert *Emerging Technology in Modelling and Graphics* (pp. 471-484): Springer.

Savage, K., Coogan, P., & Lau, H. (2015). The evolution of ransomware. *Symantec, Mountain View*.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). *Cryptolock (and drop it): stopping ransomware attacks on user data.* Paper presented at the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS).

Scalas, M., Maiorca, D., Mercaldo, F., Visaggio, C. A., Martinelli, F., & Giacinto, G. (2019). On the Effectiveness of System API-Related Information for Android Ransomware Detection. *Computers & Security*.

Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv preprint arXiv:1609.03020*.

Shakir, H. A., & Jaber, A. N. (2017). *A Short Review for Ransomware: Pros and Cons.* Paper presented at the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.

Shhadat, I., Hayajneh, A., & Al-Sharif, Z. A. (2020). The Use of Machine Learning Techniques to Advance the Detection and Classification of Unknown Malware. *Procedia Computer Science, 170*, 917-922.

Sharmeen, S., Ahmed, Y. A., Huda, S., Koçer, B., & Hassan, M. M. (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access*.

Shaukat, S. K., & Ribeiro, V. J. (2018). *RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning.* Paper presented at the 2018 10th International Conference on Communication Systems & Networks (COMSNETS).

Shukla, M., Mondal, S., & Lodha, S. (2016). *Poster: Locally virtualized environment for mitigating ransomware threat.* Paper presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information processing & management, 45*(4), 427-437.

Su, D., Liu, J., Wang, X., & Wang, W. (2018). Detecting Android Locker-Ransomware on Chinese Social Networks. *IEEE Access, 7*, 20381-20393.

Symantec. (2019). 2019 Internet Security Threat Report. From https://www.symantec.com/en/uk/security-center/threat-report

Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? *International Cybersecurity Law Review, 4*(3), 259-280.

Verma, M., Kumarguru, P., Deb, S. B., & Gupta, A. (2018). *Analysing Indicator of Compromises for Ransomware: Leveraging IOCs with Machine Learning Techniques.* Paper presented at the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI).

Villalba, L. J. G., Orozco, A. L. S., Vivar, A. L., Vega, E. A. A., & Kim, T.-H. (2018). Ransomware Automatic Data Acquisition Tool. *IEEE Access, 6*, 55043-55052.

Vinayakumar, R., Alazab, M., Jolfaei, A., Soman, K., & Poornachandran, P. (2019). *Ransomware triage using deep learning: twitter as a case study.* Paper presented at the 2019 Cybersecurity and Cyberforensics Conference (CCC).

Vinayakumar, R., Soman, K., Velan, K. S., & Ganorkar, S. (2017). *Evaluating shallow and deep networks for ransomware detection and classification.* Paper presented at the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

Wan, Y.-L., Chang, J.-C., Chen, R.-J., & Wang, S.-J. (2018). *Feature-Selection-Based Ransomware Detection with Machine Learning of Data Analysis.* Paper presented at the 2018 3rd International Conference on Computer and Communication Systems (ICCCS).

Xiao, G., Li, J., Chen, Y., & Li, K. (2020). MalFCS: An effective malware classification framework with automated feature extraction based on deep convolutional neural networks. *Journal of Parallel and Distributed Computing*.

Yang, J., Yan, R., & Hauptmann, A. G. (2007). *Cross-domain video concept detection using adaptive svms.* Paper presented at the Proceedings of the 15th ACM international conference on Multimedia.

Yaseen, S., Aslam, M. M., Farhan, M., Naeem, M. R., & Raza, A. (2023). A Deep Learning-based Approach for Malware Classification using Machine Code to Image Conversion. *Technical Journal, 28*(01), 36-46.

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks, 129*, 444-458.

Zhang, B., Xiao, W., Xiao, X., Sangaiah, A. K., Zhang, W., & Zhang, J. (2019). Ransomware classification using patch-based CNN and self-attention network on embedded Ngrams of opcodes. *Future Generation Computer Systems*.

Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., & Sangaiah, A. K. (2019). Classification of ransomware families with machine learning based on N-gram of opcodes. *Future Generation Computer Systems, 90*, 211-221. doi: 10.1016/j.future.2018.07.052.