

BSIT-S22-003 03-135191-002 Anas Nawaz 03-135191-004 Hamza Iqbal

Classification of Ransomware Attacks Using Machine Learning

In partial fulfilment of the requirements for the degree of **Bachelor of Science in Information Technology**

Supervisor: Muhammad Zunnurain Hussain

Department of Computer Sciences Bahria University, Lahore Campus

January 2023

© Bahria University, 2023

Certificate



We accept the work contained in the report titled

Classification of Ransomware Attacks Using Machine Learning

written by

Anas Nawaz

Hamza Iqbal

as a confirmation to the required standard for the partial fulfilment of the degree of Bachelor of Science in Information Technology.

Approved by: Supervisor:

Muhammad Zunnurain Hussain

(Signature)

January 10, 2023

DECLARATION

We hereby declare that this project report is based on our original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at Bahria University or other institutions.

Enrolment	Name	Signature
03-135191-002	Anas Nawaz	
03-135191-004	Hamza Iqbal	

Date : January 10, 2023

Specially dedicated to

my beloved grandfather, mother, and father

(Anas Nawaz)

my beloved grandmother, mother, and father

(Hamza Iqbal)

ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express our gratitude to my research supervisor, Mr. Zunnurain Hussain his invaluable advice, guidance and his enormous patience throughout the development of the research.

In addition, we would also like to express my gratitude to our loving parent and friends who had helped and given me encouragement.

Anas Nawaz

Hamza Iqbal

Classification of Ransomware Attacks Using Machine Learning

ABSTRACT

To make money, steal information, and harm computer systems, malware takes on a kind of dangerous presence in the online world. Ransomware is a unique form of virus that poses serious hazards to the entire planet. It has resulted in an immeasurable loss for the businesses, the government, and the people. The previous anti-malware technology employed signatures to detect malware when it came to creating a defense against it. However, once the ransomware has been installed on a victim's machine, further investigation is no longer feasible. The signature-based strategy has already started to lose its impact.

Machine learning research and advancements in ransomware detection and classification have led to effective and precise differentiation. By gathering and studying ransomware characteristics, machine learning algorithms have significantly improved the ransomware defense technology. To discover the dataset with the greatest representation of ransomware behavior, this research will proceed from basic feature collections to feature engineering. Iterative techniques are being used to construct this system.

Table of Contents

DE	CLAR	ATION	ii
AC	KNOV	VLEDGEMENTS	iv
AB	STRA	CT	v
Lis	t of tab	les:	ix
Lis	t of fig	ures	x
	Chap	ter 1	1
1	Intro	duction	1
	1.1	Background:	1
	1.2	Problem Statement:	1
	1.3	Aims and Objectives:	2
	1.4	Scope of Project:	2
	Chap	ter 2	4
2	LITE	CRATURE REVIEW	4
	2.1	Technology:	4
	2.2	Malware:	6
	2.2.1	Malware Method:	7
	2.3	Ransomware Attack:	7
	2.3.1	Ransomware Attack Variety:	8
	2.3.2	How Ransomware Works:	10
	2.3.3	Ransomware Protection:	11
	2.3.4	Ransomware Removal:	13

	2.4	Machine Learning in Ransomware Attack:	13
	2.4.1	How machine learning technologies can defend against ransomware	14
	2.5	Visualization:	15
	2.6	Systematic Literature Review (SLR):	16
	Chap	ter 3	55
3	DESI	GN AND METHODOLOGY	55
	3.1	Methodology:	55
	3.1.1	Data:	56
	3.1.2	Target Data (Dataset):	56
	3.1.3	Data preprocessing	57
	3.1.4	Attributes and Type	57
	3.1.5	Transformed Data:	57
	3.1.6	Transformed Data Attributes and type	58
	3.1.7	Patterns:	58
	3.1.8	Knowledge or Result:	58
	3.2	Deep Learning:	59
	3.3	Gradient-boosted trees (GBM):	60
	3.4	Random Forest:	60
	Chap	ter 4	62
4	DATA	A AND EXPERIMENTS	62
	4.1	Download Dataset from Kaggle:	62
	4.2	Download and Install RapidMiner:	63
	4.3	Heat Map:	64
	4.4	Import the Dataset:	64
	4.4.1	Select the location:	65
	4.4.2	Select the Data:	65
	4.4.3	Save the Data:	67
	4.4.4	Set the target Class:	68

	4.4.5	Prepare Target:	69
	4.4.6	Select Inputs Fields:	69
	4.4.7	Select the Model:	70
	4.5	Intrusion Detection System (IDS)	71
	4.5.1	SolarWinds	71
	Chapt	er 5	85
5	RESU	LTS AND DISCUSSIONS	85
	5.1	Result:	85
	5.2	Deep learning:	85
	5.3	Gradient-boosted trees (GBM):	92
	5.4	Random Forest:	95
	Chapt	er 6	98
6	CON	CLUSION AND FUTURE WORK	98
	6.1	Conclusion:	98
	6.2	Future Work:	99
RE	FEREN	ICES	100

List of tables:

Table 2.1:SLR	16
Table 3.1:Attributes and Types	57
Table 3.2: Transformed Data Attributes and type	58
Table 4.1: Events	78
Table 5.1: Result	85

List of figures

Figure 3.1: Methodology Diagram	55
Figure 4.1: Kaggle Dataset Ransomware	
Figure 4.2: Bitcoin Heist Ransomware Address Dataset	63
Figure 4.3: RapidMiner Installation	63
Figure 4.4: Heat Map	64
Figure 4.5: Import Data	64
Figure 4.6: Select Location	65
Figure 4.7: Select Data	66
Figure 4.8: Select Data Format	66
Figure 4.9: Format Columns	67
Figure 4.10: Save the Data	67
Figure 4.11: Select data of New Model	
Figure 4.12: Select Target Class	
Figure 4.13: Prepare Target	69
Figure 4.14: Select Input Fields	70
Figure 4.15: Select The Model	70
Figure 4.16: NPM Summary	72
Figure 4.17: Wireless Network Summary	72
Figure 4.18: Balancing Environment	73
Figure 4.19: NOC Dashboard	74
Figure 4.20: Energy Wise Summary	74
Figure 4.21: Capacity Summary	75
Figure 4.22: VSAN Summary	76
Figure 4.23: NetPath Services	76
Figure 4.24: Network Top 10 View	77
Figure 4.25: All Active Alerts	

Figure 4.27: Log Viewer79Figure 4.28: Traps80Figure 4.29: Message Center81Figure 4.29: Anomaly Based alerts81Figure 4.30: Anomaly Based alerts81Figure 4.31: All Report82Figure 4.32: Network Sonar Discovery83Figure 4.33: Manage Nodes83Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 4.29: Message Center81Figure 4.30: Anomaly Based alerts81Figure 4.31: All Report82Figure 4.32: Network Sonar Discovery83Figure 4.33: Manage Nodes83Figure 4.34: Manage Dashboards84Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 4.30: Anomaly Based alerts81Figure 4.31: All Report82Figure 4.32: Network Sonar Discovery83Figure 4.33: Manage Nodes83Figure 4.34: Manage Dashboards84Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 4.31: All Report.82Figure 4.32: Network Sonar Discovery83Figure 4.33: Manage Nodes83Figure 4.34: Manage Dashboards84Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 4.32: Network Sonar Discovery83Figure 4.33: Manage Nodes83Figure 4.34: Manage Dashboards84Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 4.33: Manage Nodes83Figure 4.34: Manage Dashboards84Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 4.34: Manage Dashboards84Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 5.1: Deep Learning Model86Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 5.2: Select Simulator DL86Figure 5.3: Model Details87Figure 5.4: Weight Data87Figure 5.5: Bar Chart88Figure 5.6: Pie Chart88Figure 5.7: Root Mean Square Error89
Figure 5.3: Model Details
Figure 5.4: Weight Data
Figure 5.5: Bar Chart
Figure 5.6: Pie Chart
Figure 5.7: Root Mean Square Error
Figure 5.8: Absolute Error
Figure 5.9: Relative Error
Figure 5.10: Squared Error
Figure 5.11: Correlation91
Figure 5.12: Income Summary91
Figure 5.13: Histogram Chart92
Figure 5.14: Gradient-boosted trees93
Figure 5.15: Step Line Graph93
Figure 5.16: Tree Diagram 194
Figure 5.17: Tree Diagram 294
Figure 5.18: Tree Diagram 395
Figure 5.19: Random Forest
Figure 5.20: Line Graph
Figure 5.21: Scatter / Bubbles
Figure 5.22: Bell Curve Graph97

Chapter 1

Introduction

1.1 Background:

Since the creation of computing and networking technologies, cybersecurity has been one of the main issues. Significant study has been done to build the defenses to protect people and organizations from such sabotage as criminals are becoming more sophisticated and posing new risks. Ransomware is one of the many varieties of malware that has been developing tremendously in recent years and has a particularly negative influence on the world.

1.2 Problem Statement:

The irreversible nature of a ransomware attack sets it apart from earlier computer assaults. After encryption is complete, the decryption key is the sole way to unlock the user files. To decrypt the data, the attackers demand payment in the anonymous currency known as bitcoin. Infections by ransomware damage both individuals and companies looking to boost sales. Data is disclosed in most situations. Approximately 70% of ransomware assaults, according to research, exposed the victim's data. Our goal is to review of ransomware attacks and detect the ransomware attack in dataset than visualize the attack using machine learning.

1.3 Aims and Objectives:

The aims and objectives are given below:

- i. Machine learning-based visualization of ransomware attacks.
- ii. Detection the Ransomware attacks in dataset.
- iii. The Efficiency and Accuracy of the results.

1.4 Scope of Project:

What: Ransomware attacks have increased during the previous few years, many of them in the public eye. According to a report by Compatriotic, in 2020 alone, ransomware attacks will have cost the healthcare sector more than \$20 billion in lost revenue, legal fees, and ransom payments. Over 600 hospitals, health centers, and other healthcare facilities were hit by 92 ransomware attacks throughout the year. Implementing the technology to identify the ransomware assault is thus the primary goal.

Why: Many hackers use unrest and chaos in times of crises in search of possible financial benefit. The COVID-19 problem, which started in 2020, brought further attention to cyberattacks in the healthcare industry. Cybersecurity is more crucial than ever before for protecting user or organizational data; thus, we must put this system in place.

How: First we will get the data from dataset of ransomware attack and then process the data in different virtual machine. We will visualize the result of different datasets and use different tools like RapidMiner, rattle, and Window OS.

- i. Comprehensive review of Ransomware attacks.
- ii. Detection the Ransomware attacks in dataset.
- iii. Visualization of Ransomware attacks using machine learning.

Chapter 2

LITERATURE REVIEW

2.1 Technology:

Technology is always developing new ways to improve society living. Technology advancements enable industry to carry out current activities more effectively, having a direct impact on other industries and eventually society. In the 1980s, personal computers started to become widely used. These stand-alone, permanent terminal devices made computer ideas like operating systems, programming, early business applications, and games accessible to the public. For military use, ARPANET created protocols for establishing connections between distant computers in the late 1960s. A small number of nodes interconnected via the current communications infrastructure were used in this. Hypertext Markup Language (HTML) helped the World Wide Web (WWW) gain popularity in the late 1980s (HTML). Since that time, more people have access to the internet. Access to and connectivity with the Internet are inextricably related to the development of the WWW. Advancements in data and communications have served as catalysts for the development of everything from mobile and internet services to dial-up modems and the Integrated Services Digital Network (ISDN).

Since the beginning of the 1980s, mobile Internet services have also developed. First generation (1G) gave 2.4 kbps, and second generation offered 64 kbps (2G). 2G development was supervised by Global Systems for Mobile Communications. Global Systems for Mobile marked the start of new initiatives and collaborations, including Third

Generation Partnership Projects and the Universal Mobile Telecommunications Systems (UMTS) (3GPP). From 144kbps in transit to 2Mbps stationary, 3G delivered data services. increased call, video, and communication services with download speeds of up to 100Mbps, 4G is an LTE wireless broadband service created by the 3GPP. The foundation for the development and eventual implementation of 5G services has been set through these initiatives and alliances. Society will become more valued and pertinently connected as the Internet and WWW develop. Nowadays, most communication takes place on gadgets like smartphones, laptops, tablets, etc.

A router that follows this protocol is required a network must be reachable through the internet. Up to this point, a 4th-generation Internet Protocol operated rather well. However, the arrival of more Internet-connected devices increased the pressure placed on IPV4's addressing capabilities. In 1993, the Internet Engineering Task Force (IETF) began developing concepts for IPv4's replacement and making suggestions for its implementation. Smart things will have a variety of communications capabilities, from the most basic to the most complicated. The effectiveness of the security measures will rely on the computing power of the item, making certain things more vulnerable than others. The physical properties of the smart object affect amount of processed or stored data as well. Variety installed advance items is growing along with IoT initiatives. Access control, participation, and data security are essential elements of IoT installations. For smart city residents who respect their privacy, protecting this data is crucial to building confidence. Data about an individual or a whole society may be compromised. Social media and mobile technologies have transformed the conventional idea of a smart city from one centered on industry to one that emphasizes holistic living. The confidentiality and safety of data are crucial regardless of the individual, social, or industrial IoT principles.

2.2 Malware:

Reproducible computer code was first proposed in 1949. According to this notion, programs might self-replicate and transmit their code to new programs. When Fred Cohen created a computer software that could infect a computer, duplicate itself, and spread to other devices in 1987, he coined the word "virus". In the 1980s, the personal computer and ARPANET were establishing a connected world. The possibility of developing dangerous software was also expanding. There was now a way for the self-replicating programs envisaged in 1949 to spread to other locations. Infected ARPANET terminals of the Creeper worm posted a message and established new connections with additional terminals. This annoyance proved that computer code might infect linked devices via automation and repetition even when no harm was done. These techniques led to the emergence of more harmful software. Targets included the Brain virus and MS-DOS operating system, while the Morris worm took use of a link to the ARPANET. In the early 1990s, HTML aided in the construction and growth of the WWW. The proliferation of harmful software was made easier by the increase of networked computers. Evolutionary Web X.0 paradigms gave rise to new malware techniques and varieties. The list of the WWW and the viruses it has produced is shown below:

- 1991: With the introduction of Michelangelo in 1991, the public on the Internet became aware of the danger posed by viruses. This infection increased public awareness of the risks posed by viruses and helped pave the way for the development of anti-virus software.
- 1999: The broad infection of the Internet by Melissa, ILOVEYOU, and Anna Kournikova was made possible by the efficient delivery of harmful code via email.
- 2003: SQL flaws are made public after Slammer and Conficker were exploited to launch widespread DDoS assaults.
- ✤ 2005: Koobface is disseminated through social media channels.
- 2007: ZBot, which infects Windows workstations and is engineered to steal financial information, becomes the most successful botnet ever.
- 2010: The well-known Stuxnet malware, which aims to undermine the Iranian nuclear program, targets industrial control systems.
- ✤ 2013: Introduction of Crypto locker, which encrypts user data on computers, ransomware debuted as software that generates cash. Before the decryption key is

provided, a ransom, often in Bitcoin, must be paid. In 2017, WannaCry spread internationally, harming individuals, businesses, and governmental organizations in over 150 nations.

2016: Targeting insecure IoT devices led to the creation of the Mirai botnet in 2016.
 High-profile web services were paralyzed because of the DDoS assault.

2.2.1 Malware Method:

The first Creeper worm spread and infected terminals via automated and repeated methods. These traits are present in all the malware categories listed above. The malware is created, programmed, and released by humans. A person botmaster is also in charge of the command and control (C&C), may be contacted by infected computers. End users unknowingly permit material, which promotes to infection due to human naivety. Global infection, however, mostly on automation and repetition techniques. Botnets offer a method for the infection and control of cyberattacks on a worldwide scale. A botnet assault will typically include two sets of IP addresses. The hacked hosts are the first group of IP addresses. These are ordinary infected devices that unintentionally take part in an assault. The C&Cs make up the second group of IPs.

There are three ways for C&C and the compromised host to communicate:

- ♦ A concept based on Internet Relay Chat that uses take orders from C&C.
- ✤ An internet approach that uses host-based pull instructions.
- ◆ Peer-to-peer (P2P) paradigm, where bots communicate with one another.

2.3 Ransomware Attack:

Users are attacked by ransomware, a type of malware that encrypts data without their permission. Limits authorized access to user data. Users are not allowed to utilize their own assets because of this. The irreparable nature of a ransomware attack sets it apart from earlier computer assaults. The user files can only be unlocked using the decryption key after encryption is complete. To decrypt the data, the attackers want money in bitcoin, an undetectable money. Threats by ransomware damage both individuals and corporations by reducing income. Attackers benefit from the undetectable currency and long-lasting harm that ransomware assaults create. Threats are made against the victim, including that his data will be misused, destroyed, or revealed, as well as that private details like search history [1]. The data is disclosed in most situations. According to a survey, data from the victim was exposed in around 70% of ransomware assaults.

2.3.1 Ransomware Attack Variety:

There are a huge variety of ransomware malware strains. [2]

Locky

Locky allows for the encryption of 160 file types, mostly those used by designers, engineers, and testers. It was first launched in 2016. Hackers send e - mails inviting recipients to download malicious ZIP files or Word, Excel, or PowerPoint files from Microsoft Office. It is frequently spread by phishing or exploit kits.

WannaCry

WannaCry is a beginner-level malware that spreads itself among computers by exploiting a hole in the Windows SMB protocol. The WannaCry packager, a self-contained application, extracts the encryption/decryption software, files containing encryption keys, and the Tor communication software. It is not difficult to locate and remove, nor is it disguised. 2017 saw the rapid spread of WannaCry across 150 nations, resulting in \$4 billion in damage to 230,000 machines.

Crypto locker

Nearly half a million computers were hacked by the 2017 version of Crypto locker. Typically, e - mail, file-sharing websites, and unprotected downloads are how malware spreads to PCs. In addition to files on the local workstation, it may also encrypt objects it has authority to write to and search mapped network devices. Current iterations of Crypto locker can evade firewalls and anti-virus software from the past [3].

Cerber

Cerber, a ransomware-as-a-service tool, may be used by cybercriminals to initiate attacks and distribute their loot alongside the malware author. Cerber runs covertly while encrypting data and may attempt to disable antivirus and Windows security features in order to prevent users from reinstalling the operating system. The desktop wallpaper changes to a ransom message after the computer's data has been successfully encrypted.

Petya

Using the Master File Table to encrypt the whole hard disc, Petya is a ransomware malware that seizes control of a computer (MFT). The entire disc is inaccessible even though the files are not encrypted. Petya spread mostly through a fake cover letter for a job that contained a link to an infected Dropbox file, which was how it was first identified in 2016. PCs with only Windows were affected.

Grand Crab

2018 saw the release of Grand Crab. The attackers threatened to reveal the victims' propensity for watching porn in ransomware-based extortion activities, and it encrypts data on the victim's computer and demands a payment. There are various variations, and they are all designed for Windows computers. Most Grand Crab versions may currently be decrypted for free.

Ryuk

To access computers, Ryuk utilizes drive-by downloads or email spam. It makes use of a dropper, which downloads a trojan and establishes a persistent network connection on the victim's machine. Attackers can use Ryuk as the foundation for an Advanced Persistent Threat (APT) and then add keylogging software, carry out privilege escalation, and engage in lateral movement. Ryuk is installed on every system to which the attacker gains access after that.

2.3.2 How Ransomware Works:

The ransomware attack continues as following when the infected code is found on a device. Ransomware may stay dormant on a system and wait to launch an assault at a time when it is least secure [4]. Seven-stage of Ransomware:

Execution- In order to carry out its harmful actions, ransomware seeks and register's locations for specific documents, including locally stored files, mapped and unmapped network-accessible systems. Backup files and folders may potentially be lost or encrypted as a result of some ransomware attacks.

Infection- Ransomware is installed and stealthily downloaded onto the computer.

Encryption- During the encryption stage, ransomware trades keys with the command-andcontrol system. Then, during the Execution stage, the ransomware utilizes the encryption key to encrypt any files discovered. Similarly, the information's accessibility is restricted.

User Notification- Before displaying a ransom note to the victim, ransomware installs files with instructions explaining the compensation process.

Cleaning up-Ransomware often shuts down and deletes itself, just the files with the financial transactions remain.

Payment- The target hits an URL in the financial transactions, which takes them to a website with more instructions on how to transfer the required ransom. To prevent being detected by network traffic monitoring, these messages are commonly wrapped and disguised utilizing secret TOR facilities.

Decryption- After paying the ransom, the victim may get the decryption key via the attacker's Bitcoin address. However, there is no guarantee that the decryption key will be sent as promised [5].

2.3.3 Ransomware Protection:

The following recommended practices will assist you in preventing and guarding against Ransomware attacks in your business:

Endpoint Protection

The apparent first line of defense against ransomware is Endpoint Protection Antivirus, however outdated antivirus technologies can only offer limited protection. A component of modern endpoint security solutions, next-generation antivirus provides protection from signature - based attacks like WannaCry, zero-day malware, and ransomware whose signature is not yet available in malware databases. They also have device firewalls and

endpoint detection and response capabilities, which help security teams recognize and block endpoint attacks fast.

Patch Management

Update the operating system, installed programs, and security patches on the device. Conduct vulnerability scans to find and swiftly fix known issues.

Data Backup

Data should be frequently backed up to an external drive using the 3-2-1 rule and versioning control create three backup copies on two different media with one backup stored in a separate location. If you can, unplug the hard drive from the computer to prevent the backup data from being encrypted [6].

Control and Application Spam filtering

Establish device restrictions to limit installed programs to a centrally controlled checklist. Users should boost their browser security settings, turn off Adobe Flash and other shoddy browser plugins, and use web filtering to prevent them from visiting hazardous websites. Turn off macros in word processors and other exposed programs.

Network Security

Use a firewall or web application firewall, intrusion prevention/intrusion detection systems, and other limitations to prevent ransomware from interacting with command-and-control centers.

Email Security

Tests should be given to evaluate if employees can recognize and avoid phishing emails, and they should be educated to recognize social engineering emails. Use spam prevention and endpoint protection software to automatically filter out dubious emails and to block the hazardous content if a user does happen to click on one of the links.

2.3.4 Ransomware Removal:

Here are the initial actions you should take to reduce the ransomware danger if you discovered an infestation in your network:

Isolate- Isolate the infected computers by locating them, cutting them off networks, then locking share discs to stop encode. Look into the backups that are accessible for encrypted data. Check to see what kind of ransomware you were exposed to and whether any decryptors are available. Determine whether the ransom is a feasible option [7].

Recover- Recover your data from a backup if no decryptor tools are available. In most nations, paying the ransom is not advised, although in some severe circumstances, it could be an alternative. Follow industry standards when erasing and reimaging affected systems to get rid of ransomware.

Reinforce- In order to comprehend how computer systems were compromised and prevent a recurrence, reinforce conduct a lesson learned workshop. Determine the critical flaws or inadequate security procedures that let the attacker's entry and fix them.

Evaluation- It's important to evaluate what happened and the lessons that might be used when the crisis is resolved. How did ransomware operate effectively? Which security flaws allowed for penetration? Why did email filtering and antivirus fail? How much of a spread did the illness have? Were infected computers able to be cleaned up and reinstalled, and was a backup restoration successful? To be better prepared for the next assault, address the areas where your security posture is lacking.

2.4 Machine Learning in Ransomware Attack:

Given the wide range of handwriting styles, it would be challenging to create a program that could recognize handwritten letters. Even if you could take into consideration these variations, creating the software itself could take too much time or be too difficult [8].

Such a challenge is not "game over" with today's machine learning technologies. Instead, by giving it instances to analyze, this technology may be used to address the same problem in novel circumstances. The examples act as a manual for correctly identifying letters. In essence, the goal is to teach the computer to solve issues using examples or recognize patterns, just like you could teach a young child to distinguish between a cat and a dog.

ML is a branch of AI research that creates statistical models using principles from computer science and statistics. These modules are used for two different things:

- ✤ Inferring from information requires finding connections.
- Use knowledge of the past to anticipate the future and make (very correct) assumptions about it.

ML focuses more on making predictions about the future than does AI, which frequently focuses on teaching computers to make judgments (predicated on Machine learning and logical sets of guidelines). This is where ML technology differs from AI.

2.4.1 How machine learning technologies can defend against ransomware

Ability to foresee is the hidden weapon that ML possesses. With more accurate information points available for it to learn from, this ability is enhanced. Imagine playing game repeatedly with the one same partner and then with different players. As you gain experience, you become more adept at predicting your adversaries' future moves. You have additional alternatives to think about by incorporating the lessons discovered from prior opponents, allowing you to modify your own approach accordingly. The foundation of the machine learning procedure in the context of data protection is stack trace analysis. Consider the fact that a program leaves a trail of what has occurred at various times in time. Normal activity is made evident by examining what transpires at each stage, and a reference

model is established. In the case of a ransomware attack, new code will be inserted into this process, which would be evident.

The most effective software uses ML that ignores aberrations and just considers the most often used reference points. This method progressively develops the computer's understanding of legitimate vs harmful code, improving accuracy while also enhancing software speed due to the machine learning model's reduced data usage.

2.5 Visualization:

Graphs, charts, and plots can be used to display analysis of a dataset that has been captured. These do a better job of communicating the information. Additionally, it effectively conveys massive statistics to a target audience. To help people, comprehend and make sense of massive volumes of data, data visualization is a technique that makes use of a variety -of static and dynamic visualizations within a given context. To visualize patterns, trends, and connections that could otherwise go missing, the data is sometimes presented in a narrative style.

2.6 Systematic Literature Review (SLR):

TABLE 2.1:SLR

Year	Paper Title	Author	Objectives	Methodology	Contribution	Future Gap
2017	STUDY ON	Ganesh	The objectives of this	The methodology	The contribution of	Future Work or Future
	RANSOMWARE	Gupta	paper:	used in this paper:	the paper:	Gap:
	ATTACK AND		• Cybersecurity	• Using	• The	• While some
	ITS		education can raise	various	significance	commercial
	PREVENTION		awareness among	intrusion	of having a	antivirus
			less experienced	prevention	traffic-	products come
			computer users.	system (IPS)	filtering	with an
			• Regular practice of	technology,	system that	automatic update
			preventative	malicious	can offer	module and a
			strategies can also	traffic from	proactive anti-	real-time
			be provided.	exploit kit	ransomware	scanner, anti-
				activity can	defense.	ransomware
				be detected		security

				and blocked,		technologies can
				preventing		be a dependable
				the		alternative.
				ransomware		• To provide more
				installation		reliable antivirus
				process.		product for
						future.
2019	Prevention of	S. H. Kok	The objectives of this	The methodology	The contribution of	Future Work or Future
	Crypto-	and	paper:	used in this paper:	the paper:	Gap:
	Ransomware	Mahadevan	• Only focuses	• The two-	• In terms of test	• The PEDA
	Using a	Supramani	on crypto	phased pre-	error, FPR,	concept attempts
	Pre-Encryption	am	ransomware	encryption	AUC, and	to save users
	Detection		because it	detection	detection rate,	from having to
	Algorithm		makes data	algorithm	LA surpasses	pay ransom by
			unrecoverable	(PEDA).	other learning	spotting
			and once	• A Windows	algorithms	ransomware
			suspect's	application	like RF and	before it encrypts
			documents	programming	NB.	data. It is
			were	interface in	• LA or PEDA-	possible to think
			encrypted.	PEDA-	Phase-l has	of this restriction

			• Developed a	Phase-I.	successfully	as a research goal
			pre-encryption	(API). the	identified	for the future.
			detection	PEDA-	crypto-	• PEDA-Phase-II
			method	Phase-II	ransomware	intends to create
			(PEDA) for	signature	using only	a Signature
			ransomware	repository.	API data,	Repository by
			cleanup with		demonstrating	storing the
			the least		its	signature of all
			amount of		effectiveness	discovered
			danger.		as a prediction	ransomware.
					model.	
2016	Automated	Daniele	The objectives of this	The methodology	The contribution of	Future Work or Future
	Dynamic Analysis	Sgandurra	paper:	used in this paper:	the paper:	Gap:
	of Ransomware:		• Developed	• Elderan	• Demonstrated	• The authors
	Benefits,		EldeRan, a	Sandboxed	that ML is a	predict how
	Limitations and		framework to	Training	workable and	ransomware will
	use for Detection		recognize the	• Analysis	efficient	develop in the
			most important	Elderan Live	method for	future, including
			dynamic	Detection.	identifying	by focusing on
			ransomware		new	the wearables

traits and	ransomware	sector
utilize them to	families and	(commonly
identify	variations for	known as
ransomware.	analysis and	"ransom wear").
• EldeRan's	signature	By
capacity to	extraction in	demonstrating
identify new	addition to	that (prudent)
ransomware	AV.	statistics for
families, with	• It achieves	Crypto Locker
an average	substantially	account for \$3
detection rate	better	million in
of 93.3%.	outcomes than	revenue in 2013-
	more	2014, among
	simplistic	other things,
	methods and	characterize the
	compares	underground
	favorably with	market for
	more complex	scareware and
	algorithms in	ransomware. In,
		the authors

					terms of	suggest a brand-
					output.	new technique
						for identifying
						and learning
						about malware
						activity.
2020	A Study of	Saurabh	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware	Kumar Sen	paper:	used in this paper:	the paper:	Gap:
	Detection and		• This study lays	• Limit users'	• The major	• With the advent
	Prevention at		the	ability to	objective of	of new
	Organizations		groundwork	install and	this	technologies, it
			for future	utilize	research is to	will become
			studies to	unsuitable	implement	easier to detect
			address the	software	risk using	malware in the
			issue of	programs.	machine	future and to
			ransomware	You should	learning and	reduce business
			attacks in	prevent the	the Python	losses brought on
			businesses.	attachment of	programming	by ransomware.
			Chart	file types of	language in	Additionally, this
			representations	exe/url/tmp/p	accordance	paper inspires

			for cycles are	if/vb/vbe/scr/	with	new analysts and
			known to IT	reg/cer/pst/c	organizational	researchers for
			security	md/bat/dll/hl	research.	the decryption of
			specialists and	p/wsf/hta/js.	• Techniques to	contaminated
			researchers.	• Set up the	limit	files.
				installation of	ransomware	
				host-level	attack gaps in	
				antiexploitati	the network	
				on tools like	and methods	
				the Enhanced	to lessen harm	
				Mitigation	from	
				Experience	ransomware	
				Toolkit.	assaults.	
2019	Situational	Juan A.	The objectives of this	The methodology	The contribution of	Future Work or Future
	Awareness of	Herrera	paper:	used in this paper:	the paper:	Gap:
	Ransomware	Silva and	• Offers a	• Support	• The main goal	• Ransomware
	Attacks—	Lorena	ransomware	vector	of this page is	attacks can
	Detection and	Isabel	article	machines,	to advance	seriously impact
	Prevention	Barona	classification	decision	research in	businesses of all
	Parameters	López	based on	trees, and	this field by	sizes. They

	methods for detection and avoidance. • The ransomware life cycle and the threat detection model.	Bayesian networks (BN). Prevention Detection	the publication of updated papers that compile the most recent findings and offer a comprehensiv e analysis of ransomware.	safeguard systems from ransomware variations by employing customary procedures like antimalware. However, due to ransomware's intelligence and ongoing evolution, these techniques are insufficient to detect and prevent fresh attacks.
--	--	--	--	---

2022	Ransomware	Sonal	The objectives of this	The methodology	The contribution of	Future Work or Future
	Malware and	Yadav and	paper:	used in this paper:	the paper:	Gap:
	Ransomware	Neha Soni	• The analysis of	• Detection By	• Attacks	• In the future,
	Detection		delivery	Signature	should be	individuals and
	Techniques		product assault	• Detection By	stopped by	organizations
			discovery	Behavior	individuals	should stop
			strategies and	• Detection By	and	attacking, and the
			ransomware	Abnormal	organizations,	detection of such
			network	Traffic	and finding	an attack is a
			attacks are the		such attacks is	crucial step in the
			main		a crucial step	ransomware
			objectives of		in developing	attack
			this research.		a ransomware	countermeasure
			There are		attack defense	to secure the
			numerous		strategy.	systems.
			recognition			
			techniques or			
			methodologies			
			that can be			
			used to identify			

			payment			
			product assault.			
			• Network			
			security,			
			malware,			
			ransomware,			
			and			
			ransomware			
			detection			
			methods are			
			some related			
			terms.			
2020	Android	Manish	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware and	Kaushik	paper:	used in this paper:	the paper:	Gap:
	Its Detection	and Leena	• This paper's	• Static,	• This study	• High accuracy
	Methods	Bhatia	primary goal is	dynamic, and	illustrates the	detection
			the detection	hybrid	detection of	techniques for
			of:	approaches	ransomware	mobile
			• Crypto	are used to	using static,	ransomware
			Ransomware		dynamic, and	must be

(File Encryptor	identify	hybrid	developed using
Ransomware)	ransomware.	approaches.	both static and
• Locker		Compared to	dynamic
Ransomware		dynamic	techniques.
(Lock Screen		methods,	
Ransomware).		static methods	
		are more	
		accurate.	
		in order to find	
		ransomware.	
		However, they	
		are useless.	
		with	
		infections	
		during	
		runtime. The	
		shortcomings	
		of static and	
		dynamic	
		approaches	

					are overcome through hybrid approaches.	
2019	Systematic	Alhassan,	The objectives of this	The methodology	The contribution of	Future Work or Future
	literature review	Haruna	paper:	used in this paper:	the paper:	Gap:
	and metadata	Chiroma	• We categorize	• Search/data	• In this paper,	• For future
	analysis of	and	ransomware	sources.	we give a	research, we also
	ransomware	Emmanuel	assault	• Search	thorough	provide proactive
	attacks and	Gbenga	strategies.	keywords.	analysis of	computational
	detection	Dada	• We looked at	• Explicit	ransomware	intelligent
	mechanisms		the criteria	inclusion and	attacks and	prediction
			used to rate	exclusion	countermeasu	models.
			ransomware	criteria.	res. The	Intelligent
			attack,	• Data	publications	techniques
			protection, and	collection	under	published by
			detection	and synthesis	consideration	Abdullahi and
			systems.	of results	clarified	Ngadi,
			• For a future	Study	several	Abdulhamid et
			investigation of	selections.	fundamental	al., and others

the anatomy of	characteristics	can be used to
ransomware,	and signs of	predict a
we collated and	ransomware.	ransomware
summarized all	• The evaluated	attack before it
research	articles	even happens.
datasets that	focused a lot	
were available.	on the	
	environment,	
	particularly	
	the Windows	
	and Android	
	platforms,	
	which serve as	
	a haven for	
	ransomware	
	activities due	
	to their	
	pervasive	
	vulnerabilities	

2017	Ransomware-	Kyun	groul	The objectives	of this	The	methodology	The contr	ibution of	Future	Work	or Fut	ure
	Prevention	Lee,	Insu	paper:		used i	n this paper:	the paper:		Gap:			
	Technique Using	Oh,	and	• This	work	•	Ransomware	• The	suggested	•	In th	ne futu	ure,
	Key Backup	Kangl	oin	offers	a		infiltrates the	rans	somware-		having	;	an
		Yim		preventa	ative		target system	pre	vention		extrem	nely rob	bust
				techniqu	ie for		and activates	tech	nnique in		endpoi	int secu	irity
				user P	Cs in		the	this	study uses		solutio	on will	be
				addition	to a		encryption	а	main-		crucial	l	to
				range	of		feature to	bac	kup		preven	ting	
				systems	, such		encrypt the	pro	cedure to		ranson	nware.	
				as 1	nassive		target	reco	over the		Your	endpo	oint
				platform	ns, to		system's	enc	rypted		device	S	are
				provide			files; in this	file	s from a		equipp	ed w	with
				security	from		case, the	syst	tem that		these	solutio	ons,
				cybercri	me		prevention	has	been		which	prev	vent
				based	on		application	infe	ected by		malwa	re fr	rom
				ransomy	ware.		passes the	ran	somware.		infection	ng y	our
							encryption	Bec	ause		system	18.	
							feature rather	ran	somware				
								use	s aberrant				

than blocking	behaviour,	
it.	such as	
• When the	locking the	
ransomware	victim's	
calls the key-	system or	
generation	encrypting	
and key-	system or	
import	files, to	
methods of	interfere with	
the CNG	a victim's	
library, the	system, this	
hooking code	paper suggests	
gives the key	a key-backup	
to the	technique for	
prevention	which the	
software and	encryption	
then transfers	key is	
execution	maintained in	
control to the	a safe	
ransomware.	repository.	

2021	Android	Iman	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware	Almomani	paper:	used in this paper:	the paper:	Gap:
	Detection Based	Raneem	• The goal of this	• The	• Outline in	• Although more
	on a	Qaddoura	study is to	suggested	detail the most	data and more
	Hybrid	and Maria	detect malware	method is	recent	advanced models
	Evolutionary	Habib	with good	based on a	advancements	to handle the
	Approach in the		performance	combination	in	acquired big
	Context of Highly		using an	of an	ransomware	data, such as
	Imbalanced Data		extremely	oversampling	detection	deep learning
			unbalanced	methodology	technologies.	algorithms that
			dataset.	, a	• By taking into	are more capable
			• Similar to the	classification	account the	of inferring
			Android	strategy, and	most recent	accurate patterns
			Market, there	an	Android	of relationships,
			aren't many	evolutionary	release,	could be used in
			ransomware	process for	provide a	this research
			programmers	optimizing	resent dataset	study to expand it
			compared to	unbalanced	of the Android	into further
			other kinds of	data.	OS (version	research, the
			software.		11, API level	results have

				A. Structure of	30). An	shown the merits
				the particle	unbalanced	of the proposed
				B. Fitness	dataset of safe	approach's
				function	and malicious	capacity to detect
				(internal	applications	Ransomware
				evaluation)	will be created	efficiently
				C. How the	in order to	(97.5% of g-
				algorithm is	simulate the	mean).
				implemented	real-market	
					situation.	
2019	Situational	Juan A.	The objectives of this	The methodology	The contribution of	Future Work or Future
2019	Situational Awareness of		The objectives of this paper:	The methodology used in this paper:	The contribution of the paper:	Future Work or Future Gap:
2019			Ū			
2019	Awareness of	Herrera	paper:	used in this paper:	the paper:	Gap:
2019	AwarenessofRansomware	Herrera Silva and	paper:Modernized	used in this paper: • Intelligent	the paper:Cloud-based	Gap: • Predicting
2019	AwarenessofRansomwareAttacks—	Herrera Silva and Lorena	paper:Modernized methods and	used in this paper: • Intelligent techniques,	the paper: • Cloud-based recovery	Gap: • Predicting ransomware is
2019	AwarenessofRansomwareAttacks—Detectionand	Herrera Silva and Lorena Isabel	paper: ● Modernized methods and strategies for	used in this paper: • Intelligent techniques, including	the paper: • Cloud-based recovery solutions and	Gap: • Predicting ransomware is one of the
2019	AwarenessofRansomwareAttacks—DetectionandPrevention	Herrera Silva and Lorena Isabel Barona	paper: ● Modernized methods and strategies for analyzing,	used in this paper: • Intelligent techniques, including Bayesian	the paper: • Cloud-based recovery solutions and distributed	Gap: • Predicting ransomware is one of the upcoming trends
2019	AwarenessofRansomwareAttacks—DetectionandPrevention	Herrera Silva and Lorena Isabel Barona	paper: • Modernized methods and strategies for analyzing, preventing, and	used in this paper: • Intelligent techniques, including Bayesian Networks	the paper: • Cloud-based recovery solutions and distributed computing	Gap: • Predicting ransomware is one of the upcoming trends in order to spot

			attacks on	support	both	stop the attack in
			Windows	vector	contribute to	time.
			devices. It will	machines	reducing	• Future research
			act as a	(SVM), have	result of	will also focus on
			beginning	been	ransomware	establishing a
			point for	presented in	assaults.	database of
			further	recent study.	Ransomware	information on
			research.	The focus of	attacks are	the financial
			• The first	each of these	rendered	features of
			proposal to	segments is	useless, there	ransom payment
			recapitulate the	the following	will be less	systems.
			criteria used in	action:	incentive in	
			current	• Detection	creating new	
			investigations	Prediction	dangers.	
			is this paper.	• Prevention		
2017	СКҮРТО	ASHWINI	The objectives of this T	The methodology	The contribution of	Future Work or Future
	RANSOMWARE	BALKRUS	paper: u	sed in this paper:	the paper:	Gap:
	ANALYSIS	HNA	• This system's	• The file	• A traditional	• This paper offers
		KARDILE	goal is to	system	method for the	a wealth of
			introduce new	access and	analysis and	insightful

AND	methods for	I/O traces	detection of	information and
DETECTION	automated	implemented	the most	can act as a
USING	ransomware	using Process	recent	cornerstone for
PROCESS	detection	Monitor and	ransomware	numerous
MONITOR	employing	how to setup	was described	upcoming
	dynamic	Cuckoo	in this paper.	efforts. The
	methodology,	Sandbox	This	authors, like
	not merely	along with	technology	anybody else
	dynamic	Virtual	can identify	who creates
	analysis of	machine	the typical	malware-fighting
	malware.	configuration	actions of	methods, express
	• This system		ransomware,	concern about the
	tracks file	• Generating	such as the	possibility that
	access and I/O	realistic user	harmful	malware writers
	traces to find	environment	encryption of	will modify their
	user-level	• File paths.	user's data.	programs once
	malware.	Valid	• This study	more to counter
		Contents.	also	even hardware-
		Monitoring	demonstrates	based strategies
		file system	the	like the one

				activities	interactions a	covered in their
				using Process	ransomware	study.
				Monito.	sample has	
					when it	
					attacks a	
					machine,	
					namely with	
					the file	
					system.	
	Machine	KYUNGR	The objectives of this	The methodology	The contribution of	Future Work or Future
2019	Learning Based	OUL LEE,	paper:	used in this paper:	the paper:	Gap:
	File Entropy	SUN-	• The key	• Entropy	• The	• In the future,
	Analysis for	YOUNG	advantage of	measurement	ransomware	we'll get
	Ransomware	LEE, AND	employing a	methods	detection	outcomes for a
	Detection in	KANGBIN	backup	• Machine	methods now	range of file
	Backup Systems	YIM2	solution is the	learning	in use do not	types and
			user's ability to	MODELS	detect	investigate a
			back up their	1. LINEAR	malware files	method for
			files. If a user's	MODEL	within	artificially
			files have been	2. KNN	backup.	identifying

encrypted by 3. DEC	CISION However, this	ransomware by
ransomware, TRE	EE paper	figuring out the
they can restore ENS	SEMBLE effectively	ideal settings and
their original 4. DEC	CISION detects	parameters for
contents by TRE	EE ransomware-	every individual
synchronizing ENS	SEMBLE infected files	user on every
or transferring 5. KER	RNEL delivered to	user's backup
data from TRI	CK the backup	files.
backup 6. NEU	JRAL system in real	
systems, NET	TWORK time using the	
including cloud (DE	EP reference	
services like LEA	ARNING) value derived	
Dropbox and • Mod	lel through	
Google One valie	dation Machine	
Drive, USB	Learning	
storage, and	Based File	
external	Entropy	
devices.	Analysis for	
However, if the	Ransomware	
ransomware-	Detection in	

			infected files		Backup	
			are synced to		Systems	
			the backup		machine	
			system, the		learning based	
			files cannot be		on entropy	
			restored using		according to	
			the backed-up		different file	
			files.		formats.	
-2021	A framework for	Francesco	The objectives of this	The methodology	The contribution of	Future Work or Future
	supporting	Mercaldo	paper:	used in this paper:	the paper:	Gap:
	ransomware		• The system	• Static	• In this study,	• As part of our
	detection and		created in this	analysis	we proposed a	ongoing
	prevention		research aims	enables us to	hybrid	research, we
	based on hybrid		to reduce and	extract from	solution to	intend to assess
	analysis		prevent	the	counter the	the suggested
			ransomware	executable	ransomware	framework's
			threats. It	beneath	threat that	performance on a
			includes a top-	scrutiny a list	uses both API	wider range of
			level design or	of such APIs	calls and	applications,
			an evaluation	and libraries	commands	

of the	being used	(via static	both good and
suggested	using a	analysis) (by	bad.
framework.	reverse	dynamic	• To improve
	engineering	analysis). We	accuracy for the
	technique.	tested the	tasks of
		ability of	ransomware
		using API	detection and
		calls and	mitigation, we
		commands,	also intend to
		separating	consider the
		malware from	adoption of
		genuine	formal
		programs	approaches.
		using the	
		Cuckoo	
		framework,	
		and we found	
		positive	
		findings.	

2019	A Study of	Aini	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware	Khalida	paper:	used in this paper:	the paper:	Gap:
	Attacks:	Muslim1,	• The evolution	• Ransomware	• This study	• The widespread
	Evolution and	Dzunnur	of ransomware	attacks have	will help new	usage of
	Prevention	Zaily Mohd	assaults and	been	researchers	industrial robots
		Dzulkifli	methods for	analyzed	find research	in industry and
			diagnosing	using	gaps by	the
			ransomware	qualitative	providing	infrastructural
			were examined	research as a	summaries of	sectors that link
			in this study.	tool. The	previously	smart cities are
			This study	information	published	examples of
			poses two	gathered for	research	larger targets that
			questions,	this study's	publications.	attackers may
			including	research is		choose to attack
			"How have	secondary		in the future.
			ransomware	information.		• Cybercriminals
			assaults	Field		can invent,
			evolved over	research can		launch, and profit
			time?"	be used to		greatly from this
			likewise, "How	gather		threat of

	to handle the	secondary	cybercrime in the
	escalating	data.	future.
	ransomware	• Examples of	
	attacks?"	secondary	
		data for	
		social science	
		include	
		information	
		from	
		organizations	
		and	
		scrutinized	
		government	
		agencies, in	
		addition to	
		data that	
		were first	
		obtained for	
		various	

				research		
				purposes.		
-2021	SDN-Based	FAHAD M.	The objectives of this	The methodology	The contribution of	Future Work or Future
	Detection of Self-	ALOTAIBI	paper:	used in this paper:	the paper:	Gap:
	Propagating	AND	• One of the	• THE WORM	BadRabbit	• In upcoming
	Ransomware:	VASSILIO	main goals of	COMPONE	underwent a	work, a strategy
	The Case of	S G.	our work is to	NT	thorough	to evaluate the
	BadRabbit	VASSILA	understand the	• THE	investigation,	IDPS's
		KIS	process	ENCRYPTI	and it was	effectiveness and
			through which	ON	discovered	performance in a
			this kind of	COMPONE	that this	real network. The
			targeted	NT	family of	existence of
			ransomware	• ENCRYPTI	ransomware	various
			operates.BadR	ON	does not	programmers,
			abbit Analysis	PROCESS	interact with	realistic
				• ENCRYPTI	other entities	background
				ON	in order to	traffic, and the
				PROCESS	exchange an	operation of
				PROPAGAT	encryption	additional
					key. Instead, it	security

				ION	makes use of a	appliances and
				METHODS	public key that	features will all
					is built into its	be taken into
					data.	account for
						validation
						reasons.
2014	DNA-Droid: A	Amirhossei	The objectives of this	The methodology	The contribution of	Future Work or Future
	Real-time	n Gharib	paper:	used in this paper:	the paper:	Gap:
	Android		• Discovered	• Static	• A freely	• Explore new
	Ransomware		novel traits	Analysis	accessible,	sources of
	Detection		with strong	• Text	fully	information.
	Framework		discriminative	Classificatio	automated	• Visualization of
			strength that	n Module	Android	the DNAs.
			enable the	(TCM)	sandbox that	• Experiment on a
			DNA-Droid to	• Image	can report the	larger dataset.
			identify	Classificatio	order of API	• Experiment with
			unidentified	n Module	calls as a web	real malware.
			ransomware	(ICM)	service was	
			samples.	• API calls and	made	
				permissions	available.	

• Examined how	Module	• Used an	
well Deep Auto	(APM)	extensive	
Encoder	• Feature	collection of	
reduced and	Learning and	various	
picked up new	Reduction	ransomware	
features.	• Dynamic	samples for	
	Analysis	experimental	
	• Sandbox	examination.	
	• API Calls		
	Refining		
	• Multiple		
	Sequence		
	Alignment		
	(MSA)		
	• Detection		
	Module		
	• Static		
	Classificatio		
	n		

				• DNA		
				Matching		
2018	The Ransomware	Baris	The objectives of this	The methodology	The contribution of	Future Work or Future
	Detection and	CELIKTA	paper:	used in this paper:	the paper:	Gap:
	Prevention tool	S	• Demonstrate	• Static	• A thorough	• Users have a
	design by		the hybrid	detection	analysis of	better
	using signature		process	technique	pertinent	understanding of
	and anomaly-		ransomware	• Dynamic	literature and	the key traits of
	based detection		prevention and	detection	expert reports	the Ransomware
	methods		detection	technique	indicates that	Prevention and
			solution, which	• Hybrid	relying solely	Identification
			seeks to	detection	on the	Tool that may be
			operate well on	technique	signature-	used as a remedy,
			Windows OSs	• Method of	detection	software
			with a minimal	detection	process to	developers, and
			amount of false	based on	identify and	security
			positive alerts.	signatures	stop malware	managers as a
			• Consider the	Method for	is ineffective.	result of this
			fact that this	anomaly-		study.
			concept will act			

			as a guide for	based		• This work will
			scholarly	detection		serve as a guide
			investigation of	• Ransomware		for upcoming
			ransomware.	Detection		scholarly
				Methods		investigations of
						malware,
						including
						ransomware.
2022	Ransomware	Adhirath	The objectives of this	The methodology	The contribution of	Future Work or Future
	Detection,	Kapoor,	paper:	used in this paper:	the paper:	Gap:
	Avoidance, and	Ankur	• Extremely	• Ransomware	• We present	• Future work will
	Mitigation	Gupta, and	risky	recognition,	DAM, a	concentrate on
	Scheme:	Innocent E.	Ransomware	static,	conceptual	developing a
	A Review and	Davidson	assaults have	dynamic,	framework for	browser
	Future Directions		suddenly	hybrid, string	evaluating and	extension
			increased,	extraction,	classifying the	powered by
			crippling both	PE file	tools,	artificial
			individuals and	segments,	approaches,	intelligence that
			most	static linking,	and mitigation	will be used to
			enterprises.	stub analysis,		monitor both

			Ransomware is	automated	methods for	personal and
			a serious	sandboxing,	ransomware.	corporate online
			menace that	manual code	• We proposed	safety.
			requires an	reversing,	a continuum	
			international	manual	for preventing	
			response.	debugging,	ransomware.	
			• The best	malware	Different	
			ransomware	reconstructio	enterprises,	
			prevention	n, machine	from small	
			methods	learning	businesses to	
			require	classifiers,	critical	
			specialized	and memory	deployments,	
			mitigation and	dump	can use this	
			recovery	evaluation.	continuum.	
			efforts.			
2020	Analysis,	Ziya Alper	The objectives of this	The methodology	The contribution of	Future Work or Future
	Detection, and	Genç	paper:	used in this paper:	the paper:	Gap:
	Prevention		• To develop a	• The steps that	• In this	• This section
	of Cryptographic		protection	make up the	research, we	serves to alert the
	Ransomware		system that	detection	investigated	scientific

pushes the	process we	potential	community to
boundaries of	use in this	restrictions	potential
technology by	chapter are as	decoy tactics	ransomware
researching	follows:	may run	threats.
ransomware	First, we	against when	• Keeping anti-
behavior,	collect the	used to	ransomware
flaws, and	traces by	combat	ideas in mind in
cryptographic	repeatedly	ransomware.	advance could be
origins.	running a	We start by	a game-changing
	malware	addressing the	element because
	sample in a	problem	it is predicted
	sandbox.	theoretically,	that the
	• Subsequently	and we then	ransomware
	, we look to	explain a real-	threat will grow
	see if the	world proof-	in sophistication
	sample	of-concept	rather than in
	engaged in	that	quantity of
	any	demonstrates	attacks.
	suspicious	how certain	
	behavior	existing	

				during the	decoy-based	
				initial run but	solutions can	
				then behaved	be easily	
				maliciously	thwarted.	
				during		
				subsequent		
				runs. If this is		
				the case, it		
				indicates that		
				the malware		
				has some		
				evasive		
				capabilities.		
	Ransomware	Marvic	The objectives of this	The methodology	The contribution of	Future Work or Future
2018	Activity Detection	Grima	paper:	used in this paper:	the paper:	Gap:
			• The main	• Sandbox	• The results of	Additional
			objective of	Environment	this study	investigation
			this research is	• Prototype	suggest that	using a larger
			to determine	Ransomware	monitoring	sample size can
			whether		file access by	reveal additional

	behavior of ransomware detection can enhance security prior to the delivery of new anti- malware signatures by the anti- malware solution provider.	Detection Application Hardware Software Features Activity Monitoring Mechanism Process Information Collection Sollection Watchdog Detector Protector Protection Mechanism Configuratio n Configuratio n	active processes on a Windows computer is a useful method for spotting dangerous ransomware activities.	techniques to enhance and maximize the effectiveness of the detection systems as well as uncover fresh defenses against the execution of the destructive encryption process itself.
--	---	---	---	--

2019	Analysis of		The objectives of this	The methodology	The contribution of	
	Infection,	Akbanov	paper:	used in this paper:	the paper:	Gap:
	Persistence,	and	• In addition to	• Static and	• This study	• The results of
	Recovery	Vassilios G	conventional	dynamic are	concentrated	this study could
	Prevention and		security	two major	on the first	be applied to the
	Propagation		measures, new	categories	interactions	development of
	Mechanisms		countermeasur	that apply to	and infection	efficient
			es are seen as a	techniques.	process of	WannaCry and
			crucial and	While	WannaCry, as	other
			fashionable	dynamic	well as its	ransomware
			responsibility	analysis	persistence	families that
			in this industry.	includes	mechanism,	display similar
			• However, to	running the	encryption	behavior
			create such a	malicious	process,	mitigating
			solution, a	binary in a	recovery	measures. The
			thorough	controlled	prevention,	work on this is
			examination of	environment,	and	postponed.
			ransomware	static	communicatio	
			behavior and	analysis is		

			functionality is	carried out	n with C&C	
			necessary.	without	servers.	
				doing so.		
2020	RAPPER:	Manaar	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware	Alam1,	paper:	used in this paper:	the paper:	Gap:
	Prevention via	Sayan	• Provide a two-	• The	• In this paper,	• Recovering the
	Performance	Sinha	step	RAPPER	we give a	AES key by
	Counters		unsupervised	two-step	thorough	focusing on the
			detection tool	detection	explanation of	AES CBC
			that finds	framework	how	process would be
			malicious	employs Fast	ransomware	a difficult task.
			process activity	Fourier	affects typical	We will save that
			with the least	Transformati	system	for a later scope
			number of	on and	operations.	of work, though.
			traces possible	Artificial	Using a two-	
			when it thinks a	Neural	step detection	
			process activity	Network to	methodology,	
			to be	create a	we enlist the	
			malicious.	highly	help of an	
				accurate,	artificial	

				quick, and	neural	
				reliable	network to	
				ransomware	find the	
				detection	presence of	
				method with	ransomware.	
				a minimum		
				number of		
				trace points.		
				• The two		
				phases of the		
				detection		
				process are		
				called the		
				Offline Phase		
				and the		
				Online		
				Phase.		
2020	A Three-Level	Amos Lo	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware	Yee Re	paper:	used in this paper:	the paper:	Gap:

Detection and	and Chong	• Instead of	Vaccination	• The notion of	• As technology
Prevention	Tze Liang	enabling	from Not	Petya and Not	advances, we
Mechanism		malware to	Petya	Petya is	anticipate being
		infect the host	• Updates and	covered in this	able to run more
		system, the	Patches	study;	virtual computers
		objective is to	• Anti-	whereas Petya	on a single
		separate	Malware &	encrypts only	computer.
		potentially	Anti-	the MBR, Not	Virtual machines
		hazardous	Ransomware	Petya encrypts	may prove to be
		items into a	software	both files and	an efficient
		virtual	• Least	the MBR.	deterrent to
		environment	Privilege	• With the	malware,
		and place it in	Principle	ability to act	according to our
		quarantine.	• Prudence,	like a worm	research, and this
			Self-	and take	is a positive
			awareness,	advantage of	development in
			and Logic	open	the fight against
				vulnerabilities	malware.
				, Not Petya	
				arose.	

2020	Analysis of	A. D. C	The objectives of this	The methodology	The contribution of	Future Work or Future
	Ransomware and	Navin	paper:	used in this paper:	the paper:	Gap:
	its prevention	Dhinnesh	• Users should	• Keep your	• The history	• Ever since
			be warned not	System	and	ransomware was
			to click on any	Isolated	development	first identified in
			dubious links	• Avoid Paying	of	2000, it has
			they receive	Ransom	ransomware	caused extensive
			through email.	• Do not click	are explained	damage. Up until
			For these kinds	the unknown	in this study. It	now,
			of attacks,	links	also examines	ransomware
			companies	• Never open	the decision to	prevention has
			must employ a	unknown	use encryption	been described.
			few security	email	for	Let's examine
			measures.	attachments	ransomware	how to react to a
			Their software	• Use proper	attacks.	ransomware
			needs to be	filtering	• In this paper,	attack now.
			updated	• Update	the author	
			properly.	software	discusses how	
				periodically	to avoid	
				1 5	ransomware	

Periodic Data	and how to	
Back up	deal with an	
	attack.	

Chapter 3

DESIGN AND METHODOLOGY

3.1 Methodology:

Utilize exploratory data analysis to examine dataset columns and rows. We will then have a dataset with pre-selected columns and traits for further research. We will now produce visualizations or graphs of the data we collected after running the program.

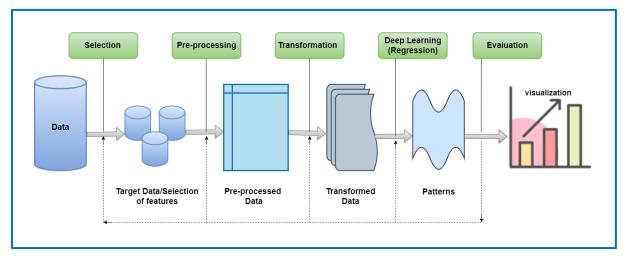


FIGURE 3.1: METHODOLOGY DIAGRAM

Stages of progress throughout the project

- i. Data collection
- ii. Target Data
- iii. Data preprocessing

- iv. Transformed Data
- v. Patterns
- vi. Knowledge or Result

3.1.1 Data:

The first step is to gather data. Data can take the shape of text, comments, graphics, photographs, statistics, charts, and signs. The data might, for example, comprise specific dates, costs, sizes, addresses, ages, names, temperatures, or lengths. Data lacks significance and use on its own since it is an incomplete sort of knowledge. A data set is a collection of data or dataset. Within scenario of tabular data, a data set is associated with one or more database tables, where each row alludes to a particular record in the associated data set and each column to a particular parameter. Our dataset consists of 100,000 samples of ransomware attack.

3.1.2 Target Data (Dataset):

Our target data is Ransomware. While gathering the ransomware set of data was an essential component of our study, we go into considerable depth in this section regarding how we chose the ransomware samples. We gathered malware samples from many sources to create a complete ransomware data collection. The collected ransomware data set consists of 100,000 samples. Dataset is **Bitcoin Heist** that contain different amount of data in the form of table which has numbers of entities like row number, address, year, date, day, length, weight and count etc. Every row and column contain different of different person and of different year. The dataset needs some data mining like data cleaning or data pre-processing.

3.1.3 Data preprocessing

Data preprocessing, which is an important step in the data mining procedure, may be described as the modifying or deleting of data before to use in order to ensure or enhance performance. Rubbish in, garbage out is especially true for projects requiring data mining and machine learning. For the preprocessing of dataset number of attributes are label, year, count, date, length, day, and address etc. Then heat map is generated of the processed data [9].

3.1.4 Attributes and Type

Attributes	Туре
Address	String
Income	Decimal
Looped	Integer
Length	Integer
Weight	Float
Count	Integer
Day	Integer
Neighbours	Integer
Year	Integer
Label	String

TABLE 3.1: ATTRIBUTES AND TYPES

3.1.5 Transformed Data:

Data transformation is the process of converting data from one format, such as an Excel spreadsheet database file, or XML document, into another. Transformations often entail cleaning,

validating, and making useable a raw data source. Then heat map is generated of the processed data.

3.1.6 Transformed Data Attributes and type

Attributes	Туре
Length	Integer
Weight	Float
Count	Integer
Neighbor	Integer
Income	Decimal
Label	String

TABLE 3.2: TRANSFORMED DATA ATTRIBUTES AND TYPE

3.1.7 Patterns:

Data analysts search for patterns in the present data by looking for sets of data that have a recognized pattern. Because each dataset is unique, it's important to recognize patterns and trends in the underlying data. If a company wants to provide accurate, trustworthy results, it must choose the algorithm and strategy that are most suited for the data and analysis.

3.1.8 Knowledge or Result:

See chapter five.

3.2 Deep Learning:

The core of H2O's deep learning system is a multi-layer feedforward artificial neural network that was trained using stochastic gradient descent via back-propagation. The network may have several hidden layers made up of neurons with the tanh, rectifier, and max out activation functions [10]. Let's think about how a neural network calculates a single unit. Y is the output, z is the weighted input, and (z) is the activation function that simulates the sigmoid function.

Nowadays, ReLU function is advised as an activation function instead of sigmoid function since it solves "The vanishing gradient problem." The function that mimics the neurons in a human brain, step function, was replaced by the sigmoid function, a basic differentiable activation function. In the tutorial that follows, we'll use the sigmoid function to help us better comprehend backpropagation. In this tutorial, the sigmoid function will be used.

$$z = x1w1 + x2w2 + b$$
$$y = \sigma(z) = 11 + exp(-z)$$

The inputs are x1 and x2. The coefficient weights for each input are w1, w2.

In essence, x1 and x2 represent data that have undergone normalization or standardization. Better performance is made possible by techniques like applying normalization or standardization to input data. For instance, when normalizing a picture with a 0-255 color range, we divide the picture by 255 to get a 0-1 color range. Gradients exist in the early learning state because the weights initialize in a small range. There are techniques for initializing weights, including using a Gaussian distribution. We will set the values in this tutorial from 0 to 1. Due to initial 0 bias producing improved learning accuracy, bias is set to 0. The bias will be updated as more is learned.

3.3 Gradient-boosted trees (GBM):

This algorithm's main idea is to create models sequentially while aiming to reduce the shortcomings of the previous model. However, how should we approach that? What can be done to reduce the error? This is achieved by building a new model on the residuals or mistakes of the previous one [11].

Progressive Boosting When the target column is continuous, a regressor is utilized; if classification is the issue, a gradient boosting classifier is. The "Loss function" is the sole difference between the two. Gradient descent will be used to increase weak learners and decrease this loss function. We will have a variety of loss functions for regression issues, such as for classification problems and Mean Squared Error, such as log-likelihood, since it is based on a loss function.

Formula:

$$Fm(x) = Fm_1(x) + vmhm(x)$$

The number of decision trees created is m. Here, nu is the learning rate, which is typically chosen between 0-1, and Fm-1(x) is the prediction of the base model (prior prediction). Long-term accuracy is increased since it lessens the impact that each tree has on the outcome of the prediction. The most recent DT performed on the residuals is Hm(x).

3.4 Random Forest:

To address classification and regression problems, the Random Forest Algorithm, a very well-liked supervised machine learning method, is used. A forest is made up of several different species of

trees, and the forest will be more vigorous the more trees there are. In this way, as the number of trees in a Random Forest Algorithm increase, so do its accuracy and ability to solve problems [12].

The steps listed below are how the Random Forest Algorithm functions:

- Step 1: Select randomly selected samples from a specified data collection or training set.
- ✤ In step 2, this algorithm will create a decision tree for each training batch of data.
- ✤ The third decision tree's average will be used to perform the voting.
- ♦ As the last prediction result in step 4, select the outcome that garnered the greatest support.

This combination of several models is referred to as an ensemble. Ensemble uses two methods:

Boosting: Is the process of transforming weak learners into strong ones through the development of subsequent models with the aim of reaching the highest level of accuracy. XG BOOST and ADA BOOST are two examples.

Bagging: Bagging is the method of replacing a sample training dataset with a different training subset. A majority vote is required to determine the result.

Chapter 4

DATA AND EXPERIMENTS

4.1 Download Dataset from Kaggle:

Data scientists and machine learning experts may connect online at Kaggle. Users of Kaggle may work together, access and share datasets, use notebooks with GPU integration, and compete with other data scientists to solve data science problems [13].

The dataset is Bitcoin Heist Ransomware Address.

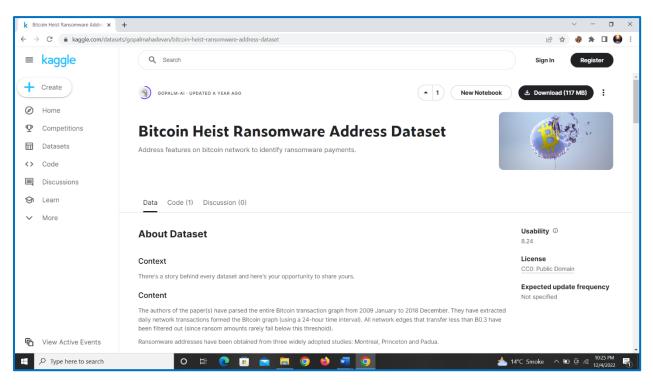


FIGURE 4.1: KAGGLE DATASET RANSOMWARE

→ C	asets/gopalmahadevan/bitcoin-heist-ra						☞ ☆		1 😫	
⊧ kaggle	Q Search						Sign In	Register		
Create		Bitcoin Heist Ransomware Address Dataset Data Code (1) Discussion (0)								
) Home										
Competitions	BitcoinHeistDat	ta.csv (235.88 MB)		¥ []	>	Data Explorer Version 1 (235.88 Mi	3)		
Datasets			,				BitcoinHeistData			
Code	Detail Compact	Column			10 of 10 columns	~				
Discussions	▲ address =	# year =	# day =-	# length =	# weight =	# c				
Learn	Bitcoin address (string)	integer	integer (1-365)	integer	FIGAL	inte				
More										
	2631095 unique values	2011 2018	1 365	11	0 1.94k					
	111K8kZAEnJg245r2cM6 y9zgJGHZtJPy6	2017	11	18	0.0083333333333333333	1				
	1123pJv8jzeFQaCV4w64 4pzQJzVWay2zcA	2016	132	44	0.000244140625	1				
	112536im7hy6wtKbpH1q YDWtTyMRAcA2p7	2016	246	0	1	1				
View Active Events	1126eDRw2wqSkWosjTCr e8cjjQW8sSeWH7	2016	322	72	0.00390625	1				

FIGURE 4.2: BITCOIN HEIST RANSOMWARE ADDRESS DATASET

4.2 Download and Install RapidMiner:

RapidMiner is a potent data mining program that supports model deployment, model operations, and data mining. All the data preparation and machine learning skills required to make a significant effect throughout your business are provided by our end-to-end data science platform [14].

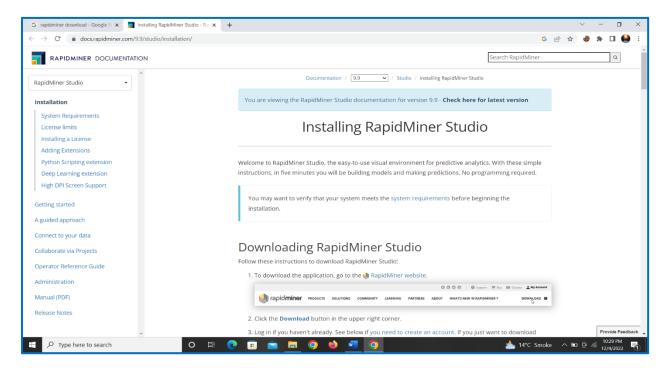


FIGURE 4.3: RAPIDMINER INSTALLATION

4.3 Heat Map:

In a two-dimensional heatmap, a graphical representation of data, the individual values included in a matrix are shown as colors. A matrix of the variables that is colored according to the intensity of the value is called a heatmap. As a result, it provides an excellent visual tool for contrasting numerous objects. This heat map show there is no null values in dataset [15].

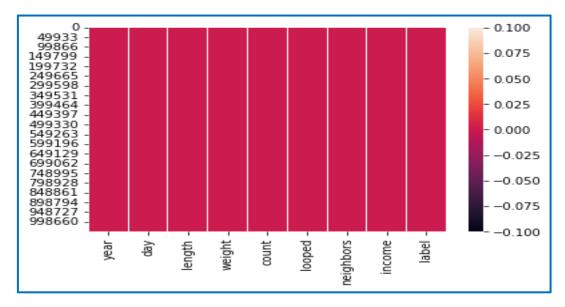


FIGURE 4.4: HEAT MAP

4.4 Import the Dataset:

Utilizing the drag and drop functionality is all that is required to import data into your repository.

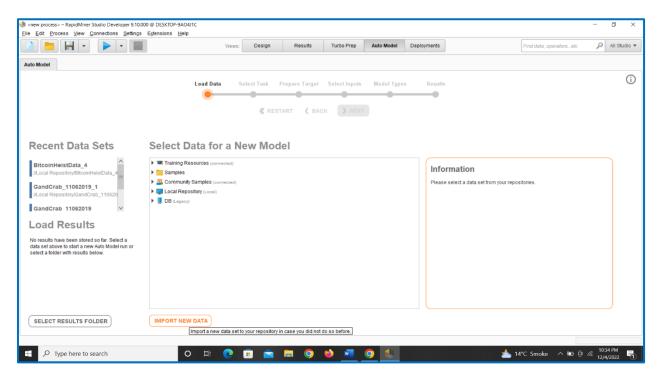


FIGURE 4.5: IMPORT DATA

4.4.1 Select the location:

🧶 <new process=""> – RapidMiner Studio Developer</new>			– 🗆 🛛
Eile Edit Process View Connections Se	Import Data - Where is your data? X	1	
	import Data - where is your data?	data, operatorsetc	🔎 All Studio 🔻
			•
Auto Model	Where is your data?		
		-	
			(j)
	My Computer		
	My Computer Database		
	Import data from file-based data sources like Excel, CSV, SAS or Access.		
	Get support for more data sources from the RapidMiner Marketplacet		
Recent Data Sets			
Recent Data Sets			
BitcoinHeistData_4			
//Local Repository/BitcoinHeistData_4			
GandCrab_11062019_1		3.	
//Local Repository/GandCrab_110620			
GandCrab 11062019 V			
Load Results			
No results have been stored so far. Select a			
data set above to start a new Auto Model run select a folder with results below.			
SELECT RESULTS FOLDER			
Type here to search	O 🖽 💽 🛱 🚔 🧱 💽 🍅 🚾 💽 🐔 📥 14°C	Smoke 🔨 🖻 🖗	10:34 PM
			12/4/2022

Simply drag the file into the canvas from your file browser and continue.

FIGURE 4.6: SELECT LOCATION

4.4.2 Select the Data:

Verify that the target or label is correctly tagged and that the data types are accurate. This method of opening data differs significantly from other methods in that it does not constantly read the original source file from scratch. Therefore, you must overwrite the stored data if you want to update.

- - -	🐠 Import Data - Select th	e data location.			X 1 data, operato	rsetc 🔑 All Stu
el		Select th	ne data location.			
	Bitcoin_Dataset			▼ ← 📮 🚖 🚖	•	
	Bookmarks	File Name	Size	Type Last Modified		
	★ Last Directory	BitcoinHeistData.csv	224 MB 42 MB	Microsoft Excel Comma Se Mar 30, 2022 Microsoft Excel Comma Se Nov 5, 2022	^	
		BitcoinHeistData_2.csv	33 MB	Microsoft Excel Comma Se Nov 6, 2022		
		BitcoinHeistData_3.csv BitcoinHeistData_4.csv	30 MB 31 MB	Microsoft Excel Comma Se Nov 6, 2022 Microsoft Excel Comma Se Nov 6, 2022		
ent Data Sets		download.png	18 KB	PNG File Nov 5, 2022		
nHeistData_4 Repository/BitcoinHeistData_4						
crab 11062019 1					s.	
Repository/GandCrab_110620						
Crab 11062019						
Results						
s have been stored so far. Select a						
above to start a new Auto Model run o older with results below.						
					~	
	BitcoinHeistData.csv					
	All Files				*	
				The selected file will be imported as: CSV	Change	
CT RESULTS FOLDER				← Previous → Next Go to the	next page.	

FIGURE 4.7: SELECT DATA

to Model						Specify your	data forn	nat					
	✓ н	leader Row			1 🗘 🛛 File	Encoding	windows-12	52 💌	🕑 Use Quotes	-			(
	Start F	Row			1 CESC	Escape Character			Trim Lines				
	Colun	nn Separator	(Comma ","	▼ Dec	mal Character			🛃 Skip Commen	s #		1	
	1	address	year	day	length	weight	count	looped	neighbors	income	label	<u>_</u>	
Recent Data Sets	2	111K8kZAE	2017	11	18	0.00833333	1	0	2	100050000	princetonCe		
vecent Data Sets	3	1123pJv8jz	2016	132	44	0.00024414	1	0	1	1e+08	princetonLo		
BitcoinHeistData 4	4	112536im7	2016	246	0	1	1	0	2	2e+08	princetonCe		7
//Local Repository/BitcoinHeistData_4	5	1126eDRw	2016	322	72	0.00390625	1	0	2	71200000	princetonCe		
GandCrab_11062019_1 //Local Repository/GandCrab_110620	6	1129TSjKb	2016	238	144	0.07284840	456	0	1	2e+08	princetonLo	s.	
	7	112AmFATx	2016	96	144	0.08461399	2821	0	1	5e+07	princetonLo		
GandCrab 11062019	8	112E91jxS2	2016	225	142	0.00208851	881	0	2	1e+08	princetonCe		
	9	112eFykaD	2016	324	78	0.00390625	1	0	2	100990000	princetonCe		
.oad Results	10	112FTiRdJj	2016	298	144	2.30282830	4220	0	2	8e+07	princetonCe		
	11	112GocBgF	2016	62	112	3.72529029	1	0	1	5e+07	princetonLo		
io results have been stored so far. Select a ata set above to start a new Auto Model run c	12	112gXL4Ae	2013	317	4	0.00714285	2	0	1	1e+08	montrealCry		
elect a folder with results below.	13	112nEBUad	2016	247	0	1	1	0	2	108560000	princetonCe		
	14 15	112Ns49Uo	2016	146	144	0.87748478	4817	0	1	104020000 5.6e+07	montrealCry		
	15	112vq2Wt7 112wED5u	2017	3	4	3.05175781		0	2	5.5e+07 1.2e+08	princetonCe montrealCry		
	10	112wED5u	2016	156	8	0.75	2	0	4	2.4e+08	montrealCry		
		112WED30	2010	150		0.75		~		2.40100	mondearciy	1	
											🥝 no problems.)
SELECT RESULTS FOLDER									- Prev	ious → Ne	t X Cancel		

FIGURE 4.8: SELECT DATA FORMAT

				_						t data, operatorsetc 🔎
to Model				F	ormat your co	lumns.				
	I	Qate format Enter va	lue	•	Replace	errors with missing v	alues ①			
		address 🔹 🕶	year O 🕶 integer	day 🗢 🕶 Integer	length 🗢 👻 integer	weight Ø 🕶 real	count © •	looped • •	neighbors Integer	
	1	111K8kZAEnJg2	2017	11	18	0.008	1	0	2 ^	
	2	1123pJv8jzeFQa	2016	132	44	0.000	1	0	1	
Recent Data Sets	3	112536im7hy6wt	2016	246	0	1.000	1	0	2	
	4	1126eDRw2wqS	2016	322	72	0.004	1	0	2	
BitcoinHeistData_4	5	1129TSjKtx65E3	2016	238	144	0.073	456	0	1	
//Local Repository/BitcoinHeistData_4	6	112AmFATxzhuS	2016	96	144	0.085	2821	0	1	
GandCrab_11062019_1	7	112E91jxS2qrQY	2016	225	142	0.002	881	0	2	3.
//Local Repository/GandCrab_110620	8	112eFykaD53KE	2016	324	78	0.004	1	0	2	
GandCrab 11062019 🗸	9	112FTiRdJjMrNg	2016	298	144	2.303	4220	0	2	
	10	112GocBgFSnao	2016	62	112	0.000	1	0	1	
_oad Results	11	112gXL4AeJ62D	2013	317	4	0.007	2	0	1	
No results have been stored so far. Select a	12	112nEBUadWiMx	2016	247	0	1.000	1	0	2	
data set above to start a new Auto Model run c select a folder with results below.	13	112Ns49UobQn	2016	146	144	0.877	4817	0	1	
select a folder with results below.	14	112vq2Wt7Mo8R	2017	3	4	0.016	1	0	2	
	15	112wED5uHhY1	2016	158	56	0.000	1	0	1	
	16	112wED5uHhY1	2016	156	8	0.750	2	0	4	
	17	112wjYgWapZU8	2016	273	144	0.009	1168	0	1	
	10	<	0040		1	0.440		•	· · · · · ·	
								0	🕗 no problems.	
SELECT RESULTS FOLDER								revious → Next	X Cancel	
SELECT RESULTS FOLDER								iewous — Next	A Cancel	

FIGURE 4.9: FORMAT COLUMNS

4.4.3 Save the Data:

However, once the import is complete, a local copy is maintained in RapidMiner's repository, allowing you to choose to delete the original source file if you so desire.

🥠 <new process=""> – RapidMiner Studio Developer</new>			– 0 ×
Eile Edit Process View Connections Se	Import Data - Where to store the data?	1	
	import Data - where to store the Data:	data, operatorsetc	🔎 All Studio 🔻
Auto Model	Where to store the data?		
		-	0
	Local Repository (Local)		(i)
Descript Data Cata			
Recent Data Sets			
BitcoinHeistData 4			
//Local Repository/BitcoinHeistData_4			
		5.	
GandCrab_11062019_1 //Local Repository/GandCrab_110620			
//Local Repository/GandCrab_110620			
GandCrab 11062019 V			
Lood Deputée			
Load Results			
No results have been stored so far. Select a			
data set above to start a new Auto Model run select a folder with results below.			
select a lotder with results below.			
	Name BitcoinHeistData		
	Location //Local Repository/BitcoinHeistData	-	
SELECT RESULTS FOLDER	- Previous 🛛 Einish 💥 Cancel		
	Finish.		
Type here to search	O Hì 💽 🛱 💼 💿 ڬ 🐖 🧿 🌜	Smoke 🔨 🖬 🛱	//: 10:35 PM 12/4/2022
>> Type here to search		Silloke 🔨 🖬 😳	12/4/2022

FIGURE 4.10: SAVE THE DATA

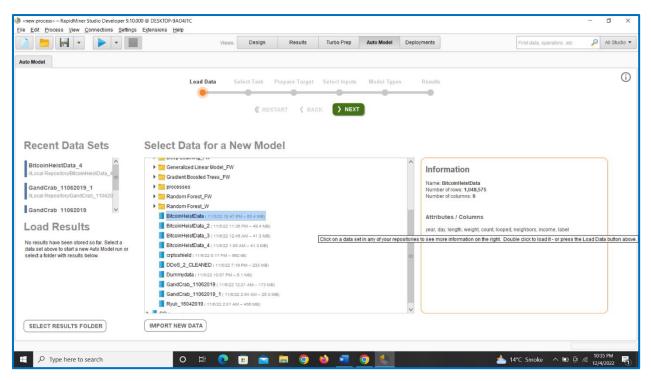


FIGURE 4.11: SELECT DATA OF NEW MODEL

4.4.4 Set the target Class:

After choosing a data set, you must determine the kind of issue you wish to address. Three different tasks are identified by Auto Model:

- Predict
- Clusters
- Outliers

à 📒 F	- ·		Views: Design	Results T	urbo Prep Auto Model	Deployments	Fh	nd datā, operators…etc 🛛 🔎	All Studio
uto Model									
		Load Dat	a Select Task F	Prepare Target Se	ect Inputs Model Types	Results			C
		-							
			« REST	ART 🕻 BACK) NEXT				
					Confirms the current selection	on and moves on to the next ste	ep in Auto Model.		
		Pre	dict	Cluster	s	Outliers			
		Want to predict the	values of a column?	Want to identify groups	in your data? Want to d	detect outliers in your data?			
ear	day	length	weight	count	looped	neighbors	income	label	
umber	Number	Number	Number	Number	Number	Number	Number	Category	0
2017	11	18	0.008	1	0	2	100050000	princetonCerber	~
2016	132	44	0.000	1	0	1	10000000	princetonLocky	
2016	246	0	1	1	0	2	20000000	princetonCerber	
016	322	72	0.004	1	0	2	71200000	princetonCerber	
016	238	144	0.073	456	0	1	20000000	princetonLocky	
016	96	144	0.085	2821	0	1	5000000	princetonLocky	
016	225	142	0.002	881	0	2	10000000	princetonCerber	
016	324	78	0.004	1	0	2	100990000	princetonCerber	
016	298	144	2.303	4220	0	2	80000000	princetonCerber	
016	62	112	0.000	1	0	1	5000000	princetonLocky	
013	317	4	0.007	2	0	1	10000000	montrealCryptoLocker	~
				3,575 rows - 9 columns (1 r					1040

FIGURE 4.12: SELECT TARGET CLASS

4.4.5 Prepare Target:

The issue is a classification issue because there are only two possible answers for "Survived," "Yes" or "No." Auto Model will typically show a bar chart with the data points in each class categorization issues. Only ten classes with the greatest number of data points are shown when there are more than ten classes.

🌒 <new process=""> – RapidMiner Studio Developer 9.10.000 @ DESKTOP-9AO4J1C</new>							- 0	×
Elle Edit Process View Connections Settings Extensions Help								
	Views: Design	Results	Turbo Prep	Auto Model	Deployments	Find data, op	eratorsetc 🔎 All Studi	io *
Auto Model								
Load Da	ta Select Task	Prepare Target	Select Inputs	Model Type	s Results		(i
•	•							
	Ҝ RES	TART 🕻 BAG	K) NEXT					
1 100 000							0	
1,100,000 - 1,000,000 -								
900,000 -								
800,000 - 700,000 -								
600,000 -								
500,000 - 400,000 -								
300,000 -								
200,000 - 100,000 -								
0 25 50 75 100 125 150 175 200 225 250	275 300 325 350	375 400 42	5 450 475	500				
Turn into Classification								
Number of Classes: 2								
Type of Class Building:								
Equal settings for all costs and benefits. Define Costs / Benefits								
							~	
Type here to search O	0 🗉 💼	I	🕹 🚾	9		📥 14°C Smoke	へ 🖻 📴 🧖 ^{10:36 PM} 12/4/2022	1

FIGURE 4.13: PREPARE TARGET

4.4.6 Select Inputs Fields:

Not all the data columns in your table will be useful for prediction. You could speed up and/or enhance the performance of your model by removing some of the data columns. However, how do you decide that? The fact that you're searching for patterns is important. The data is unlikely to be meaningful without some variance and some clearly visible patterns.

		Views: Desig	n Results T	urbo Prep Auto Model	Deployments	F	ind data, operatorsetc	🔎 All Stud
Model		Load Data Select Task	: Prepare Target Se	lect Inputs Model Ty	pes Results			
ected	Status ↑ Qu	Deselect Red ality Name	Selected: 6 / To Deselect Yellow Correlation		eselect All Stabillity	Missing	Text-ness	
	•	looped	5.13%	0.16%	92.88%	0.00%	0.00%	^
	• S	label	0.00%	0.00%	96.05%	0.00%	2.42%	
✓	e š M T	day	0.00%	0.03%	0.34%	0.00%	0.00%	
√		neighbors	45.69%	0.02%	54.81%	0.00%	0.00%	
✓		year	0.09%	0.00%	34.78%	0.00%	0.00%	
1		langth	0.31%	0.01%	27 F.R.%	0.00%	0.00%	~

FIGURE 4.14: SELECT INPUT FIELDS

4.4.7 Select the Model:

You can choose from several models that Auto Model suggests are pertinent to your issue. The ideal choice, if there is no time limit, is probably to build every one of them, then evaluate how they operate once they are all complete.

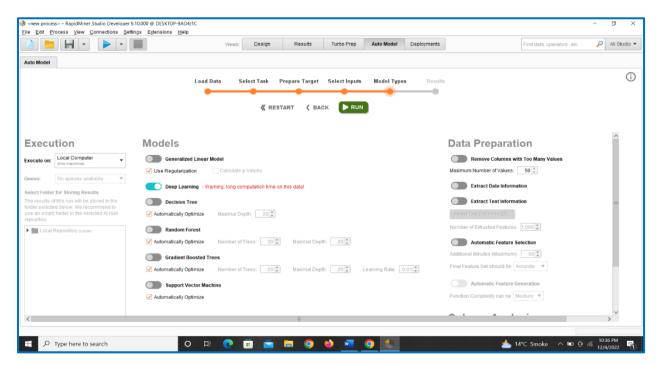


FIGURE 4.15: SELECT THE MODEL

4.5 Intrusion Detection System (IDS)

An intrusion detection system is a hardware or software program that keeps an eye out for malicious activities or policy breaches on a network or in a system. Any intrusion activity or violation is often recorded centrally using a security information and event management system, alerted to an administrator, or both.

4.5.1 SolarWinds

One pane of glass IT administration for on-premises, hybrid, and software as a service (SaaS) environment is made easier with the SolarWinds Orion Platform, a robust, scalable infrastructure monitoring and management platform.

The Orion Platform consolidates the entire set of monitoring capabilities into one platform with cross-stack integrated functionality, eliminating the need to deal with numerous incompatible point monitoring products.

NPM

With the help of the robust and reasonably priced SolarWinds Network Performance Monitor (NPM), you can easily identify, analyze, and fix network performance issues and outages.

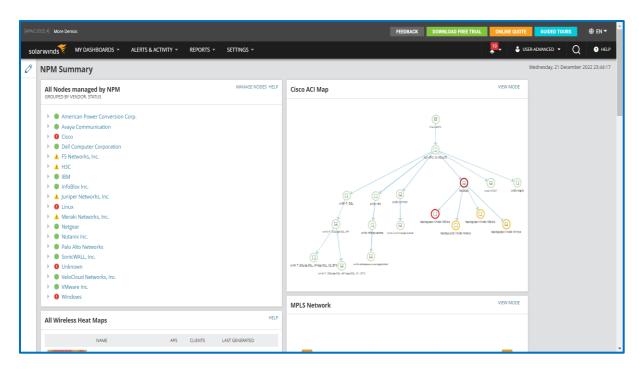


FIGURE 4.16: NPM SUMMARY

Wireless Network

Finding the devices on your wireless network is the first step in effective wireless network monitoring. As soon as the network discovery process is finished, wireless access points (APs) and controllers can be identified as wireless devices using SolarWinds Network Performance Monitor (NPM).

AC:2022.4] More Demos						EEDBACK DOWNLOAD FREE TR		IE QUOTE GUIDED TO	URS	⊕ EN ▼
olarwinds 🌾 🛛 M	IY DASHBOAI	RDS - ALERTS & ACTIVITY	✓ REPORTS ✓ SETTINGS ✓				19 •	🔒 USER-ADVANCED 👻	Q	? HELI
										0
Vireless Sum	mary Vi	ew sho	W: Access Points 🗸	SEARCH						
Monitor wireless										
A Aruba Networ	rks Inc 🏙 C	isco 📼 HPE 🔎 Meraki Netv	vorks, Inc. 😭 Meru Networks 🗼 Ruckus	Wireless Inc 🖉 Symbol Technologies, I	nc. and more!					
OUP BY: lo grouping]	~	Access Point	IP Address	Туре	SSIDs	Channels	Clients			
		Map-00000001	192.168.154.2	Thin	N/A		3			
		MAP-00000002	192.168.154.3	Thin	N/A		3			
		• 🌇 AP-00000003	192.168.154.4	Thin	N/A		3			
		March Mar	192.168.154.5	Thin	N/A		3			
		Map-00000005	192.168.154.6	Thin	N/A		3			
		March AP-00000006	192.168.154.7	Thin	N/A		3			
		AP-00000007	192.168.154.8	Thin	N/A		3			
		March AP-00000008	192.168.154.9	Thin	N/A		3			
		Map-00000009	192.168.154.10	Thin	N/A		3			
		 Mathematical AP-0000000A 	192.168.154.11	Thin	N/A		3			
		• 🐞 testWLC_AP-00fc	10.129.18.156	Thin	attwifi_Health	South, HS_Interr 6	4			
										_

FIGURE 4.17: WIRELESS NETWORK SUMMARY

Load Balancer

A load-balanced service is made up of numerous cooperating parts. You can browse each of these elements, their connections, and their current states in the Balancing Environment widget.

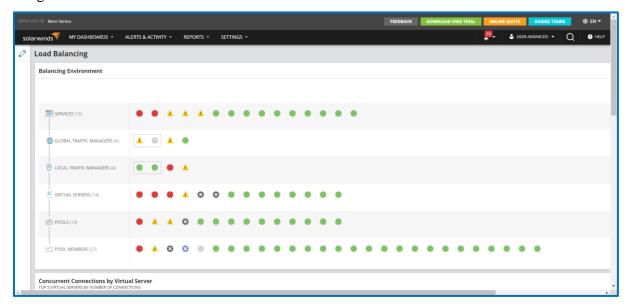


FIGURE 4.18: BALANCING ENVIRONMENT

NOC View

The Network Operations Center (NOC) view offers vital statistics for each device in your network that is being monitored. This view can be used to fill a mobile device or a wall-mounted monitor in a technical support facility used by network administrators and IT specialists who administer a network around-the-clock.

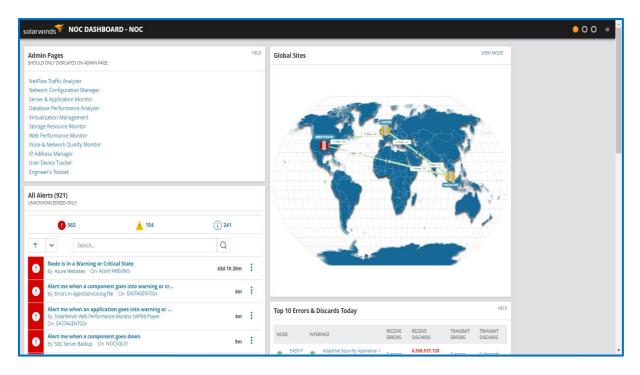


FIGURE 4.19: NOC DASHBOARD

Energy Wise

You can manage your energy costs with the help of Energy Wise. You can remotely set recurring policies and plan power usage with NCM, which can help you spend less energy. Additionally, SolarWinds NPM enables you to keep an eye on your power and energy usage.

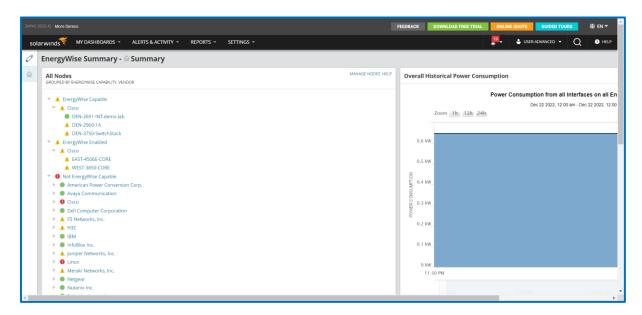


FIGURE 4.20: ENERGY WISE SUMMARY

Capacity Summary

The following metrics of monitored nodes, interfaces, and volumes are available for capacity forecasting:

- CPU uses across nodes
- Node memory usage
- Volumes' use of space
- Interface receive (in) utilization
- Interface transmit (out) utilization

	More Demos						FEEDBACK	WNLOAD FR		ONLINE QU			⊕ EN ▼
blarwir	nds MY DASH	BOARDS - ALERTS & ACTIVITY -	REPORTS	÷ SET	TINGS -					<u></u>	SUSER-ADVANCED -	Q	? HE
Сар	pacity Summa	ary											
То	op 5 CPU Capacity	Problems			HELP	HELP Top 5 Interface Capacity Problems					HELP SAN Capacity R		
N	IODE	DETAIL	WARNING	CRITICAL	AT CAPACITY	NODE	DETAIL		CRITICAL	AT	RESOURCE	TYPE	ARRAY
•	EASTWEB01v	EASTWEB01v - CPU Load	Now	Now	Now	NEWY-4331	The GigabitEthernet0/0/0.1061 · MPLS Circuit - Inter			CAPACITY	DMTST3_L	LUN	Atrem
•	EASTWEB02v	徽 EASTWEB02v - CPU Load	Now	Now	Now	-WAN	face Receive Utilization	Now	Now	3 days			
	AZRHWEB01v	徽 AZRHWEB01v - CPU Load	Now	1 day	3 days	EAST-RPi	R eth0 - Interface Receive Utilization	6 days	10 days	13 days	un2	LUN	Xtrem
	losadebkbms01	Iosadebkbms01 - CPU Load	Now	1 day	3 days	Nexus-1	Ethernet1/11 - Eth1/11 - Interface Receive Utili zation	6 days	10 days	13 days	P2TST3_LU N1	LUN	Xtrem
	EASTADDC01v	A EASTADDC01v - CPU Load	9 days	2 weeks	2 weeks	Nexus-2	T mgmt0 · management0 - Interface Transmit U tilization	8 days	11 days	2 weeks	P2TST3_LU	LUN	🗐 Xtrem
H						Nexus-2	The port-channel31 · Po31 - Interface Receive Utilization	8 days	12 days	2 weeks	StorageVol		Se vsp
То	op 5 Memory Capa	acity Problems			HELP						00:00:0d	LUN	94 VSP
N	IODE	DETAIL	WAR	RNING CRITIC	CAL AT CAPACITY	Top 5 Volume (Capacity Problems			HELP	Swi-hyv-12 r2	LUN	3PAR 00
	EASTWEB03v	EASTWEB03v - Percent Memory Usap	ge Nov	w Now	Now	NODE	DETAIL	WARNING	CRITICAL	AT CAPACITY	Se ThickLun	LUN	🚳 Nimb
	EASTCNTNR01v	EASTCNTNR01v - Percent Memory U	sage Nov	w Now	5 days	LAB-NOCEYAR 01	FV 🔯 C:\ Label: 504328B4 - Percent Disk Usage	Now	Now	8 days	In Thinvolum		UX BAR
Ľ	WESTCNTNR01v	SWESTCNTNR01v - Percent Memory	Nov	w 1 day	/ 7 days	O AZRHWEB01v	V 🔯 / - Percent Disk Usage	Now	7 days	2 weeks	e	LUN	00
		Usage				MUNICIPAL OF MUNIC	M	Nour	Now	Awooke	G_Backup_ Prod1	LUN	🕲 IBM X

FIGURE 4.21: CAPACITY SUMMARY

VSAN

A piece of software called Star Wind Virtual SAN (VSAN) merely "mirrors" internal hard disks and flash between hypervisor servers, negating the requirement for real shared storage.

PAC-2022.4) More Demos	FE	EEDBACK	DOWNLOAD FREE TRIAL	ONLINE QUOTE	GUIDED TOURS		EN 🔻
solarwinds 🐔 My Dashboards 👻 Alerts & Activity 👻 Reports 👻 Settings 👻				19 🕹 USE	R-ADVANCED 🔻	Q	7 HELP
VSAN Summary							
All VSAN Nodes	HELP	VSAN Tra	ffic				
▼ SAN0001 ▼ RERE-Tec-Mds9120 ● f ct/1 ● f ct/2 ● f ct/3 ● f ct/3 ● f ct/6 ● f ct/7 ● f ct/6 ● f ct/7 ● f ct/78 ● f ct/70 ● f ct/70 ● f ct/70 ● f ct/70 ● f ct/70		6 Mbp 5 Mbp 4 Mbp 04 3 Mbp 2 Mbp 1 Mbp 1 Mbp 1 1			VSA	N Traffic	J22, 12:
▼ ▲ FIBRE-Tex-Mds9120			21 Dec	6:00 A			

FIGURE 4.22: VSAN SUMMARY

NetPath

Slowdowns are simple to identify thanks to NetPath, which evaluates the performance characteristics of each network node and link. NetPath tracks the connectivity between your users and the services they use, identifies the infrastructure in the way, and pinpoints the locations of traffic snarls.

AC:2022.4] More Der	mos				FEEDBACK	DOWNLOAD FREE TRIAL	ONLIN		GUIDED TOUR	IS	⊕ EN ▼
solarwinds ኛ	MY DASHBOARDS 👻	ALERTS & ACTIVITY -	REPORTS 👻	SETTINGS -			10 .	🐣 USER-A	DWANCED 👻	Q	🕑 HEL
<mark>NetPath</mark> Se	ervices								(i) w	hat is N	etPath
+ CREATE NEW	SERVICE					Search					Q
	Azure Hybrid Cloud - WEB i minutes ago		2 paths					• II	+	0	ŵ
	failwind Trader 5 minutes ago		2 paths					• II	÷	O	ŵ
	Public-Facing Website 7 minutes ago		4 paths					inabled	+	0	俞
	Office 365 7 minutes ago		4 paths					inabled	(+)	0	俞
	ntranet 7 minutes ago		4 paths					inabled	(+)	0	俞
	Azure SQL Server 7 minutes ago		1 path					- II	÷	0	俞



Network Top 10

The Top 10 Interfaces by Percent Utilization, Top 10 Wireless Clients by Traffic, Top 10 Wireless APs by Clients Count, Top 10 Interfaces by Traffic, and Top 10 Interfaces by Traffic are all displayed by this service in SolarWinds. Top 10 Errors & Discards Today, Top 10 Nodes by Current Response Time Top 10 Nodes by Memory Usage, Top 10 Nodes by Average CPU Load, Top 10 Nodes by Percent Packet Loss, and Top 10 Volumes by Disk Space Usage. This window aids in our analysis of all metrics pertaining to network communication components.

	More Demos							FEEDBAC	K DOWNLOAD F	REE TRIAL	ONLINE QUOTE	GUIDED TOU	rs 💮 en
arwı	nds 🏹 MY	DASHBOARDS 👻	ALERTS & ACTIVITY -	REPORTS -	settings 🗕						🛄 🕹 USE	R-ADVANCED 👻	Q 🛛
Ne	twork To	o 10											
То	p 10 Interfa	ces by Percen	t Utilization				HELP	Тор	0 Wireless Clien	ts by Traffi	c		
N	ODE	INT	ERFACE	REC	EIVE	TRANSMIT			IP ADDRESS	SSID	CONNEC	TED	
	Nexus-2	•	port-channel31 · Po31		_	90.96	60 %		10.129.18.59	HS_Gues		22 12:37:43 AM	
	Nexus-1		port-channel99 · Po99		_				10.129.18.13	HS_Gues		22 12:37:43 AM 22 12:37:43 AM	
	Nexus-1	•	port-channel99 · Po99			68 %	76 %		10.129.18.179	HS_Gues		22 12:37:43 AM	
•	Nexus-2	•	port-channel70 · Po70			68 %	76 %	-	10.129.18.165	HS_Gues		22 12:37:43 AM	
	Nexus-1		Ethernet1/5 - Eth1/5					2	10.129.18.12	HS_Gues	t 12/22/20	22 12:37:43 AM	
1.1						58 %	72 %	120	10.129.18.242	HS_Gues	t 12/22/202	22 12:37:43 AM	
1	Nexus-1	•	Ethernet1/8 - Eth1/8			58 %	72.96		10.129.18.109	HS_Gues	t 12/22/20	22 12:37:43 AM	
	Nexus-1		port-channel32 · Po32			58 %	72 %		10.129.18.220	HS_Gues		22 12:37:43 AM	
						58.96	72 %	0 <u>×</u> 0	10.129.18.151	HS_Gues	t 12/22/20	22 12:37:43 AM	
1.1	Nexus-2	•	Ethernet1/7 - Eth1/7			58 %	72 %	Ton	0 Wireless APs b	v Clients C	ount		
	Nexus-2	•	port-channel42 · Po42			58 %	72.%	Top		, chenes e	ount		
17			-		_				AP NAME			IP ADD	
1	EAST-FW-A	•	GigabitEthernet0/3			58 %	66 %	20	testWLC_AF			10.129.1	
	Nexus-1	•	Ethernet1/11 - Eth1/11			90.96	30 %	20	testWLC_AP			10.129.1	
									testWLC_AP			10.129.1	
То	p 10 Interfa	ces by Traffic					HELP		testWLC_AP			10.129.1	
									testwic_AP			10.129.1	

FIGURE 4.24: NETWORK TOP 10 VIEW

Alerts

An alert is a computerized notification that a network event, such a server becoming offline, has occurred. The conditions you specify when configuring an alert define the network event that initiates an alert. You may establish alerts that notify various people depending on how long the alert has been activated and schedule alerts to monitor your network during a specified time period.

plarwinds MY DASHBOAI	rds -	ALERTS & ACTIVITY -	REPORTS -	SETTINGS *				<u>,</u>	🐣 USER-AD	DNANCED - Q	• В
ll Active Alerts								0 м.	anage Alerts	Show in NOC mode	 More
ROUP BY	38 A	CKNOWLEDGE BLVIEW ALI	RT DETAILS 🧷 EDI	ALERT DEFINITION 📋 CLEAR TRIGGER	D INSTANCE OF ALERT				En	nter search	
Alert name		🕅 Alert name			♥ Object that trig ♥ A		∀Ackno ∀Ackno	T Alert Limitation	🖓 Incident N	lumb 🍸 Assigne	d To (U
All (962)		Alert me when a comp	onentAlert me whe	n a component goes down	HTTP Bindings Mm	12/22/202	AcknowledsNot yet				
Nert me and trigger an NCM ac	B	Alert me when an app	icatio:Alert me whe	n an application goes down	Microsoft IIS on 1m	12/22/202	AcknowledgNot yet		525		
Alert me when a component go		Create Incident when	pplic:Create incide	nt when application goes down was tri	Microsoft IIS on 1m	12/22/202	Servic 4/11/2022		530	Helpdesk	
Vert me when a component go	=	A Response Time - Warr	ing - AResponse Tin	e - Warning - Anomaly-Based Alerting	DEN-7200-1B.den1m	12/22/202	AcknowledsNot yet				
lert me when a rogue DNS nar lert me when a rogue IP addre	ET.	A Alert me when a com	onentAlert me whe	n a component goes down	Diagnostics (Rer4m	12/22/202	AcknowledsNot vet				
lert me when a rogue MAC add	8	A CPU Threshold - Warn	ng - ACPU Thresho	d - Warning - Anomaly-Based Alerting	NEWY-EX2200-45t11m	12/22/202	AcknowledsNot vet				
Alert me when an application go	-			n an application goes down	SolarWinds Bac 14m		AcknowledsNot yet				
Alert me when an application g		A Alert me when a com			SQL Server Baci14m		AcknowledsNot yet				
Alert me when DHCP Scopes Ov		Alert me when a comp			File System Bacl14m		AcknowledsNot yet				
Vert me when server is not up i					The second second second						
Alert me when the free space of	-			n a component goes down	Exchange Backu20m		AcknowledsNot yet				
Alert me when virtual server is r Alert me when volume has less		A Alert me when a comp			File System Bacl20m		AcknowledgNot yet				
AP has more than 10 clients (1)		Alert me when an app	icatioiAlert me whe	n an application goes into warning or c	SolarWinds Wet38m	12/22/202	AcknowledgNot yet				
Application Connection status is	12	Alert me when a comp	onentAlert me whe	n a component goes into warning or cr	Errors in Agent\$38m	12/22/202	AcknowledgNot yet				
Attempt to use WinRM for appli		Alert me when a comp	onentAlert me whe	n a component goes down	Package Summ:45m	12/22/202	Acknowled(Not yet				
Azure cloud account polling faile	Ð	Alert me when an app	icatio:Alert me whe	n an application goes down	SolarWinds Patc45m	12/22/202	AcknowledgNot yet				
Azure Cloud VM is in a Warning	Ð	A Node is in a Warning o	r CritiiNode NOCEA	DDC01v is Warning.	A NOCEADDC01v 1h 1	1m 12/21/202	AcknowledsNot yet				
Cluster memory utilization (1)	100	A Mada Isla a Maralas	- Cole Alada CACTIA	1903 u la Califical	· -		A classical which to be used				

FIGURE 4.25: ALL ACTIVE ALERTS

Events

Any change in the state of a monitored object or an action taken in response to a state change is referred to as an event. To better understand the kinds of events you can anticipate, look over the list below. The range of potential outcomes is not covered by this list.

TABLE 4.1: EVENTS

Node events	Down, Up, Warning, Deleted, Added, Unmanaged, Manage,
	Rebooted, and Changed.
Interface events	Down, Up, Shutdown, Enabled, Unknown, Added, Deleted,
	Remapped, and Changed.
Volume events	Remapped, Changed, Added, Deleted, Disappeared, and
	Reappeared.
Monitoring	Started and stopped.
Failover	Failover and Failback.
Alert	Triggered and reset.

[APAC:2022.4] More	Demos	FEEDBACK DOWNLOAD F		⊕ EN ▼
solarwinds	MY DASHBOARDS + ALERTS & ACTIVITY + REPORTS + SETTINGS +		 🕹 USER-ADVANCED 👻 🔿	(B HELP
Events			🖨 Printable V	/ersion 🕐 Help
Events From All	Network Devices - Today			HIDE
FILTER DEVICES:	Network Object Type of Device All Network Objects V OR All Device Types V			
	Event Type All events			
FILTER EVENTS:	Time Period: Today V			
	Number of displayed events: 100 Ghow Cleared Events			
	REFRESH			
TIME OF EVENT	MESSAGE			
	2 12:32 AM Ath DEN-ACSRV01v to DEN-7200-DMZv2 changed its status to Critical			
	2 12:22 AM Path DEN-ACSRV01v to DEN-7200-DMZv2 changed its status to Warning			
12/22/202	2 12:12 AM Path DEN-ACSRV01v to DEN-7200-DMZv2 changed its status to Critical			
SELECT ALL	ESELECT ALL CLEAR SELECTED EVENTS			
	solar winds 🗲 _{Solar} Winds Flastern, Hybris Cloud Observability Advanced Enterprise Scale, WFM, SMM: 2022 A.D & 1999-2022 :	SolarWinds Worldwide, LLC. All Rights Reserved.		

FIGURE 4.26: EVENTS FROM ALL NETWORKS

Syslogs

System Logging Protocol enables the transmission of data in a specific message format from network devices to a central server, also known as a syslog server. By making log message handling simpler, this logging protocol is an essential component of network monitoring since it enables you to monitor the general health of network devices.

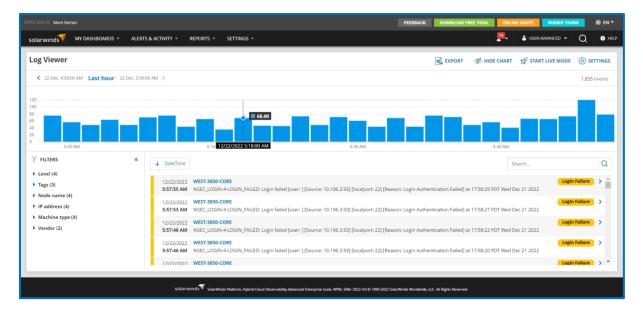


FIGURE 4.27: LOG VIEWER

SNMP Trap

An SNMP trap is sent to the designated SNMP manager by the SNMP Trap alert. Its purpose is to deliver the alert text to an SNMP manager for analysis using string pattern matching criteria, after which your current network management software reports and keeps track of it.

Any SNMP monitoring program receives an SNMP trap when you receive an SNMP trap alert. In addition to enterprise-specific and generic trap kinds like Cold Start, Warm Start, Link Down, and others, the alert supports Ip Monitor alert tokens.

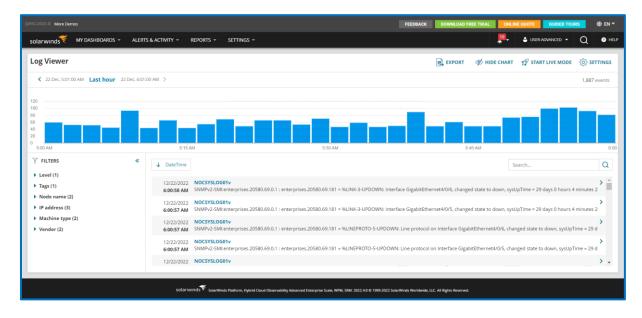


FIGURE 4.28: TRAPS

Message Center

You can view all network events, alerts, traps, and Syslog messages in the Message Center's view.

[APAC:2022.4] More 0	emos					FEEDB	ACK DOWNLOAD FREE TRIAL	ONLINE QU		s 💮 EN 🔻	
solarwinds	MY DASHBOARDS 👻	ALERTS & ACTIVITY	• REPORTS •	Settings -				19. •	user-advanced 👻	Q I HELP	
Message Ce	nter								🖨 Printal	ole Version 🕐 Help	
Events, Alerts an	d Audit Events From All N	letwork Devices - Tod	ay							HIDE	
FILTER DEVICES:	Network object All Network Objects	~	Type of device OR All Device Type		fendors All Vendors	V OR		Hostna OR	ime		
	Time period: Today	name: All Alerts	Number of displaye	d messages: 100	Show acknowled	lged					
HLTER MESSAGES:	TRA MESSAGES C Show vent messages RUTR RUMN'S Event type: All events C Show Judic Vennts RUTR RUDN'S Action type: All action types User:										
	APPLY							5	Search	SEARCH	
DATE TIM	E ·	MESSAGE TYPE	MESSAGE				Hostname		IP ADDR	ESS	
12/22/202	2 1:09:10 AM	Advanced alert	🔥 Alert me when	a component goes down			SQL Server Bac	kup	10.1.100.1	11	
12/22/202	2 1:09:10 AM	Advanced alert	🗼 Alert me when	a component goes down			File System Bac	kup	10.1.100.1	11	
12/22/202	2 1:09:09 AM	Advanced alert	Alert me when	an application goes down			SolarWinds Bac	kup (Windows)	10.1.100.1	11	
12/22/202	2 1:07:17 AM	Advanced alert	🛕 Alert me when	a component goes down			Exchange Back.	qu	10.129.40	.61	
12/22/202	2 1:07:17 AM	Advanced alert	Alert me when	a component goes down			File System Bac	kup	10.129.40	.61	
12/22/202	2 12:58:34 AM	Advanced alert	A Response Tim	e - Warning - Anomaly-Based Alerting	was triggered.		DEN-7200-DMZ	v2.demo.lab	172.16.90	.2	
12/22/202	2 12:42:51 AM	Event	A Path DEN-ACS	RV01v to DEN-7200-DMZv2 changed it	s status to Warning						
12/22/202	2 12:41:03 AM	Event	Path NOCSWO	APE01VS to Azure Hybrid Cloud - WEB	changed its status to Good						

FIGURE 4.29: MESSAGE CENTER

Anomaly-Based Alerts

To enhance regular alerts, anomaly-based alerts combine Hybrid Cloud Observability (HCO) Alerting with anomaly detection as composed alerts. In order to increase the accuracy of warnings, HCO Anomaly Detection uses machine learning to identify outliers. The alert is only triggered when both the metric condition and the anomaly are present.

omaly-Based Alerts					() A	dd New Aler	t 🕐 What is ar	Anomaly-Ba	sed Aler
LTERS	≪ ↑ Name ✓						Search		Q
• Object Type	🛕 CPU Threshold - Critical								:
Severity	🛕 CPU Threshold - Warning								:
Critical	A Packet Loss - Critical								
🗌 🛕 Warning	A Response Time - Critical								:
	🛕 Response Time - Warning	00:15	02:15		04:15			06:1	1

FIGURE 4.30: ANOMALY BASED ALERTS

Reports

For each SolarWinds Platform product, SolarWinds offers preconfigured reports. You can edit these predefined reports and make your own reports using the web-based interface.

By selecting Reports > All Reports from the menu bar, you can view a collection of predefined reports.

APA(1:2022.4) More Demos							FEEDBACK	DOWNLOAD FREE TRIAL		IE QUOTE	GUIDED TOU		⊕ EN ▼
solarwinds MY DASHBOAI	RDS -	- 3	ALERTS & ACTIVITY 👻	REPORTS -	SETTINGS -				*	🐣 USER	ADVANCED 👻	Q	HEL
All Reports													irts 🕐 Hel
										1	hursday, Decemb	per 22, 2023	
GROUP BY: Report Category	B		REPORT								Search		
		☆	Report Title =			Description	Categ	ory			Module Ti	tle	
All (523)	0	☆	All Down Nodes			Displays all Nodes that are currently Down	Curre	nt Node Status					
Active Directory Reports (2)	0	☆	Average Response Time			Displays the Average and Peak Response time for all N	lodes Curre	nt Node Status					
Agent Management (2)	0	$\dot{\Omega}$	Copy of All Down Nodes	R.		Displays all Nodes that are currently Down	Curre	nt Node Status					
APM: Current Application and C	0	☆	Current CPU Load			Displays the Current CPU Load for each Node	Curre	nt Node Status					
APM: Daily Application Availabil	0	슈	Current Response Time			Display the Current, Average, and Peak Response Time	e for Curre	nt Node Status					
APM: Exchange Reports (4)	0		Current Status of each M	Node		Displays the Current Status of each Node	Curre	nt Node Status					
APM: Historical Application CPU	0	☆	Device Polling Details			Displays the Next Rediscovery and Next Poll time of ea	ach Curre	nt Node Status					
APM: Historical Reports (3)	0	\$	Last Boot Time for each	Node		Displays the time of the Last Reboot for each Node	Curre	nt Node Status					
APM: IIS Reports (4)													
APM: SQL Reports (6)													
APM: Windows Scheduled Tasks													
ASA Reports (2)													
Asset Inventory (6)													
Audit Events (11)													
Availability (5)													
Capacity Forecast (1)													
Current Interface Status (4)													
Current Node Status (8)													
Current Volume Status (1)													
Custom (24)	۲			(A)	OF ITEMS PER PAGE:								
• · · · · · · · · · · · · · · · · · · ·			Page 1 of 1 0 0	NUMBER	OF ITEMS PER PAGE:	100					Dis	splaying ite	rms 1 - 8 0

FIGURE 4.31: ALL REPORT

Network Sonar Discovery

The list of all the findings you've set up for your network is available in the Network Sonar view.

Consult the Status column on the Network Sonar Discovery tab to learn whether a discovery was successful.

- Completed: The finding was effective in its goal and did not need to be repeated.
- Scheduled: At least one more run of the finding will occur.

larwinds 🐔 MY DASHBOARDS 👻 ALERTS & ACTIVITY	 REPORTS - SETTINGS - 				÷ *	USER-ADVANCED 👻	Q	Э н
								🥐 н
twork Sonar Discovery								
scover Network Scheduled Discovery Results Discove	ry Ignore List							
🕀 Add New Discovery 🛛 🔞 Discover Now 🖉 Edit 🛛 🗎 Im	nport All Results 🔡 🖹 Import New Resu	its 🝵 Delete						
Name Description		Frequency	Status	Last Run				
admin: 10/24/2022, 12:20 PM		Manual	Finished					
) admin: 10/24/2022, 12:24 PM		Every day at 12:00 AM	Scheduled	Tuesday, December 20, 2022 5:00 AM				
) admin: 10/24/2022, 01:08 PM		Every day at 12:00 AM	Scheduled	Wednesday, December 21, 2022 5:47 AM				

FIGURE 4.32: NETWORK SONAR DISCOVERY

Manage Nodes

In the SolarWinds Platform Web Console, the Manage Nodes view is the main view for managing devices. The terms "entities" can also be used to describe nodes and interfaces.

- Use the management actions offered in the toolbar after selecting the node or interface to manage.
- Select the devices to handle many devices at once.
- Select the box to the left of the Name column to access all monitored devices' management options.

AC:2022.4] More Demos					FEEDBACK	DOWNLOAD FREE TRIAL	ONLINE Q		JRS	⊕ EN ▼
olarwinds 🐔 MY DASHBOARDS 👻	ALE	ERTS & ACTIVITY - REPORTS -	SETTINGS -				<u>19</u> .	USER-ADVANCED 👻	Q	HELP
Admin Mode Management Manage N	lodes									
1anage Nodes	Show:	Nodes ¥		SEARCH						
Sroup by: Vendor	() AE	D NODE 🖉 CUSTOM PROPERTY ED	ITOR 🖉 EDIT PROPER	RTIES 🗎 LIS	ST RESOURCES 📓 ASSIGN POLLERS 🔗 MAINTENANCE MODE 🕤	MORE ACTIONS 💿 🍵 🛙	DELETE			
American Power Conversion Corp. (1)		Name 🔺	Polling IP Address	IP Version	Status			Contact		
Avaya Communication (1)	. ►	AUS-SUB-01	1.11.3.6	IPv4	Node status is Warning, MS TCP Loopback interface is Down.			atrick Hubbard		
tite Cisco (58)		Cisco APIC	10.199.4.70	IPv4	Node status is Up.					
Dell Computer Corporation (1)	\vdash	DEN-2691-INT.demo.lab	10.91.0.6	IPv4	Node status is Up.			enver-IT		
F5 Networks, Inc. (7)	\vdash	A DEN-2960-1A	10.1.150.109	IPv4	Node status is Warning, One or more interfaces are Down.			letwork Support - De	nver	
ec H3C (1)	. ► □	DEN-3560-ASFIr1A.demo.lab	10.95.5.2	IPv4	Node status is Up.		1	Penter-IT		
IBM (1)	. ► □	DEN-3560-ASFIr1b.demo.lab	10.96.5.2	IPv4	Node status is Up.			enter-IT		
FinfoBlox Inc. (1)	$\models \Box$	DEN-3560-ASFIr2a.demo.lab	10.97.5.2	IPv4	Node status is Up.			enter-IT		
Juniper Networks, Inc. (4)		DEN-3560-ASFir2b.demo.lab	10.98.5.2	IPv4	Node status is Up.			enter-IT		
Linux (21)	+□	DEN-3560-ASFIr3a.demo.lab	10.99.5.2	IPv4	Node status is Up.			Penter-IT		
Meraki Networks, Inc. (4) Netgear (1)		DEN-3560-ASFIr3b.demo.lab	10.100.5.2	IPv4	Node status is Up.			enter-IT		
Nutanix Inc. (3)	. ►	DEN-3560-ASFIr4a.demo.lab	10.101.5.2	IPv4	Node status is Up.			enter-IT		
Palo Alto Networks (2)	▶ □	DEN-3560-ASFIr4b.demo.lab	10.102.5.2	IPv4	Node status is Up.			enter-IT		
SonicWALL, Inc. (2)	. ►	DEN-3560-CORE_A.demo.lab	10.92.0.2	IPv4	Node status is Up.			enter-IT		
Unknown (13)	. □	DEN-3560-CORE_B.demo.lab	10.93.0.2	IPv4	Node status is Up.			enter-IT		
VeloCloud Networks, Inc. (1)	. ►	DEN-3560-Fir1.demo.lab	10.94.0.2	IPv4	Node status is Up.			Penter-IT		
WMware Inc. (15)	. ►	DEN-3560-Fir2.demo.lab	10.94.0.10	IPv4	Node status is Up.			enter-IT		
Windows (80)	▶ □	DEN-3560-Fir3.demo.lab	10.94.0.18	IPv4	Node status is Up.			enter-IT		
	* □	DEN-3560-Fir4 demo lab	10 94 0 26	IPv4	Node status is Un			enter-IT		

FIGURE 4.33: MANAGE NODES

Manage Dashboards

You can use a new, data-driven dashboard framework as in Orion Platform 2020.2.

These dashboards enhance the functionality of websites. They allow you to resize and arrange widgets in any desired position. These dashboards automatically update their data, so there is no need to force your browser to reload the page.

To customize contemporary dashboards, you require Administrator Rights or Manage Dashboard Rights.

(APAC:2022.4) More Demos					FEEDBACK	DOWNLOAD FREE TRIAL	ONLINE QUOTE	GUIDED TOURS	⊕ EN ▼
solarwinds MY DASHBO/	ARDS 🝷	ALER	RTS & ACTIVITY * REPORTS * SETTINGS *			<u>19</u>	✓ Suser-AC	WANCED - Q	HELI
Manage Dashboards									
FILTERS	«	(A	dd modern dashboard 🕘 Add classic dashboard						
• Owner			✓ ↑ Name ✓				Search.		Q
System (read-only)	5 2		Config Summary Summary	System dashboard		Public			
Version Modern	7		Executive Summary Summary	by admin updated 127 day(s) ago		Public			
Visibility Public	7		Microsoft 365 API Poller dashboard Summary	by admin updated 127 day(s) ago		Public			
Public	,		Overall Compliance Summary Summary	System dashboard		Public			
			Policy Assignment Detail Summary	System dashboard		Public			
			Policy Compliance Summary	System dashboard		Public			
			Policy Compliance Summary Summary	System dashboard		Public			
		<	1 >					1-7 of 7	10 🗸
			solar winds 😴 Solar Winds Platform, Hybrid Cloud O	bservability Advanced Enterprise Scale, WPM, SRM: 2022.4.0 © 1999-20	022 SolarWinds Worldwide, LLC.	All Rights Reserved.	_		

FIGURE 4.34: MANAGE DASHBOARDS

Chapter 5

RESULTS AND DISCUSSIONS

5.1 Result:

Models	Accuracy
Deep learning	95.4%
Gradient-boosted trees (GBM)	76.5%
Random Forest	54.7%

TABLE 5.1: RESULT

5.2 Deep learning:

A larger family of machine learning techniques built on artificial neural networks and representation learning includes deep learning. Unsupervised, semi-supervised, and supervised learning are all possible.

duction Mode	Input Data Other R	esults Process										
3	Deep Learni	ng Mode	ı –									
escription		0										
raciipaon	Model Metrics Type											
	Description: Metr				frame with	9963 samples						
	model id: rm-h2o-											
	frame id: rm-h2o-	frame-product	ion_mode	1-21815.tempo	rary.sample.	1.00%						
-	MSE: 3.701299											
notations	RMSE: 1.923876											
	R^2: 0.53389895 mean residual dev		~~									
	mean residual dev mean absolute err											
	root mean squared											
				abt rearest	on gaugeise	distribution	Quadratic	1088 2 851	vaighte/hisese so a	VB 2 500 000	training samples, m	ini-hatch ein-
		ayers (predic Ivpe Dropout	L1 L1						weights/blases, 38.2 ean Bias Bias RMS	nu, 2,500,000	visiting samples, m.	ini-Daton size
		nput 0.00 %	11	L2 riea	n Race Race I	And Homencum H	ean weight	weight KHS H	ean blas blas Mh5			
	2 50 Recti		0.000010	0.000000 0.	002255 0 000	24 0 000000	0.065751	0 170440	0.193857 0.212680			
	3 50 Recti					170 0.0000000			0.813671 0.198645			
	4 1 Li					109 0.0000000			0.046995 0.000000			
	Scoring History:	and the	0.000010	0.000000 0.	000000000000000000000000000000000000000	0.000000	0.001017	01221001	0101000000			
	Timesta	T T	uration	Training Spee	d Enochs T	erations	Samples	Training RMS	E Training Deviance	Training MAE T	raining r2	
	2022-11-06 01:08:		000 sec		0.00000	0	0.000000	Nal		NaN	NaN	
	2022-11-06 01:08:			20537 obs/se		1 250	000.000000	2.0755		0.47037	0.45752	
	2022-11-06 01:09:	23.	886 sec	21129 obs/se	c 2.00000	2 500	000.000000	1,9780	0 3.91248	0.39304	0.50731	
	2022-11-06 01:09:	11 34.	810 sec	21720 obs/se	c 3.00000	3 750	000.000000	1.9257	6 3.70854	0.45489	0.53299	
	2022-11-06 01:09:	21 45.	258 sec	22261 obs/se	c 4.00000	4 1000	000.000000	1.9238	8 3.70130	0.38952	0.53390	
	2022-11-06 01:09:	31 55.	175 sec	22819 obs/se	c 5.00000	5 1250	000.000000	2.0444	6 4.17980	0.38228	0.47364	
			444 sec	23441 obs/se	c 6.00000	6 1500	000.000000	1.9431	0 3.77564	0.44126	0.52454	
	2022-11-06 01:09:	41 1 min 4.		24100 obs/se	c 7.00000	7 1750	000.000000	2.0793	6 4.32372	0.43202	0.45552	
			129 sec				000.000000	2.0981	4 4.40219	0.38104	0.44564	
	2022-11-06 01:09:	49 1 min 13.			c 8.00000	8 2000	000.000000			0.37845	0.52921	
	2022-11-06 01:09: 2022-11-06 01:09:	49 1 min 13. 58 1 min 21.	384 sec	24750 obs/se			000.000000	1.9335	3 3.73856	0.3/045	0.52321	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09:	<pre>49 1 min 13. 58 1 min 21. 06 1 min 29.</pre>	384 sec 440 sec	24750 obs/se 25336 obs/se	c 9.00000	9 2250		1.9335		0.41390	0.52782	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09:	<pre>49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37.</pre>	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000		7 3.74954			
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:10: 2022-11-06 01:10: 2022-11-06 01:10:	49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37. 13 1 min 37.	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000	1.9363	7 3.74954	0.41390	0.52782	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:10: 2022-11-06 01:10:	49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37. 13 1 min 37.	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000	1.9363	7 3.74954	0.41390	0.52782	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:10: 2022-11-06 01:10: 2022-11-06 01:10:	49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37. 13 1 min 37.	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000	1.9363	7 3.74954	0.41390	0.52782	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:10: 2022-11-06 01:10: 2022-11-06 01:10:	49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37. 13 1 min 37.	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000	1.9363	7 3.74954	0.41390	0.52782	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:10: 2022-11-06 01:10: 2022-11-06 01:10:	49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37. 13 1 min 37.	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000	1.9363	7 3.74954	0.41390	0.52782	
	2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:09: 2022-11-06 01:10: 2022-11-06 01:10: 2022-11-06 01:10:	49 1 min 13. 58 1 min 21. 06 1 min 29. 13 1 min 37. 13 1 min 37.	384 sec 440 sec 042 sec	24750 obs/se 25336 obs/se 25947 obs/se	c 9.00000 c 10.00000	9 2250 10 2500	000.000000	1.9363	7 3.74954	0.41390	0.52782	

FIGURE 5.1: DEEP LEARNING MODEL

Select Simulator (DL) to gain further understanding. On the left are sliders and dropdown menus, while on the right are bar charts in this user interface. The Model Simulator selects average data values for its initial state.

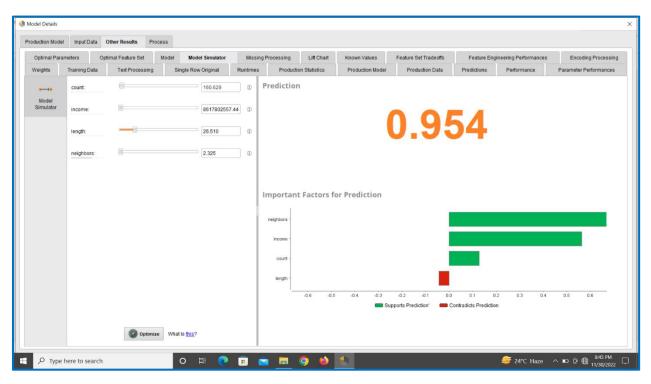


FIGURE 5.2: SELECT SIMULATOR DL

Optimal Para	meters Op	timal Feature Set	Model Model S	Simulator	Missing Proces	sing Lift Chart	Known Values	Feature Set Tradeoffs	Feature Eng	ineering Performances	Encoding Processing
Weights	Training Data	Text Processing	Single Row Or	iginal	Runtimes	Production Statistics	Production Model	Production Data	Predictions	Performance	Parameter Performances
	Row No.	weight	prediction(weight)	length	count	neighbors	income				
Explanations	1	0.073	0.413	144	456	1	20000000				
Explanations	2	0.103	0.094	144	4910	2	40000000				
	3	0.408	0.250	144	3060	2	120000000				
	4	1	0.516	2	1	1	33534612				
	5	0.026	0.087	42	7	1	50000000				
	6	1	0.688	2	1	2	55000000				
	7	0.005	0.272	144	1443	2	68830000				
	8	0.333	0.687	2	1	2	124000000				
	9	1	0.710	0	1	1	50000000				
	10	2	1.390	2	3	6	400000000				
	11	0.500	0.882	0	1	2	120000000				
	12	0.250	0.517	2	1	1	318000000				
	13	0.236	0.298	144	904	2	64111014				
	14	0.250	0.882	0	1	2	71000000				
	15	4.293	1.158	144	2043	7	2775228496				
	16	0.587	0.625	144	1605	4	874000000				
	17	1	0.711	0	1	1	60000000				
	18	0.835	0.689	144	829	4	937123869				
	19	0.788	1.172	144	1380	7	2038247863				
	20	0.778	0.335	16	9	2	1174500000				

FIGURE 5.3: MODEL DETAILS

Optimal Paran		Other Results F	Process	Model Simulator	Missing Process	ing Lift Chart	Known Values	Feature Set Tradeoffs	Feature Feat	ineering Performances	Encoding Processing
						-				-	
Weights	Training Data	Text Processin	g s	ingle Row Original	Runtimes P	roduction Statistics	Production Model	Production Data	Predictions	Performance	Parameter Performances
Data	attribute	weight									
	length	1									
	count	1									
Weight	neighbors	1									
isualizations	income	1									

FIGURE 5.4: WEIGHT DATA

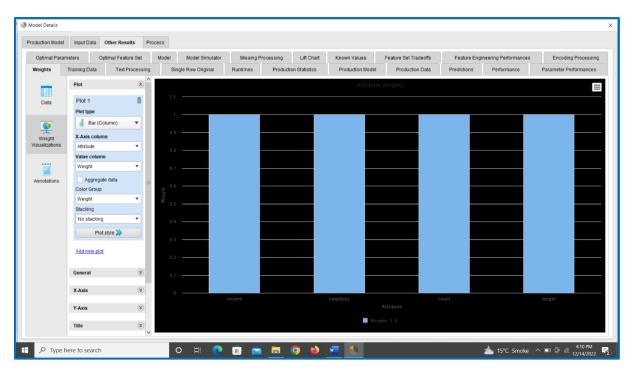


FIGURE 5.5: BAR CHART

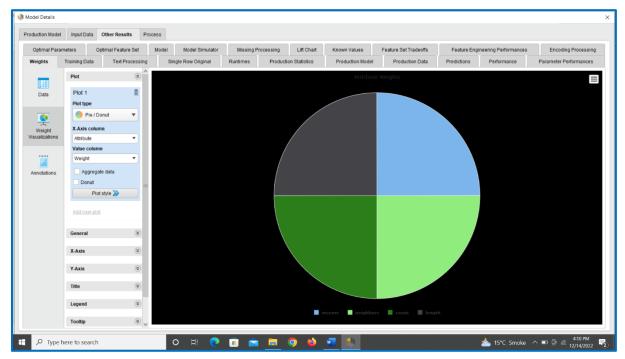


FIGURE 5.6: PIE CHART

Root Mean Squared Error class. the inaccuracy of the root-mean-square. The most widely used metric for evaluating the accuracy of numerical predictions is root mean-squared error and mean-squared error, error is the same size as predicted values themselves.

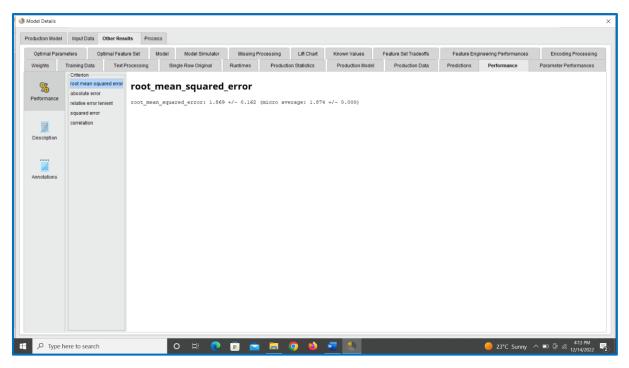


FIGURE 5.7: ROOT MEAN SQUARE ERROR

The absolute error is determined by summing the differences between all the label attribute's predicted values and actual values, Afterwards, divide the outcome by the total number of forecasts. To calculate prediction average, the actual label values are added together, and the total is divided by the overall number of instances.

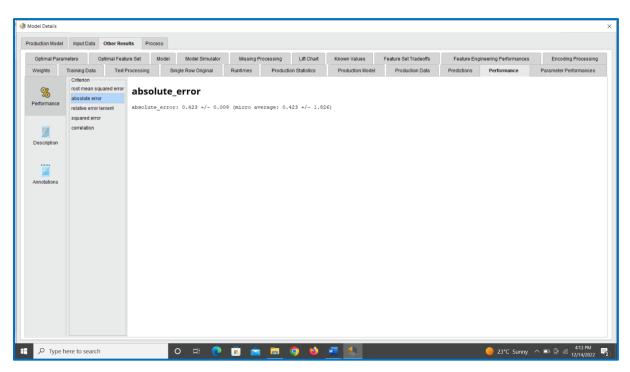


FIGURE 5.8: ABSOLUTE ERROR

The average lenient relative error is calculated by dividing the maximum of the actual value and the prediction by the average absolute deviation of the forecast from the actual value. The values of the label property correspond to the actual values.

💷 Model Details										×
Production Model	Input Data Other Res	ults Process								
Optimal Paran	neters Optimal Feat	ure Set Model	Model Simulator	Missing Processing	Lift Chart	Known Values	Feature Set Tradeoffs	Feature Eng	ineering Performances	Encoding Processing
Weights		Processing Si	ngle Row Original	Runtimes Product	tion Statistics	Production Model	Production Data	Predictions	Performance	Parameter Performances
%	Criterion root mean squared error absolute error	relative_e	error_lenier	nt						
Performance	relative error lenient	relative_error	_lenient: 61.07%	+/- 0.12% (micro av	erage: 61.074	* +/- 31.81%)				
Description	squared error correlation									
Annotations										
🛨 🔎 Туре h	ere to search		o == 💽	🖻 💼 🛤	•	🚾 🍂			23°C Suppy	∧ ■ @ <i>@</i> 4:13 PM 12/14/2022 ₹ 2
ye iypen									- Lo C Sunny	12/14/2022 (2)

FIGURE 5.9: RELATIVE ERROR

How closely a regression line resembles a set of data points is determined by the Squared Error. It is a risk function that corresponds to the squared error loss's expected value.

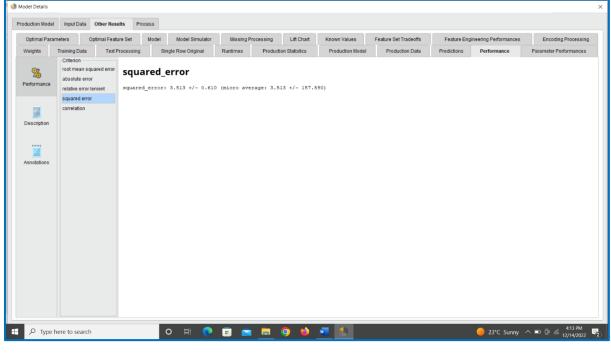


FIGURE 5.10: SQUARED ERROR

A correlation is a number that ranges from -1 to +1 and expresses how closely two attributes are related. A favorable connection is implied by a positive correlation value.

Optimal Para	meters	Optimal Featu	re Set	Model	Model Simulator	Missing F	Processing	Lift Chart	Known Values	Feature Set Tradeoffs	Feature Eng	ineering Performances	Encoding Processing
Veights	Training Data	Text P	rocessing	Sir	ngle Row Original	Runtimes	Producti	on Statistics	Production Model	Production Data	Predictions	Performance	Parameter Performances
% renformance	Criterion root mean so absolute error relative error squared error	or Ienient	COTTE)n .836 +/- 0.040	(micro avera	age: 0.837)						
Description	correlation												
Annotations													

FIGURE 5.11: CORRELATION

This shows the missing values percentage with infinite, stability, and valid values. Show statistics name and value of minimum, maximum, average and standard deviation.

													×
Production Model	Input Data	Other Results Pr	ocess										
Optimal Paran		Optimal Feature Set	Model	Model Simulator	Missing P	-	Lift Chart	Known Values	Feature Set Tradeoffs		ineering Performances	Encoding Processing	,
Weights	Training Data	0% % 18% 3%	Distrib	ution	Runtimes		n Statistics	2,000,000,000,000	2.500.000.000.000	Predictions	Performance	Parameter Performances	
	Statisti	cs											
	Name							Value					
	Minimum							3000000					
	Maximum							4970000000000	0				
	Average							8913701637.691					
	Standard [Deviation						245373662744.3	345				
🗄 🔎 Type I	here to searc	h		o H 💽	💼 💼		🧿 单	🚾 🧿 🧕		1	b 12℃ Smoke 🗥	1:58 AM	2

FIGURE 5.12: INCOME SUMMARY

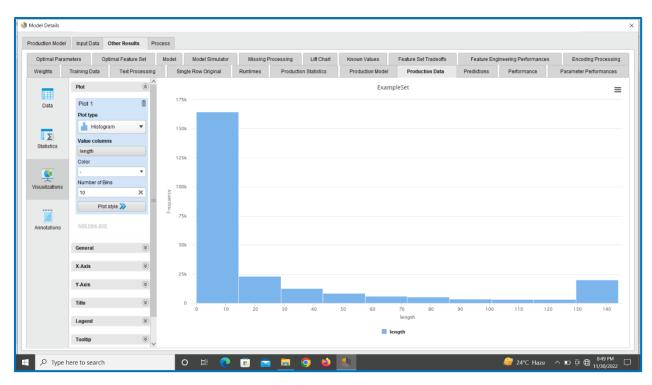


FIGURE 5.13: HISTOGRAM CHART

5.3 Gradient-boosted trees (GBM):

Gradient-boosted decision trees are a popular method for resolving prediction challenges in both the classification and regression domains. By simplifying the aim and needing fewer iterations to reach an appropriately optimum solution, the technique enhances the learning process [16].

Optimal Par	ameters	Optimal Feature Set	Model Model Simulator	Missing	Processing	Lift Chart	Known	Values	Feature Set Tradeoffs	Feature Eng	ineering Performances	Encoding	Processin
/eights	Training Data	Text Processing	Single Row Original	Runtimes	Producti	on Statistics	Produ	iction Model	Production Data	Predictions	Performance	Parameter Pe	formances
••	count	0	158.217	D D F	rediction	1							
Model imulator	income:	-	8941400681	.82 ①					0 70				
	length:		26.210	O					0.76	50			
	neighbors:	0	2.362	D									
				1	mportant	Factors f	for Predi	ction					
					neighbors								
					income -								
					count -								
					length -				1				
					-0.8	-0.7 -0.	6 -0.5	-0.4 -0		0.1 0.2	0.3 0.4 0.5	0.6 0.7	0.8
								Su Su	upports Prediction' 🧰 Co	ontradicts Predictio	n		
		Optimize	e What is this?										

FIGURE 5.14: GRADIENT-BOOSTED TREES

A step line chart is a type of line graph in which points are linked by both horizontal and vertical line segments that resemble the steps of a staircase. When it's required to draw attention to the irregularity of changes, step line charts are utilized.

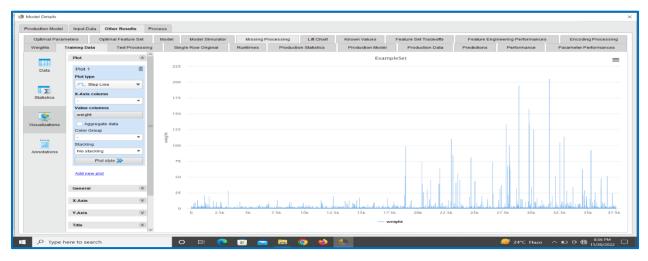


FIGURE 5.15: STEP LINE GRAPH

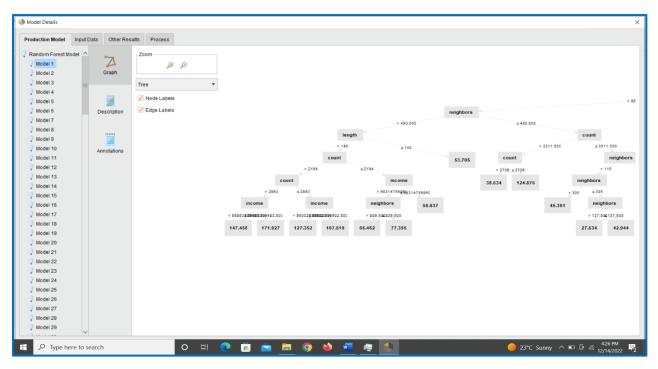


FIGURE 5.16: TREE DIAGRAM 1

🌒 Model Details															×
Production Model In	nput Data Other Res	sults Process													
Random Forest Model		Zoom													
V Model 1	A	,o ,o													
V Model 2	Graph														
V Model 3	=	Tree •													
V Model 4		Node Labels								neighbors					
Wodel 5		Edge Labels		> 9	5.500									≰ 95.500	
Model 7	Description	Luge Lubero													
Model 8															
Model 9															>1
Model 10			count										neighbors		
Model 11	Annotations		≤ 351	1.500							> 30.500			≤ 30.500	
Model 12				neighbors					income						neig
Model 13			>	115	≤ 115			> 24250000000	0 ≤2425000	00000				> 4.	500
Model 14			neighbors		neial	bors				ngth			inc	ome	
V Model 15			_				32.843			-					
V Model 16			305 ≤ 305		> 110.5	110,500			> 141	\$ 141				≤ 12845100000	
V Model 17			neigh	nbors	110.015	54.847		co	unt	neigh	hbors	len	gth	neigh	bors
V Model 18			> 137.50	£137.500				> 3372.5	02372.500	> 37	≤ 37	> 115	≤ 115	> 8.500	≤ 8.500
V Model 19			27.534	42.944				16.113	7.482	19.008	12.496	8.384	3.849	2.029	1.093
V Model 20															
V Model 21															
Model 22															
V Model 23															
V Model 24															
Model 25															
V Model 26															
Model 27															
Model 28															
V Model 29	\sim														
🛨 🔎 Type here	to search	o H	2 💼			😆 🐖	49					🛑 23°C Su	nnv 🔨 🗖		6 PM 4/2022 2
· · · · · · · · · · · · · · · · · · ·				_				~						12/1	4/2022 2

FIGURE 5.17: TREE DIAGRAM 2

🌒 Mo	del Details															×
Prod	luction Model Input	t Data Other Res	ults Process													
	mdom Forest Model		Zoom													
-	Model 1 Model 2	Graph	p p													
	Model 3	orapii	Tree													
-	Model 4		Tree *													
	Model 5		Node Labels													
0	Model 6	Description	Edge Labels													
9	Model 7				ler	gth										
9	Model 8								\$1							
2	Model 9											income				
9	Model 10	Annotations								> 18300000	0000	≤ 18300	0000000			
2	Model 11			bors				cos	int				count			
	Model 12				500							> 5.500		≤ 5.500		
	Model 13			2.				> 26.500	£ 28.500					\$ 0.000		
	Model 14					nbors		40.000	0.988		COL				count	
	Model 15				> 2.500	≤ 2.500					> 11	\$11			> 1.500 ≤	1.600
	Model 16 Model 17			inc	ome	inco	me			cou	unt	inco	ome	co	unt	0.689
	Model 18			> 3468025	8882255902	> 46972808207	286627.500			> 15	s 15	> 19997820	1057 920763	> 3.500	£ 3.500	
	Model 19			3.963	0.698	0.436	0.253			18.000	12.000	9.000	6.083	3.776	1.462	
9	Model 20															
9	Model 21															
	Model 22															
	Model 23															
9	Model 24															
	Model 25															
	Model 26															
	Model 27															
	Model 28 Model 29															
	M00e125	v														
		search	O ⊟ł	0 🕫	1	. 🧿	😆 📼	1					😑 23°C S	unny 🔨 🛙	□ @ <i>@</i> 1	4:26 PM 2/14/2022

FIGURE 5.18: TREE DIAGRAM 3

5.4 Random Forest:

The ensemble learning strategy is used for regression in a supervised learning method known as Random Forest Regression. In order to provide predictions that are more accurate than those from a single model, the ensemble learning technique integrates predictions from several machine learning algorithms [17].

2001	meters	Optimal Feature Set	Model Model Simulator	Missing	g Processing	Lift Chart	Known Values	Feature Set Tradeoffs	Feature Eng	ineering Performances	Encoding Processi
Veights	Training Data	Text Processing	Single Row Original	Runtimes	Production	Statistics	Production Model	Production Data	Predictions	Performance	Parameter Performances
	count:		158.217	D D	Prediction						
Model Simulator	income:		8941400681	.82 ①							
	length:		26.210	D D				0.54	+ /		
	neighbors:	0	2.362	Œ							
					Important F	Factors for	Prediction				
					length -0.8	-0.7 -0.6	-0.5 -0.4 -0	3 -0.2 -0.1 0.0	0,1 0,2	0.3 0.4 0.5	0.6 0.7 0.8
									ontradicts Prediction		

FIGURE 5.19: RANDOM FOREST

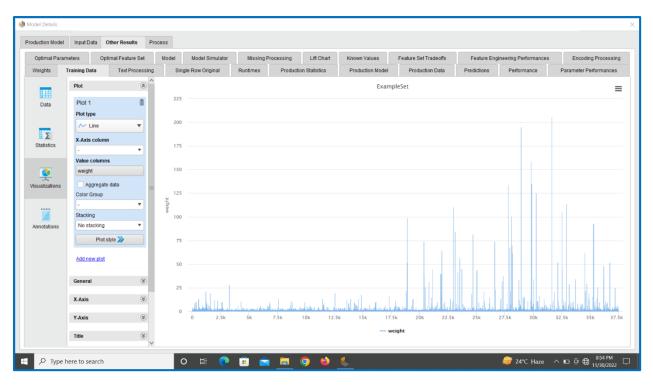


FIGURE 5.20: LINE GRAPH

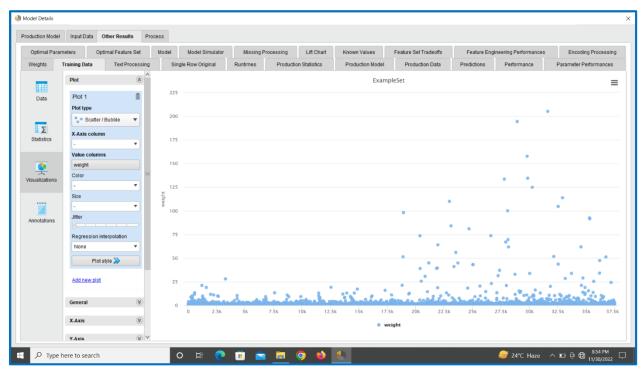


FIGURE 5.21: SCATTER / BUBBLES

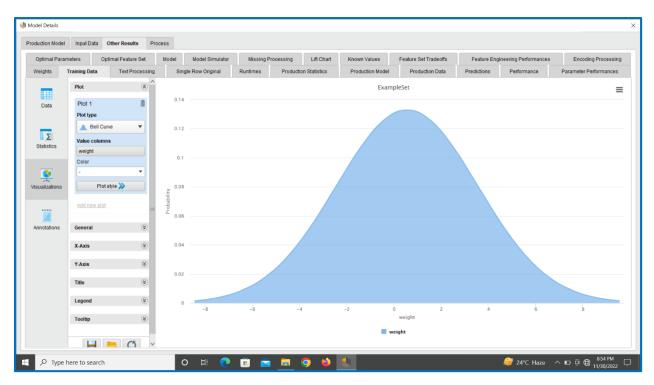


FIGURE 5.22: BELL CURVE GRAPH

Chapter 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion:

Deep learning techniques have been presented to analyze the dataset and produce effective findings (95.6% correct) by analyzing theories to find the presence of a ransomware attack. High-performance deep learning architectures are used and compared in this proposed work. Other methods are also used in this work Gradient-boosted decision trees (GBM) and random forest. Data pre-processing plays very important role in increasing the efficiency and accuracy of the results. We use a technique called backpropagation, also known as backward propagation of mistakes, is created to check for errors as they travel backward from input nodes to output nodes. For data mining and machine learning to increase the precision of predictions, it is a crucial mathematical tool. In fields like deep learning, backpropagation algorithms are frequently employed to train feedforward neural networks. The gradient of the loss function with respect to the network weights is easily computed. It enables the training of multilayer networks and the updating of weights to minimize loss using gradient methods, such as gradient descent or stochastic gradient descent.

Since the data is collected by Kaggle contain few datasets because of the privacy of data.

We have created a model where we can detect Ransomware Attack from the datasets. Secondly, we won't be restricted with only to Ransomware Attacks. We can create a model that will help to detect other attacks. The only thing that will be needed for achieving these goals is dataset. We can create a platform where individuals from all over the world can interact and check their work from our model.

REFERENCES

- M. Grima, "Ransomware Activity Detection," *Ransomware Activity Detection*, 2018.
- [2] D. K. Tripathi, vol. 3, no. 5, 2017.
- [3] kaspersky, "ransomware-attacks-and-types," [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types.
- [4] A. D. C. N. Dhinnesh, "Analysis of Ransomware and its prevention," *Analysis of Ransomware and its prevention*, vol. 5, p. 4, 2020.
- [5] checkpoint, "What is Ransomware?," checkpoint, [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.
- [6] cisecurity.org, "steps-to-help-prevent-limit-the-impact-of-ransomware," [Online]. Available: https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limitthe-impact-of-ransomware.
- [7] imperva, "Ransomware Protection," imperva, [Online]. Available: https://www.imperva.com/learn/application-security/ransomware/.
- [8] securityboulevard, "machine-learning-tackles-ransomwar," [Online]. Available: https://securityboulevard.com/2022/06/machine-learning-tackles-ransomwareattacks/.
- [9] researchgate, "Data-preprocessing," [Online]. Available: https://www.researchgate.net/figure/Data-preprocessing-steps_fig3_228630212.

- [10] docs.h2o.ai, "Deep Learning (Neural Networks)," docs.h2o.ai, [Online]. Available: https://docs.h2o.ai/h2o/latest-stable/h2o-docs/data-science/deep-learning.html.
- [11] "datascience," gradient-boosted-trees, [Online]. Available: https://towardsdatascience.com/a-visual-guide-to-gradient-boosted-trees-8d9ed578b33.
- [12] "analyticsvidhy," understanding-random-forest, [Online]. Available: https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/.
- [13] "bitcoinheist-ransomware-dataset," .kaggle, [Online]. Available: https://www.kaggle.com/datasets/sapere0/bitcoinheist-ransomware-dataset.
- [14] "development-platform-for-data-minin," analyticsvidhya, [Online]. Available: https://www.analyticsvidhya.com/blog/2021/10/intro-to-rapidminer-a-no-codedevelopment-platform-for-data-mining-with-case-study/.
- [15] N. Chourey, "A Study of Ransomware Detection and Prevention at Organizations," 2020.
- [16] "neptune," boosted-decision-trees-guide, [Online]. Available: https://neptune.ai/blog/gradient-boosted-decision-trees-guide.
- [17] "towardsdatascience," visualize-individual-decision-trees-in-a-random-forest,
 [Online]. Available: https://towardsdatascience.com/4-ways-to-visualizeindividual-decision-trees-in-a-random-forest-7a9beda1d1b7.
- [18] "neptune," gradient-boosted-decision-trees-guide, [Online]. Available: https://neptune.ai/blog/gradient-boosted-decision-trees-guide.