VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

BCI 3002: Disaster Recovery and Business Continuity Management (DRBCM)

Slot: A1+TA1

Project Document

TITLE: PREVENTION OF ATTACKS USING ONE CLASS CLASSIFICATION AND AUTO ENCODERS

26th November 2021

Team Leader:
Rohan Allen 18BCI0247

Team Members:
Rakshith Sachdev 18BCI0109
Harshita Pundir 18BCI0192

1. DRBCP:

1.1 PHASES OF DRP AND BCP (DISASTER RECOVERY PLAN AND BUSINESS CONTINUITY PLAN)

Disaster Recovery Plan

Phase 1: Disaster Assessment and Risk Analysis

This project can be divided into functionalities like malware profiling, feature generation, feature database, machine learning classifier, and finally malware detection which separates into malware traffic and clean traffic. Each functionality has different criticality based on its importance. In this, the machine learning classifier and malware detection are mission-critical, and feature generation and feature database fall into business-critical functionalities.

Disasters that have the likelihood to disrupt the system are

- Flood or any natural disaster
- Disasters like fire
- Electrical storms
- Electrical power Failure
- Loss of communications network services

Any damage to the feature database or malware detection system would cause a great threat to the system as a whole and would give free access to all the malicious users to the inside of the system. The damage caused to the organization can include attacks like DDoS, ransomware, or the installation of backdoors in the system. These can be extremely critical and also cause irreversible damage. In case of any disaster, priority needs to be given to the malware detection system and then to feature the database to get them up and running to minimize the loss to the organization.

Phase 2: Activation and Planning

The team will be contacted and assembled by the Emergency Response Team. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with the disaster recovery team, first responders, etc.
- Report to the emergency response team

The planning process should take an “all-hazards” approach. There are many different threats or hazards as mentioned previously. The probability that a specific hazard will impact the system is hard to determine. That’s why it’s important to consider many different threats and hazards and the likelihood they will occur.

Strategies for prevention/deterrence and risk mitigation should be developed as part of the planning process. Threats or hazards that are classified as probable and those hazards that could cause injury, property damage, business disruption, or environmental impact should be addressed.

The system requires hardware, software, data, and connectivity. Without one component of the “system,” the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices, and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

Phase 3: Execution of the Disaster Recovery Plan

In the execution phase, the recovery team finally gets into action and begins executing the recovery activities as per the procedures specified in the plan. For recovery strategies, there are vendors that can provide “hot sites” for IT disaster recovery. These sites are fully configured data centers with commonly used hardware and software products. Subscribers may provide unique equipment or software either at the time of disaster or store it at the hot site ready for use.

Data streams, data security services, and applications can be hosted and managed by vendors. This information can be accessed at the primary business site or any alternate site using a web browser. If an outage is detected at the client site by the vendor, the vendor automatically holds data until the client’s system is restored. These vendors can also provide data filtering and detection of malware threats, which enhance cyber security.

Phase 4: Integrating the Disaster Recovery Plan with the Project Plan

Disaster recovery is not something that is carried out completely in isolation. Thus, in this phase, efforts are made to integrate the disaster plan with the overall project plan.

Procedures for system break-ins:

- Immediately notify management via a predefined emergency notification list and notify the affected network manager.
- Follow up with a system security report to management in the System Security Template. The report will include an assessment of compromised systems or information, system risks, and corrective actions.
- Security management will determine the appropriate corrective action and direct the corrective action based on priority.

Other procedures include the following:

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control systems must be enabled.

Phase 5: Reconstitution and Restoration

Once the execution and testing of the recovery plan are over, this reconstitution phase begins and may last even for a few weeks. The resources and team members that were diverted toward the disaster recovery must be moved back to their original places. Here are some of the activities that form a part of the restoration and reconstitution phase:

- Ensure that there are no remaining aftereffects of the disaster and that no threats have remained unaddressed
- All team members have returned to their original roles
- All resources deployed for the recovery have been secured and relocated to where they are needed
- The disaster recovery efforts are completely over.

Business Continuity Plan:

Phase 1: Business Impact Analysis

A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs), and recovery

point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions, and plans.
Potential effects include the loss of data, equipment, and revenue, loss of staff, reputational damage, and other types of business losses. In this system, functionality like machine learning classifiers and malware detection is critical to the mission, and feature generation and feature databases are critical to the business. With this, the priority of the functions can be set to get the impact analysis.
Risk lurks in all corners of any business: from operational, financial, and strategic risk, to IT and security risk. The potential consequences of those risks include loss of revenue and possible legal action, application outages, and inability to deliver key customer services.
RTO (recovery time objective)
Recovery time objective (RTO) is a key metric that helps calculate how quickly a system or application needs to be recovered after downtime so there is no significant impact on the business operations. In short, RTO is the measure of how much downtime can be tolerated.
If any disaster occurs on this system, the response team begins the recovery process, which starts through the RTO process. This includes restoring backups of feature databases, and machine learning classifiers.
RPO (recovery point objective)
Recovery point objective (RPO) is a metric set for the amount of data loss the business can endure and continue to function without any effect on the business operations.
To calculate the recovery objective values, you need to prepare a list of the workloads and divide them based on their criticality levels. Depending on the priority of applications, individual RPOs and RTOs typically range from 24 hours down to four, down to near-zero measured in minutes.

Criticality level of workload	RTO & RPO values
Mission-critical Workloads	Less than 15 minutes
Business-critical Workloads	2 to 4 hours
Non-critical Workloads	12 - 24 hours

If any disaster occurs on this system, in the RPO phase, critical business functionality of the malware detection and traffic separation function is restored.

Phase 2: Recovery Strategies and Continuity Development

Recovery strategies require resources including people, facilities, equipment, materials, and information technology. An analysis of the resources required to execute recovery strategies should be conducted to identify gaps.
Strategies may involve contracting with third parties, entering into partnership or reciprocal agreements, or displacing other activities within the company. Staff with in-depth knowledge of business functions and processes are in the best position to determine what will work. Possible alternatives should be explored and presented to management for approval and to decide how much to spend.
There are many vendors that support business continuity and information technology recovery strategies. External suppliers can provide a full business environment including office space and live data centers ready to be occupied. Other options include the provision of technology-equipped office trailers, replacement machinery, and other equipment. The availability and cost of these options can be affected when a regional disaster results in competition for these resources.

Phase 3: Implementation and Testing

An effective BCP must be written and communicated to all employees on an ongoing basis.

Phase 4: Maintenance
Risk is not static. Personnel changes, potential threats, and critical business functions will change over time. A BCP must be validated through testing or practical application and must be kept up to date.

1.2 FUNCTIONAL AREA

Modules are grouped into three functional areas:
1. Data Gathering
The model collects intrusion detection and vulnerability data. For intrusion detection in both real-time and non-real-time, the model needs to
• Collect suspicious traffic and ancillary information that describes or characterizes the traffic, identify distinct network connections or associations (connectionless traffic) and include enough detail to assist criminal investigations and prosecutions
• Detect intrusions specific to a designated area of protection
• Detect denial of service attacks to include service overloads, broadcast storms, and message flooding
• Automatically record events and incidents
• Monitor and scan networks
• Monitor and scan hosts
• Detect based on content; for example, a packet body
• Detect intrusions for multiple operating systems
• Detect intrusions for multiple platforms (hosts, switches, routers, etc.)
For vulnerability detection, the model needs to
• Scan networks
• Scan hosts
• Detect vulnerabilities for multiple operating systems
• Detect vulnerabilities for multiple platforms (i.e., hosts, switches, routers, etc.)

2. Decision Support
The model analyzes intrusion detection and vulnerability data. It needs to
• Identify the vulnerability exploitation type of a discovered vulnerability (for example, component, protocol, application, and configuration) and provide information relevant to remedying the vulnerability—whether a remedy is available, what it is, how to apply it, and so forth
• Correlate raw or refined data, such as associating multiple attacks occurring at different targets with the same source and associate system vulnerabilities with attacks
• Aggregate inputs from several sources of the same type into a single incident report and fuse inputs from several sources of disparate types and possibly differing security levels into a single situation report
• Provide both local and remote data analysis tools Ideally, the model at every level of the enterprise will employ a single standardized interface to analysts.

3. Data Storage
• The model should have the ability
– To feed information about verified intrusions and vulnerabilities to a central (single logical) database for analysis and long-term storage
– To use distributed database capability with the attendant ability to feed data from one to another
– To feed “up” to the centralized database from distributed databases
– To feed “down” from archival storage at the centralized database to enable certain kinds of analysis
• Centralized management components of the model should have
– Capacity to store 90 days of collected enterprise data for immediate access and analysis in the manager
– Capability automatically to back up 365 days of collected enterprise data in the manager, with capability for an operator to retrieve and review this historical data

1.3 TECHNICAL AREA

The network IDS usually has two logical components: the sensor and the management station.

1. The sensor sits on a network segment, monitoring it for suspicious traffic. The management station receives alarms from the sensor(s) and displays them to an operator. The sensor enables it to detect any immediate security threats and is the main component. They usually have a signature database that allows them to identify malicious activity. The sensors are usually dedicated systems that exist only to monitor the network. They have a network interface in promiscuous mode, which means they receive all network traffic, not just that destined for their IP address, and they capture passing network traffic for analysis. If they detect something that looks unusual, they pass it back to the analysis station.
2. The analysis station can display the alarms or do additional analysis. Some displays are simply an interface to a network management tool, like HP Openview, but some are custom GUIs designed to help the operator analyze the problem. This consists of two parts: the backend and the frontend. The backend is responsible for alerts and recording any events. The alerts can be sent in a variety of ways, whether it is a database log, email, or console display. Depending on the version, some backend components are able to provide a temporary connection block, which prevents the hacker from accessing its initial target. The front end is the last component, which is the user's interface. The user interface allows the user to view any events that the sensor has detected or set up an IDS configuration. The user can also update the sensor and signature databases. All of these components work together as a whole to provide the ultimate protection against hackers or any type of malicious software that threatens network security.

2. DISASTER RECOVERY PLAN:

2.1 SECURITY

Modern networked business environments require a high level of security to ensure safe and trusted communication of information between various organizations. With the widespread use of technology, businesses of all sizes have significantly benefited from the utilization of the Internet and technical resources. On the other hand, virtual security threats are an ever-increasing problem, and an intrusion detection system can help protect from external threats and provide network security. An intrusion detection system simply monitors network traffic and will alert the network administrator of any unusual activity.An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats.

An intrusion detection system can protect networks and computers from a variety of threats. Besides hackers, an intrusion detection system can protect against all forms of malware or Internet worms. A network intrusion detection system is specifically created to monitor network traffic and it will automatically send an alert of abnormal activities. Whether it is a man-made virus or an international hacker, a network intrusion detection system is the ultimate protection against security threats of all kinds. No firewall is foolproof, and no network is impenetrable. Attackers continuously develop new exploits and attack techniques designed to circumvent your defenses. A network intrusion detection system is crucial for network security because it enables you to detect and respond to malicious traffic.

The primary benefit of an intrusion detection system is to ensure IT personnel is notified when an attack or network intrusion might be taking place. A network intrusion detection system monitors both inbound and outbound traffic on the network, as well as data traversing between systems within the network. The network IDS monitors network traffic and triggers alerts when suspicious activity or known threats are detected, so IT personnel can examine more closely and take the appropriate steps to block or stop an attack.

2.2 OPERATIONAL/APPLICATION/INVENTORY PROFILES

Based on the research gaps identified in previous techniques, we have provided an architecture for securing systems towards network-based attacks. Our proposed network intrusion detection system is an architecture that presents an autoencoder based anomaly detection model for intrusion detection, we use

the NSL-KDD dataset, this dataset is a benchmark for machine learning-based intrusion detection, however, it suffers from several inefficiencies such as class imbalance, where for instance in the NSL-KDD training dataset only 0.04% of the samples belong to the u2r attack type making it severely underrepresented, the case is similar for the r2l and probe attack types whereas the majority of attack records are representing the DDOS attack type, this fact made it difficult for classifiers to detect these underrepresented types resulting in poor accuracy. Another issue is that this dataset is unrealistic, in reality, most traffic in a network is benign and only a small percentage might be malicious, while in the NSL-KDD training set, for example, attack samples compose 80% of the entire dataset which makes the models trained using this dataset ineffective in real-life situations. Our autoencoder-based approach attempts to overcome these problems.

The 37 attack types available in the dataset can be clustered into four general attack types

- Denial of service attacks
- Remote to Local attacks
- User to Root
- Probe attacks

Our model will perform binary classification of the data to two classes indicating whether the traffic is normal or an Attack, however, we will use the four attack types to analyze the results and calculate performance metrics for each general attack type.

The next section replaces the current outcome field with a Class field that has one of the following values:

- Normal
- Dos
- R2L
- U2R
- Probe

In order to avoid the imbalance of the samples representing each attack type in the training data, and to avoid the model's inability to learn about new attack types by observing existing ones, we present an approach that utilizes autoencoders and reconstruction error to detect anomalies.

In this approach we implemented a sparse autoencoder with dropout on the inputs, it consists of an input layer of 122 neurons due to the fact that the number of features for each sample is 122 followed by a dropout layer and a hidden layer of 8 neuron units so the hidden representation of the autoencoder has a compression ratio of 122/8 forcing it to learn interesting patterns and relations between the features, finally, there is an output layer of 122 units, the activation of both the hidden layer and the output layer is the real function.

The autoencoder was trained to reconstruct its input, in other words, it learns the identity function, the model was trained using only the samples labeled "Normal" in the training dataset allowing it to capture the nature of normal behavior, this was accomplished by training the model to minimize the mean squared error between its output and its input.

The model performs anomaly detection by calculating the reconstruction error of samples, since the model was trained using normal data samples only the reconstruction error of samples that represent attacks should be relatively high compared to the reconstruction error of normal data samples, this intuition allows us to detect attacks by setting a threshold for the reconstruction error, if a data sample has a reconstruction error higher than the preset threshold then the sample is classified as an attack, otherwise, it's classified as normal traffic.

For the choice of a threshold two values can be helpful for guiding the process, the model loss over the training data and over the validation data, we found by experiment that a choice around these values produces acceptable results, for our experiments we use the model loss over the training data as a threshold.

Due to the nature of this approach, it can only be used for 2-Class classification as it is purely for anomaly detection and not classification.

2.3 DRP

A network disaster recovery plan is a set of procedures designed to prepare an organization to respond to an interruption of network services during a natural or manmade catastrophe.

Voice, data, internet access, and other network services often share the same network resources. A network disaster recovery (DR) plan ensures that all resources and services that rely on the network are back up and running in the event of an interruption within certain a certain specified time frame.

Such a plan usually includes procedures for recovering an organization's local area networks (LANs), wide area networks (WANs), and wireless networks. It may cover network applications and services, servers, computers, and other devices, along with the data at issue.

Network services are critical to ensuring uninterrupted internal and external communication and data sharing within an organization. Network infrastructure can be disrupted by any number of disasters, including fire, flood, earthquake, hurricane, carrier issues, hardware or software malfunction or failure, human error, and cybersecurity incidents and attacks.

Some important caveats to consider when preparing a network disaster recovery plan include the following:

- Use business continuity standards. There are nearly two dozen BC/DR standards and they are a useful place to start when creating a contingency plan.
- Determine recovery objectives. Before starting on a plan, the organization must determine its recovery time objective (RTO) and recovery point objective (RPO) for each key service and data type. RTO is the time an organization has to make a function or service available following an interruption. RPO determines the acceptable age of files that an organization can recover from its backup storage to successfully resume operations after a network outage. RPO will vary for each type of data.
- Stick to the basics. A network DR plan should reflect the complexity of the network itself and should include only the information needed to respond to and recover from specific network-related incidents.
- Test and update regularly. Once complete, a network DR plan should be tested at least twice a year and more often if the network configuration changes. It should be reviewed regularly to ensure it reflects changes to the network, staff, potential threats, as well as the organization's business objectives.
- Stay flexible. No one approach to creating a network disaster recovery plan will work for every organization. Check out different types of plan templates and consider whether specialized network DR software or services might be useful.

Network disaster recovery planning provides guidelines for restoring network services and normal operations following a disaster. The plan outlines resources needed to perform network recovery procedures, such as equipment suppliers and information on data storage. It describes how off-site backups are maintained, and it identifies key staff members and departments, and outlines their responsibilities in an emergency. The plan spells out responses unique to specific types of worst-case scenarios, such as a fire, flood, earthquake, and terrorist attack or cyberattack.

A network disaster recovery plan also identifies specific issues or threats related to an organization's network operations. These can include interruptions caused by loss of voice or data connectivity as a result of network provider problems or disasters caused by nature or human activities.

Some specific sections that should be included in a network disaster recovery plan include the following:

- Emergency contacts and actions. List the IT network emergency team members and their contact information at the front of the plan for fast access. A list of initial emergency response actions should also be upfront.
- Purpose and scope. Outline the purpose of the plan and its scope, along with assumptions, team descriptions, and other background information.
- Instructions for activating the plan. Describe the circumstances under which the contingency plan will be activated, including outage time frames, who declares a disaster, who is contacted and all communication procedures to be used.
- Policy information. Include any relevant IT BC/DR policies, such as data backup policies.

- Emergency management procedures. Provide step-by-step procedures on how networks will be reconfigured and data accessed, what outside help might be needed and how staff will be accommodated for each different kind of potential disaster.
- Data collection. Describe the information that might be needed before officially declaring a network disruption, including network performance data and staff and first responder reports.
- Disaster declaration. Identify actions to take once the network emergency team determines it's necessary to declare a network disaster, including how the decision is communicated, who is contacted, and what additional damage assessments are needed.
- Disaster recovery. Provide instructions on restoring network operations, connectivity, devices, and related activities.

The network disaster recovery plan doesn't exist in a vacuum, but rather is part of an organization's broader IT disaster recovery plan. Data backup is a key part of both the overall IT plan and the network plan, and information on an organization's backup policies and procedures should be included in DR planning.

Options for data backup range from having dual data centers in different locations, each of which can handle all of an organization's data processing needs. The data centers run in parallel and synchronize or mirror data between them. Operations can be shifted from one data center to another in an emergency. Dual data centers are not an option open to every organization. Leased colocation facilities are an alternative.

Other options include backing up data to dedicated backup disk appliances with management software that's either integrated into the appliance or run on a separate server. The backup software runs the data copying process and enforces backup policies for an organization. A backup appliance is an effective option as long as it's located where it won't be hit by the same disasters as an organization's original data.

2.4 BIA

A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs), and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions, and plans.

Its purpose is to determine how the interruption of the business operations may affect your organization. Potential effects include the loss of data, equipment, and revenue, loss of staff, reputational damage, and other types of business losses. In this system, functionality like machine learning classifiers and malware detection is critical to the mission, and feature generation and feature databases are critical to the business. With this, the priority of the functions can be set to get the impact analysis.

Risk lurks in all corners of any business: from operational, financial, and strategic risk, to IT and security risk. The potential consequences of those risks include loss of revenue and possible legal action, application outages, and inability to deliver key customer services.

One of the most critical risks organizations face is a disruption to their key business applications, such as e-commerce, email, purchasing, etc, leading to loss of revenue or productivity. As such, it’s important that the network and security operations teams focus their risk mitigation efforts on ensuring that the applications, servers, and network infrastructure that support and drive key revenue-generating business processes are hardened against potential disruption or compromise. So how can IT teams approach this?

Identifying network security risk

First and foremost, organizations must identify the potential risks points within their enterprise networks. The key to this is identifying all firewalls and routers in the network, and then conducting an in-depth examination of each device including all the policies and rules that each device supports. When done manually, this is an extremely time-consuming process of mapping and documenting flows; it can be accelerated dramatically with an automated security management solution.

Once every device's policies and rules are fully documented and traffic flows mapped, it is then possible to identify the risks that exist within the network and security infrastructure – which will generally speak fall into one of three categories.

The first of these is incorrect device configuration, which occurs when IT teams fail to ensure that each network security device is configured in accordance with vendor guidelines.

Risk is also introduced into the security fabric in instances where it fails to support the compliance and regulatory requirements of the organization, either in terms of the capabilities of the solutions deployed, or the rule sets that must be implemented.

Utilizing BIA principles
With the risks in the network infrastructure identified it is now possible to start remediating them using BIA methodology principles.

At the heart of this is establishing which of the processes affected by these risks are critical to business operations. By taking the inventory of firewall devices, policies, and rules and overlaying it with a map of all of the applications in the network and their connectivity flows, organizations can then identify how these flows support business processes and, more importantly, which of those processes are critical to core business functions.

Finally, the IT team can then prioritize the network security risks based on their impact on business-critical applications, and remediate them accordingly.

Less risk, enhanced business-driven security
Identifying network security risks is critical to any business. However, it is likely that there will be too many risks to address all at once. By aligning with the BIA methodology, the IT team will not only have greater visibility of the risks that exist but also how those risks will impact the organization if they are not remediated. And ultimately, this enables the IT team to ensure that the organization's security infrastructure is strategically supporting, and driving, the needs of the business.

2.5 STEPS

Network connectivity often gets overlooked in disaster recovery management as business owners are more concerned about network security and ensuring that no unauthorized user can access data transferred over the network.

1. Identify business continuity and disaster recovery objectives
This is an important step in network disaster recovery planning because identifying your business continuity (BC), and disaster recovery objectives allows you to determine what your DR plan needs to accomplish. Recognizing the expectations for network disaster recovery helps to define how the DR plan should be structured in order to achieve the best results.

2. Assess potential risks and threats
Determine various risks and threats which the organization is most exposed to that can disrupt the network services. After assessing potential dangers, come up with preventive measures to stop them from occurring in the future or, at least, mitigate their possible impact on the infrastructure.

3. Create an IT recovery team and assign responsibilities
It is not enough to create a network disaster recovery plan, also decide who will implement the plan when an actual disaster strikes. Thus, create a recovery team and identify the employees that will join it. Each

recovery team member should be assigned a specific role and a unique set of responsibilities to avoid any confusion and panic during a DR event.

4. Determine critical network components and the impact of their failure
Every infrastructure consists of various components which have different levels of importance and criticality. When it comes to network connectivity, it is crucial to determine possible repercussions in case a particular network device goes down and identify which network services are most critical for business performance.

5. Regularly test and update the plan
After designing the network disaster recovery plan, notify staff about what it includes and what actions they should undertake before, during, and after a DR event. Even though the plan might look good on paper, still need to test it in your production environment to verify that everything works as planned, the employees know their roles and responsibilities, and the BC goals and DR objectives are realistic and can be easily met.

6. Keep various network types in mind
It is extremely rare for an organization to use only one network for conducting business operations. If the organization uses multiple networks for data transfer and service delivery, consider how different those networks are and what would be the impact of their disruption on business. After that, consult with the network administrator and come up with a set of workable mechanisms and procedures for recovering each type of network within the system.

7. Back up network configuration files
When it comes to network disaster recovery planning, the main aim is to ensure that a network is restored to its normal state as rapidly as possible. That is why it is important to regularly back up network configuration files, including the initial parameters and settings for configuring network devices. For that purpose, install third-party data protection software, which can be used to back up and recover mission-critical data when your infrastructure is hit by a disaster.

8. Reconfigure network infrastructure
Network disaster recovery planning helps identify vulnerabilities in the network infrastructure and, as a result, this might require reconfiguring all network devices in the system. To transform the network infrastructure, make sure that the network doesn't have a single point of failure. For that purpose, add new network paths, routers, switches, and other network components, which would serve as a safety net in case the network ever goes down.

9. Document each step of the network disaster recovery process
Even though it might seem as an obvious step, it is crucial to write down everything clearly and in detail so as to avoid any confusion and misleading interpretations during an actual disaster. Also, don't forget to document the process of plan testing as it helps to identify weaknesses and inconsistencies in the network infrastructure and evaluate the efficiency of the current network disaster recovery plan.

2.6 NOTIFICATION AND ACTIVATION PROCEDURES

Activation is the means by which the actions contained in a documented DRP are initiated and executed. A qualifying event occurs and planned steps are taken.
To that end, activation procedures should be defined according to three primary guidelines:

1. Activation scope must incorporate five key elements to ensure that related procedures are fully actionable (considering DRP scope and specifics).
2. Activation guidelines must focus on triggering events and conditions, to clearly analyze and evaluate current circumstances, and to determine whether the DRP will be activated.

3. Activation steps must be defined so that they can be executed in a consistent, orderly fashion. Everyone should know what they need to do and how they need to do it.

Activation scope the totality of all related strategies and procedures to ensure that the DRP can be invoked when needed, and in an orderly, effective fashion, encompassing the following elements:

- Activation Criteria. To identify the specific disaster conditions triggering plan activation.
- Assessment Procedures. To evaluate potential disaster events in order to ensure that activation criteria have been met.
- Approval Mechanisms. To obtain appropriate approvals for plan activation, considering IT management personnel, line of business management personnel, and company executives.
- Activation Logistics. To ensure that all facilities and systems are available as needed to support plan activation, including the designated Command Center location, where most, if not all, disaster recovery "command and control" activities can be executed.
- Communication Procedures. To inform all employees and other interested parties (customers, vendors, suppliers, the public) of all activation-related decisions and activities.

3. BUSINESS CONTINUITY MANAGEMENT

3.1 BCP AND STRATEGIES STANDARDS AND GUIDELINES

Recovery strategies require resources including people, facilities, equipment, materials and information technology. An analysis of the resources required to execute recovery strategies should be conducted to identify gaps.

Strategies may involve contracting with third parties, entering into partnership or reciprocal agreements or displacing other activities within the company. Staff with in-depth knowledge of business functions and processes are in the best position to determine what will work. Possible alternatives should be explored and presented to management for approval and to decide how much to spend.

Depending upon the size of the company and the resources available, there may be many recovery strategies that can be explored.

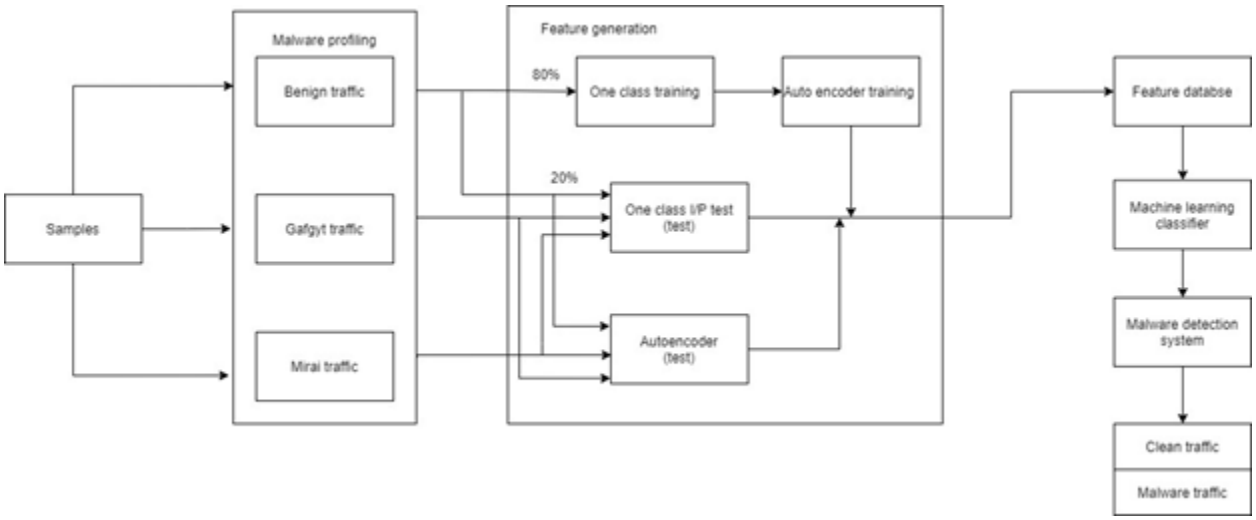
Utilization of other owned or controlled facilities performing similar work is one option. Operations may be relocated to an alternate site - assuming both are not impacted by the same incident. This strategy also assumes that the surviving site has the resources and capacity to assume the work of the impacted site. Prioritization of production or service levels, providing additional staff and resources, and other action would be needed if capacity at the second site is inadequate.

In an emergency, space at another facility can be put to use. Cafeterias, conference rooms, and training rooms can be converted to office space or to other uses when needed. Equipping converted space with furnishings, equipment, power, connectivity and other resources would be required to meet the needs of workers.

Partnership or reciprocal agreements can be arranged with other businesses or organizations that can support each other in the event of a disaster. Assuming space is available, issues such as the capacity and connectivity of telecommunications and information technology, protection of privacy and intellectual property, the impacts to each other’s operation, and allocating expenses must be addressed. Agreements should be negotiated in writing and documented in the business continuity plan. A periodic review of the agreement is needed to determine if there is a change in the ability of each party to support the other.

There are many vendors that support business continuity and information technology recovery strategies. External suppliers can provide a full business environment including office space and live data centers ready to be occupied.

3.2 PROJECT ORGANISATION



There are three types of datasets given as input - benign traffic containing 40,395 records, Mirai traffic containing 652,100 records, and Gafgyt traffic containing 316,650 records. Benign traffic is the good traffic containing clean data whereas Gafgyt and Mirai traffic both contain malicious data which comprises malware traffic. 115 features belong to each record that was produced by the publishers of the dataset through the raw characteristics of the network traffic. Here, both Gafgyt and Mirai traffic is combined to build the malicious data (968,750 records) since they are both generated from attack activity. 80% of the benign traffic data is given as input to the one-class classifier for training the model. This means that 32, 316 records were used to train the model and (40,395 – 32,316) + (652,100 + 316,650) = 976,829 records were used to evaluate the performance of the model. This is also further given as input for the training of the autoencoder model. The rest 20% of the benign traffic data is sent to the testing phase of both the one-class classifier and autoencoder model.
The Gafgyt and Mirai traffic data, which contains the malicious data are inputted along with the 20% of the benign traffic data to test the one class classifier and autoencoder models whether they help in sorting the traffic into clean and malware traffic.
Pre-processing of data is done so as to improve the quality of the datasets involved. Since there are multiple datasets involved, functions are constructed to ensure that these multiple datasets are loaded to be entered into the required model.

So, in this project, the training model is created only using benign instances, and this trained model is then implemented to detect any unknown/new cases of traffic using machine-learning and other statistical methods. If the data targeted shows considerable diversion according to predetermined calculations, it will be labeled as out-of-class. Thus, one-class classifiers that may belong to different families are examined here under the criterion of performance. The two one-class classifiers and their corresponding families have shown here are the One-Class Support Vector Machine from the typical ML family and Autoencoder from the deep learning family. Here, we are considering that benign occurrences have a different kind of structure compared to that of corrupted occurrences. This structural difference is taken as the basis for creating the Autoencoder model.
One-class classifiers help detect instances of a particular class from all the other instances, through training sets containing only the instances of that class. The particular class considered here is a benign

class. There are other kinds of one-class classifiers where opposite instances are considered to sharpen the limit of classification.
The support vector machine, or SVM, algorithm can be incorporated into one-class classification, even though it's mostly meant for binary classification. In cases of imbalanced classification, the weighted and standard support vector machine can be applied on the dataset before one-class classifiers are implemented. For one-class classification, the algorithm helps size up the density of the majority class and categorizes the extreme cases of the density function on either side as outliers. This variation of support vector machine is called a one-class support vector machine.
Autoencoder neural network is an unsupervised ML algorithm that incorporates backpropagation by keeping the required values the same as the inputted values. This helps decrease the size of the input into reduced representation. The original data can be reassembled from the compressed data. The primary goal of autoencoders is to learn the representation of a dataset, mainly for the simplification of dimensionality, by training it to overlook noise data. The input is compressed and put into a latent-space representation and the autoencoders then reconstruct the output out of this.
The features extracted through the above algorithms are then registered and stored in a database called the feature database. The machine learning classifiers included in the project are explained above. Thus, malware detection can be directly implemented resulting in allowance of the benign traffic to be sent and received through the device and removal of any transmission back and forth
of malicious data found due to the presence of Gafgyt and Mirai datasets

3.3 CRISIS COMMUNICATION PLAN

While crisis communication is often reactive, having a crisis communication plan in place can make the process go more smoothly for the team.

1) Spokesperson Response
The best thing to do when firm makes a mistake is apologize and be human. The most efficient approach to do so is to appoint a spokesperson to represent the company. After all, relating to one person is much easier than relating to a bunch of lawyers.
This individual could be CEO, a company executive, or someone else believed most suited to represent the organization. It's critical to pick a good communicator because their actions will have an impact on how key stakeholders respond to the circumstance. Stakeholder support will be greatly enhanced if they can make organization appear human and mistakes appear manageable.

2) Damage Control in Advance
Even though things are going well right now, always be prepared for a disaster. What to do to lessen or prevent the effects of a crisis before it happens is known as proactive damage control. Adding security software that records and backs up project data can help avoid a malware attack.

3) Reaction on social media
Social media is a fantastic marketing tool that enables businesses to contact consumers all over the world. Customers may share tales, photos, and videos with the rest of the world, so this reach works both ways. A single viral video that portrays the company in a poor way might cause millions of people to have a negative impression of organization. Both in-person and online, crises are combated. As a result, business requires a social media strategy to control the digital buzz surrounding it. This might entail assigning more representatives to watch social media platforms or providing new information to fans.

4) Collecting and analyzing customer feedback
A catastrophe may arise, but it isn't reported on the front page of the newspaper or goes viral on social media. Instead, it's quietly harming your consumers and leading to churn, but you're not aware of it since you're not collecting enough input from them.

Getting input is a fantastic strategy to avoid a problem. This is because it gives you insight into how your customers feel about your company. This enables you to identify key impediments before they become a problem. It also allows customers to provide negative feedback, which you can use to improve the experiences of other customers.

3.4 EMERGENCY RESPONSE PLAN

A Cybersecurity Incident Response Plan (CISRP) is a document that instructs IT and cybersecurity experts on how to respond to a significant security incident, such as a data breach, data leak, ransomware attack, or loss of critical data. Most effective incident response plans, according to the National Institute of Standards and Technology (NIST), have four phases: preparation, detection, and analysis, containment, eradication, and recovery, and post-event activities.

- Conduct a risk assessment across the organization to determine the likelihood vs. severity of hazards in key areas. Check to see if the risk assessment is up to date.
- Determine who are the most important members of the team and who are the most important stakeholders.
- Types of security incidents should be defined.Inventory your assets and resources.
- Draw a diagram of the information flow.
- Prepare a number of different public statements. To avoid reputational harm from security issues, have the appropriate data breach notification letters ready to go ahead of time.
- Make a log of the incident's events. Keep note of everything done during and after a cybersecurity event to assess the effectiveness of response and learn from it. During and after threat identification, this account will assist the legal team and law enforcement.

3.5 CONTINGENCY PLAN

The purpose of contingency planning is to ensure that business operates as smoothly as possible, despite mistakes and unexpected events. A basic contingency plan would be to back up all website data in the event that your site is hacked. After regaining access and changing passwords, restore the data if this scenario occurs.

A denial-of-service (DoS) attack attempts to halt traffic flow to and from the target system. The IDS receives an unusual volume of traffic that it cannot handle, and it shuts down to protect itself. This makes it impossible for typical traffic to access a network. An online business might be inundated with online orders on a major sale day, and because the network can't handle all of the requests, it would shut down, preventing paying consumers from making purchases.

Building a strong infrastructure is undoubtedly the cornerstone of DDoS mitigation. The following are all key initial steps for DDoS mitigation: Keeping resilience and redundancy top-of-mind through the following are all crucial first actions for DDoS mitigation:

- Increasing bandwidth capability
- Segmenting networks and data centers in a secure manner
- Mirroring and failover configuration
- Adding robustness to applications and protocols
- Using resources such as content delivery networks to improve availability and performance (CDNs)

4. DRP IMPLEMENTATION:

4.1 IMPLEMENTATION

Evaluation

To evaluate the model we calculate the following performance metrics:

- Accuracy

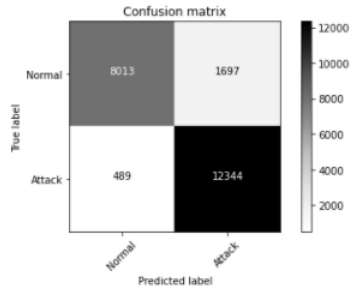
- Recall
- Precision
- F1 Score
- Detection rate for each of the five possible labels

```
accuracy=accuracy_score(y0_test,testing_set_predictions)
recall=recall_score(y0_test,testing_set_predictions)
precision=precision_score(y0_test,testing_set_predictions)
f1=f1_score(y0_test,testing_set_predictions)
print("Performance over the testing data set \n")
print("Accuracy : {} , Recall : {} , Precision : {} , F1 : {}\n".format(accuracy,recall,precision,f1 ))

#


for class_ in classes:
    print(class_+" Detection Rate : {}".format(len(np.where(np.logical_and(testing_set_predictions==1 , y_test==class_))[0])/len(
```

```
Performance over the testing data set

Accuracy : 0.9030297653373552 , Recall : 0.9618951141588094 , Precision : 0.8791396624172068 , F1 : 0.9186574384163132

Normal Detection Rate : 0.17476828012358395
Dos Detection Rate : 0.9414614981665793
R2L Detection Rate : 0.9856035437430787
U2R Detection Rate : 0.9552238805970149
Probe Detection Rate : 1.0
```

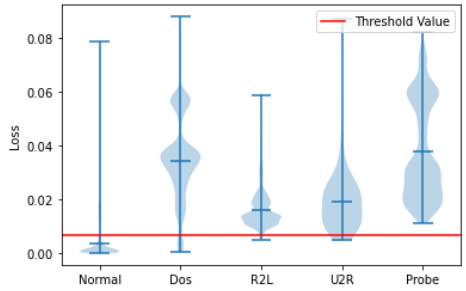
Plotting confusion matrix

```
#Plotting confusion matrix

def plot_confusion_matrix(cm, classes,
                          normalize=False,
                          title='Confusion matrix',
                          cmap=plt.cm.Greys):
    """
    This function prints and plots the confusion matrix.
    Normalization can be applied by setting `normalize=True`.
    """


    plt.imshow(cm, interpolation='nearest', cmap=cmap)
    plt.title(title)
    plt.colorbar()
    tick_marks = np.arange(len(classes))
    plt.xticks(tick_marks, classes, rotation=45)
    plt.yticks(tick_marks, classes)

    fmt = '.2f' if normalize else 'd'
    thresh = cm.max() / 2.
    for i, j in itertools.product(range(cm.shape[0]), range(cm.shape[1])):
        plt.text(j, i, format(cm[i, j], fmt),
                 horizontalalignment="center",
                 color="white" if cm[i, j] > thresh else "black")

    plt.tight_layout()
    plt.ylabel('True label')
    plt.xlabel('Predicted label')
c = confusion_matrix(y0_test,testing_set_predictions)
plot_confusion_matrix(c,["Normal","Attack"])
```



Violin plot

```
plt.ylabel('Loss')
plt.xticks(np.arange(0,5), classes)
plt.violinplot([test_losses[np.where(y_test==class_)] for class_ in classes],np.arange(0,len(classes)),showmeans =True )
plt.axhline(y=threshold,c='r',label="Threshold Value")
plt.legend();
```



4.1.1 RESULTS WITH NECESSARY METRICS WITH GRAPH

- CBA metric

To form the Cost-Benefit Analysis metric we follow the following steps:
1. Identification of the Assets and Values
2. Identification of Threats and Vulnerabilities
3. Risk Assessment and Prediction of the Likelihood of Occurrence
4. Computation of Annual Loss Expectancy (ALE)
5. Management and Control
6. Cost-Benefit Analysis

- Audit metrics

There are many classification metrics for IDS, some of which are known by multiple names.

IDS are typically evaluated based on the following standard performance measures:
1.) True Positive Rate (TPR): It is calculated as the ratio between the number of correctly predicted attacks and the total number of attacks. If all intrusions are detected then the TPR is 1 which is extremely rare for an IDS. TPR is also called a Detection Rate (DR) or the Sensitivity. The TPR can be expressed mathematically as
TPR=TP/(TP+FN)

2.) False Positive Rate (FPR): It is calculated as the ratio between the number of normal instances incorrectly classified as an attack and the total number of normal instances.
FPR=FP/(FP+TN)

3.) False Negative Rate (FNR): False-negative means when a detector fails to identify an anomaly and classifies it as normal. The FNR can be expressed mathematically as:
FNR=FN/(FN+TP)

4.) Classification rate (CR) or Accuracy: The CR measures how accurate the IDS is in detecting normal or anomalous traffic behavior. It is described as the percentage of all those correctly predicted instances to all instances:
Accuracy=TP+TN/(TP+TN+FP+FN)

- RM metrics

The level of dangerousness (Risk) of an alert can be classified using a number of characteristics. It is critical to comprehend their significance in order to properly manage notifications based on their level of importance.

1. Priority: As a result, this level is solely determined by the alert. This parameter's value can be changed between 0 and 5.

2. The monetary worth of the target host: This is a value used to indicate how important a host is on the network. This number must be between 0 and 5, with 0 denoting a less important machine and 5 denoting a very important machine. For each device in the organization, this value is kept in a MySQL database.

3. Reliability: As a result, the term reliability might be translated as the assurance that an alarm is not a false positive. This parameter's value ranges from 0 to 10. This value is saved in a MySQL database and is linked to a different kind of event (IDS Signature).

4. The alert's severity: Each generated alert has a severity rating connected with it to assist us to understand the hazard posed by the occurrence. Severity levels range from 0 to 5 (0 = Clear, 5 = Critical). To assess the risk of an alert, use the Risk Calculation to connect the four preceding parameters using the formula below:

RiskAssessment(RA)=((P)*(D)*(S)*(R))/125

The 125-value was generated by calculating the Risk using the Maximum Value of each parameter, keeping in mind that the Risk Assessment must not exceed 10.For each Alert, the suggested model calculates the risk.

Risk value	Signification
0, 1, 2, 3	Low
4, 5, 6, 7	Medium
8, 9, 10	High

5. TESTING:

5.1 RISK MANAGEMENT

5.1.1 RISK MANAGEMENT LIFE CYCLE POLICIES AND PROCEDURES

The risk management process is a framework for the actions that need to be taken. There are five basic steps that are taken to manage risk; these steps are referred to as the risk management process. In manual systems, each step involves a lot of documentation and administration.

Step 1: Identify the Risk
The first step is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks – legal risks, environmental risks, market risks, regulatory risks, and much more. It is important to identify as many of these risk factors as possible. In a manual environment, these risks are noted down manually.

Step 2: Analyze the Risk
Once a risk has been identified it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the organization. To determine the severity and seriousness of the risk it is necessary to see how many business functions the risk affects. There are risks that can bring the whole business to a standstill if actualized, while there are risks that will only be minor inconveniences in the analysis.

Step 3: Evaluate or Rank the Risk
Risks that need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on the severity of the risk. A risk that may cause some inconvenience is rated lowly, risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization to gain a holistic view of the risk exposure of the whole organization.

Step 4: Treat the Risk
Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs. In a manual environment, this entails contacting each and every stakeholder and then setting up meetings so everyone can talk and discuss the issues. The problem is that the discussion is broken into many different email threads, across different documents and spreadsheets, and many different phone calls. In a risk management solution, all the relevant stakeholders can be sent notifications from within the system. Instead of everyone contacting each other to get updates, everyone can get updates directly from within the risk management solution.

Step 5: Monitor and Review the Risk
Not all risks can be eliminated – some risks are always present. Market risks and environmental risks are just two examples of risks that always need to be monitored. Under manual systems monitoring happens through diligent employees. If any factor or risk changes, it is immediately visible to everyone. Computers are also much better at continuously monitoring risks than people. Monitoring risks also allows your business to ensure continuity.

5.2 ASSESSMENT AND EVALUATION

5.2.1 DEVELOPMENT OF RISK ASSESSMENT METHODOLOGY

5.2.1.1 CBA

To form the Cost-Benefit Analysis metric we follow the following steps:

1. Identification of the Assets and Values - In order to start our analysis, we must identify the assets of a network system and their values. Similarly to computer systems, the assets of a network system can be divided into several categories: Equipment and Hardware(computers, disks, tape drivers, printers, telecommunication, network systems, modems), Software (operating systems, utility programs, diagnostic programs, application programs.), Services (commercially provided services, such as teleprocessing, local batch processing, on-line processing, internet access, e-mail, voice mail, telephone, fax, and packet switch of data), Supplies (any consumable item designed specifically for use with equipment, software, service or support service), Personnel (salaries and benefits for persons who perform functions, such as development, support, management, operation and analysis for running this system) and other resources.
To properly assign values to assets, we need to consider their market value, depreciation, and discount value. When an asset is first purchased, it is purchased at its market or book value. After a certain amount of time, the value of the asset will decrease, thus resulting in depreciation. We then use the following formula to calculate the actual value of an asset at any given point in time:

$P= F(1/(1+I)n)$
Where P = present value, F = Future Value, I=Interest rate, and n = number of years.

2. Identification of Threats and Vulnerabilities - A threat is any action that can affect the security of assets and cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. Vulnerabilities are the weaknesses in the defense mechanisms of an information system. A threat is manifested by a threat agent using a specific technique, methodology, or spontaneous occurrence to produce an undesired effect on a network system. To clearly identify risks, we must identify the various threat agents and the methodologies that they use.

3. Risk Assessment and Prediction of the Likelihood of Occurrence - items and procedures to the likelihood of occurrence relate to the stringency of the existing controls:
i) Calculate the probability that the risk may happen, found in the observed data for the specific system.
ii) Estimate the number of occurrences in a given time period.
iii) Estimate the likelihood from a table. The analyst gives a rating based on several different risk analysis methodologies and then creates a table to hold and compare the ratings.
iv) The Delphi approach: several raters individually estimate the probable likelihood of an event, combine their estimates, and choose the best one.

4. Computation of Annual Loss Expectancy (ALE) - Because of the complication of assets and threats, it is difficult to estimate the precise value of each event. We use annual loss expectancy (ALE) to represent the cost of every event in a year. Once we determine the cost of one event, we can calculate the ALE by multiplying that cost by the number of incidents. For example, one event, with an expected cost of $20,000, may happen 2 times a year, while another event that costs $500,000 may occur once every 4 years. The ALE of the first event is $40,000, while the ALE of the second event is $125,000. We calculate the total ALE for this organization by adding the ALE's of the events together.

5. Management and Control - The purpose of management and control is to evaluate identified risks according to the degree of their acceptability/unacceptability, in consideration of the nature of the threats and vulnerabilities as they relate to risk, as well as identifying and selecting countermeasures to effectively reduce the risk. In other words, with the existing control, we calculate the expected loss. If the loss is unacceptably high, then we implement new controls. This process includes selecting countermeasures, testing their effectiveness, and performing a cost-benefit analysis. Some suggested countermeasures are cryptographic controls, such as secure protocol and operating system protection features. Also available are identification and authentication countermeasures, such as access controls and physical controls

6. Cost-Benefit Analysis - The purpose of the cost-benefit analysis is to periodically review the effectiveness of planned and implemented security controls to determine if they are doing what they are supposed to do, rather than creating additional vulnerabilities. It is used to support the management and control actions. After completing steps 1 to 5, we compute the true cost or savings from the implementation of new countermeasures. We then calculate the effective cost, which is the new countermeasure cost minus any reduction in ALE from the use of the new countermeasure.

Justification of an Intrusion Detection System

ITEM	AMOUNT
Risk: disclosure and damage of company confidential data	
Cost to recover data: $200,000 @ 50% likelihood per year	$100,000
Effectiveness of the tool: 85%	-$85,000

Cost of tool	$40,000
ALE due to loss and control: $100,000 -$85,000 + $40,000	$55,000
Savings: $100,000 -$55,000	$45,000

5.3 TOOLS AND TECHNIQUES

Selected tools and techniques commonly applied to risk management in projects were presented to respondents to select as it applies to projects in their organisations. The data as presented in the table below shows checklist, brainstorming, and benchmarking as the most ranked. Risk simulation, risk probability assessment, graphical representation of risk, and risk classification were the listed ranked.

Which of these applies to your projects	Frequency	Mean	Rank
Checklist	53	0,155	22
Brainstorming	39	0,114	20
Training Programmes	17	0,050	15
Analysis Of Trend And Deviations	7	0,021	8
Requirement Management	11	0,032	11
Benchmarking	45	0,132	21
Cause And Effect Analysis	16	0,047	14
Cost-Benefit Analysis	22	0,065	17
Contingency Plans For Risk Analysis	8	0,023	9
Time-Limited Actions	11	0,032	11
Customer Satisfaction	31	0,091	19
Replanning Of Project	11	0,032	11
Graphic Representation Of Risk	2	0,006	3
Responsibility Assignment	23	0,067	18
Quality Control And Management	6	0,018	6
Risk Classification	2	0,006	3
Risk Quantative Simulation	0	0,000	1
Risk Documentation	3	0,009	5
Ranking Of Risk	9	0,026	10
Risk Prioritization	19	0,056	16
Risk Impact Assessment	6	0,018	6
Risk Quantative Probability Assesment	0	0,000	1

The result in the table above could be interpreted that a more qualitative analysis based on experience, perception, or expert opinion is applied by SMEs in which case prior project experience or length of work experience in the project is vital to the organization. The problem here is that in such a situation, experienced staff within the organization could undermine the contribution or opinion of the less experienced staff and ultimately impose their decision on them. As shown in the figure below, the top three most influenced decision-makers in the order of highest ranked are site managers, entrepreneurs, and project managers.This could perhaps be attributed to on-site decision makings by site managers in the construction sector rather than the overall decision-making of entrepreneurs or project managers on the project. The reality here also is that most of the entrepreneurs double as the project manager or site manager. This presents a conflicting issue in answering the questionnaire. Respondents are more likely to select

the title as it applies to their organization. It is therefore possible respondents are talking of the same person under different role or title names.

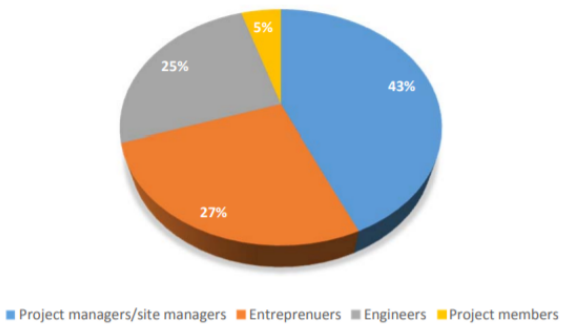


Figure: Most influenced decision-makers in Projects

Data for selected software tools for project decisions presented in the table below shows that the most commonly used software tool, as indicated by respondents, is the Gantt chart. More advanced tools such as the Microsoft project were not being applied. Advanced software is more expensive for these small organizations to usually invest in. The low level of training and skills in project management among respondents means their organizations are less likely to give priority and invest in such expensive management tools where no staff are likely to utilize in their operations for the benefit of the organization.

Which of these tools applies to your projects	Frequency	Rank
PERT	4	4
Microsoft project	0	1
Gantt chart	27	6
Critical path method	4	4
Stage gate process	0	1
Earned Value Measurement	0	1

5.4 RISK CONTROL POLICIES AND COUNTERMEASURES

Control policies and Analysis policies

SHSU considers all electronic information transported over the university network to have the potential to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as such.

While it is not the policy of SHSU to actively monitor internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the university's internet links. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all
applicable federal and state statutes and by SHSU policies.

Audit logging, alarms, and alert functions of operating systems, user accounting, application software, firewalls, and other network perimeter access control systems will be enabled and reviewed annually. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Information Security Officer.

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- Local Area Network (LAN) traffic; protocols, and device inventory
- Operating system security parameters

The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Service desk trouble tickets and telephone call logs
- Network printer logs

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Operating system and software licenses

Attack methods and countermeasures

Any machine learning-based IDS attack has three basic criteria that describe the type of attack it will be, categorizing it into one of eight possible attack classes. It's worth noting that the positive is assumed to be malevolent, while the negative is assumed to be normal. The three distinct classes are listed below, each with two distinct characteristics:

Influence:
Causative attacks have an impact on learning since they have control over the training data (alter training process)
Exploratory assaults produce Denial of Service (DoS) (by exploiting existing flaws), and are frequently accompanied by false positives (rejects good input)

Security Violation:
Integrity assaults harm assets by producing false negatives (accepts malicious input)
Availability attacks result in a denial of service, which is mainly caused by false positives (rejects good input)

Specificity:
Targeted assaults are those that are focused on a specific instance (lets certain input pass)
Indiscriminate attacks include a wide range of scenarios (lets a lot of things pass)

These assaults are then divided into four categories: DoS, Probe, User to Root (U2R), and Root to Local (R2L). These assault kinds are focused on various results, with each attack's goal listed below:

A denial-of-service (DoS) attack attempts to halt traffic flow to and from the target system. The IDS receives an unusual volume of traffic that it cannot handle, and it shuts down to protect itself. This makes it impossible for typical traffic to access a network. An online business might be inundated with online orders on a major sale day, and because the network can't handle all of the requests, it would shut down, preventing paying consumers from making purchases.

A probe or surveillance attack attempts to obtain data from a network. The purpose is to impersonate a thief and steal vital information, such as client personal information or banking information.

U2R is a type of attack that starts with a regular user account and attempts to achieve super-user access to the system or network (root). The attacker attempts to get root privileges/access by exploiting system vulnerabilities.

R2L is a method of gaining local access to a remote machine. An attacker who does not have local access to the system or network attempts to "hack" their way in.

6. STORAGE DISASTER RECOVERY SERVICE TOOLS:

6.1 DATABASE DETAILS

As flash-based solid-state drive (SSD) becomes more prevalent because of the rapid fall in price and the significant increase in capacity, customers expect better data services than traditional disk-based systems. However, the order of magnitude performance provided and new characteristics of flash require a rethinking of data services. However, the tools perform time-consuming jobs, and the methods may negatively affect run-time performance during normal operation even though high-performance SSDs are used. To handle these issues, we use an SSD-assisted backup/recovery scheme for database systems.

6.1.1 DATA BACKUP TECHNIQUES AND RECOVERY TOOLS

Overview of flash-based SSD

The FTL is one of the core engines in flash-based SSDs. In flash memory, any update of the data in a page must be written to a free page due to the out-of-place update nature of the flash memory. To hide this unique characteristic of flash memory from the host, the FTL maps the logical page number (LPN) from the host to the physical page number (PPN) in flash memory. The old page that has the original copy of the data becomes unreachable and obsolete. FTL erases dirty blocks which have obsolete pages and recycles these pages (garbage collection). To offer high performance and reliability, enterprise SSDs are equipped with supercapacitors that protect data on the DRAM buffer from a power outage. This guarantees that any writes sent to the DRAM buffer are successfully written to the flash memory even in the event of a power loss. Such supercapacitors also minimize the overhead caused by a flushing command for ordering and durability.

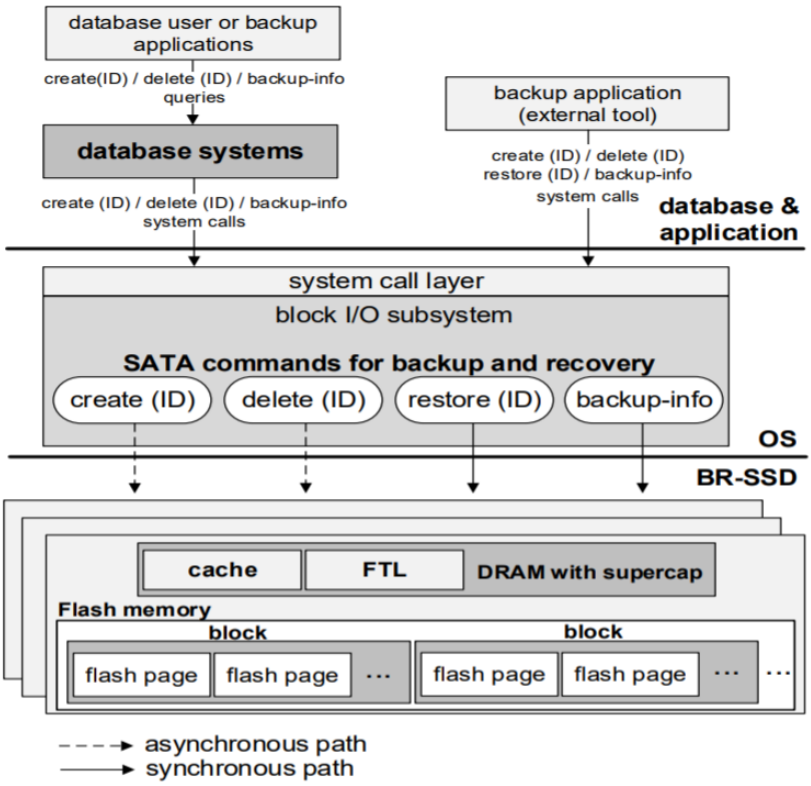


Figure: overall architecture

Backup and recovery operations in BR-SSD

We describe the internal procedure of BR-SSD while processing the create, delete, and restore operations. We add a reference count (refcount) to each block in SSD as the metadata for the operations. The refcount value represents the number of preserved pages in a block for backups. Meanwhile, refcount is decreased by one when the page is dereferenced by a delete operation.

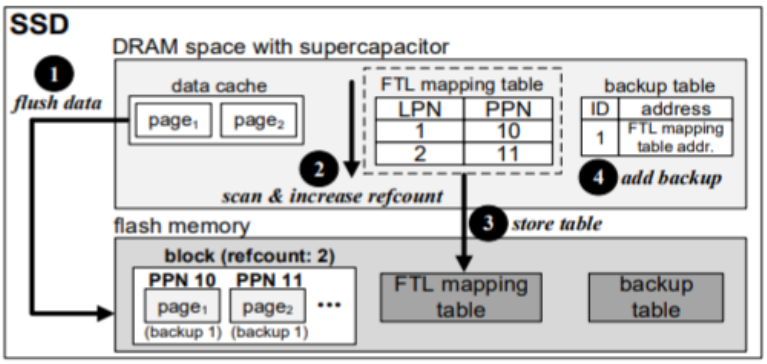


Figure: creating a backup

Create operation: We describe create operation(s) for backup(s) in BR-SSD as shown in the figure above. When a create command is issued from the host, a create operation is performed by BR-SSD in the following steps:

• BR-SSD flushes the current dirty pages from DRAM to persistent flash memory. This operation preserves the pages at a given point.

• BR-SSD scans for all entries in the FTL mapping table while increasing the refcount of blocks corresponding to the entries.
• BR-SSD flushes the FTL mapping table to flash memory in order to save the mapping information for the preserved pages.
• BR-SSD adds the address of the stored FTL mapping table to the backup table.

The figure above illustrates an example of a create operation inside BR-SSD. In this example, there are two pages, such as page 1 (LPN 1) and page 2 (LPN 2) in the data cache, and each page is mapped to PPN 10 and 11, respectively. When the host issues a create command to BR-SSD, the SSD flushes the current data (two pages mapped to PPN 10 and PPN 11) from the data cache (DRAM space) to flash memory. After flushing the data, BR-SSD traverses two entries in the FTL mapping table while increasing refcount to two so that these pages do not get garbage collected. And then, the SSD flushes the FTL mapping table to flash memory. Then, an entry that includes the address for the stored FTL mapping table is added to a backup table which is written into the flash memory asynchronously. The FTL mapping table is the space overhead from the create operation. In our storage device, the size of the FTL mapping table is about 70 MiB. A more detailed explanation of the create operation can be referenced from our previous work.

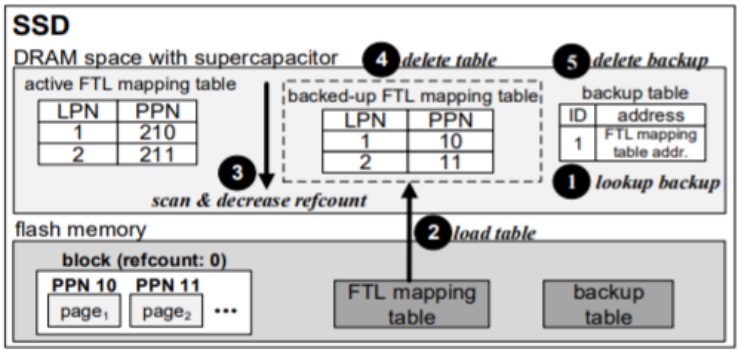


Figure: Deleting a backup

Delete operation: the figure above illustrates an example of a delete operation inside BR-SSD. When the host issues a delete command with a given backup ID to BR-SSD, the SSD searches the entry in the backup table according to the backup ID. If BR-SSD finds the entry in the backup table, the SSD obtains the address of the FTL mapping table to be deleted. Otherwise, BR-SSD returns an error message for this delete command to the host. After BR-SSD obtains the address, the SSD loads the backed-up FTL mapping table from flash memory to DRAM. Then, BR-SSD scans all entries in the backed-up FTL mapping table while decreasing refcount of the block, including the preserved pages to invalidate the pages. In this example, refcount of the block including the two pages is decreased and the pages will be garbage collected since refcount is zero; if the pages are associated with another backup, refcount is not zero. Then, BR-SSD deletes the backed-up FTL mapping table and the entry including the address of the stored FTL mapping table. During the delete operation, BR-SSD does not touch the active FTL mapping table. Consequently, this delete operation allows the backup to be deleted independently from other backups due to the full backup strategy

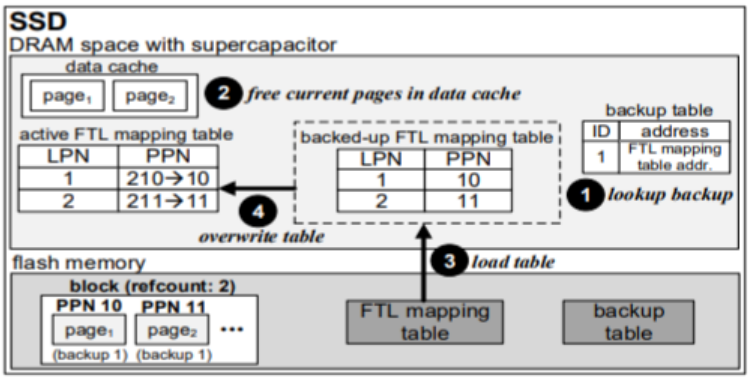


Figure: Restoring a backup

Restore operation: the figure above illustrates an example of a restore operation in BR-SSD. When the host issues a restore command with a given backup ID to BR-SSD, the SSD searches the entry in the backup table according to the backup ID. If BR-SSD finds the entry, the SSD obtains the address of the backed-up FTL mapping table in the backup table. Otherwise, the SSD returns an error message for this restore command to the host. After BR-SSD obtains the address, the SSD frees the current pages in the data cache. And then, BR-SSD loads the FTL mapping table from flash memory to DRAM. Then, BR-SSD overwrites all entries in the backed-up FTL mapping table to those in the active FTL mapping table. In this example, the active FTL mapping table contains page 1 and page 2 mapped to PPN 210 and PPN 211, respectively. During the restore operation, each PPN field of page 1 and page 2 in the active FTL mapping table is overwritten to 10 and 11, respectively. The two pages mapped to PPN 210 and PPN 211 will be garbage collected if the pages are not referenced by any backup. Consequently, this restore operation provides the full backup restoration by replacing all current entries with backed-up entries without data copies.

7. BUSINESS RECOVERY:

7.1 BUSINESS RECOVERY TEAM

For today's businesses, disaster can entail a variety of things. A natural calamity that affects power and infrastructure, or a cyberattack that cripples their network systems, are both possibilities. Whether a natural or man-made disaster strikes, it can jeopardize an organization's capacity to access and use the data and network technologies that enable it to operate. As a result, it's vital that businesses prepare for disaster by putting together a disaster recovery plan and forming a disaster recovery team.

Executive Management
Although senior management may not need to be involved in all parts of disaster recovery planning, they must be present at all meetings about disaster mitigation initiatives because they will be the ones to sign off on budget proposals and broader policies in the end.

IT Administration
Members of the organization's IT department will handle the majority of the more technical components of the disaster recovery plan. They have the best understanding of current network and computer infrastructure requirements and how to assure system availability in the case of a crisis. Any disaster recovery planning process should include senior IT managers who are familiar with the organization's storage and database systems, networking, and applications.

Advisors to Critical Business Units

Although IT workers are familiar with the ins and outs of the company's systems, they may not be aware of how important they are to other departments. The team can more effectively assess downtime tolerance by incorporating members from those departments in the planning phase. Some departments may be able to design workarounds that provide the recovery team more time to get systems back up and operating. As a result, the whole catastrophe recovery budget might be reduced.

Management of Security and Compliance
Data availability and security may be harmed as a result of a disaster, exposing the company to significant legal consequences. Compliance requirements are frequently complicated, and the team must ensure that the methods it implements to mitigate a disaster meet those criteria. This is especially crucial if the company is bound by service level agreements (SLAs) that outline its obligations to its consumers. It's not worth taking chances when it comes to data integrity and security.

7.2 ASSESSMENT OF DAMAGE AND BUSINESS IMPACT

A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs), and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions, and plans.

It is critically important for the survival of your business to identify processes, systems, and operations that are of eminent priority; that is the central focus of the business impact analysis (BIA). Its purpose is to determine how the interruption of your business operations may affect your organization. Potential effects include the loss of data, equipment, and revenue, loss of staff, reputational damage, and other types of business losses. Business impact analysis is an important stage in developing a disaster recovery (DR) plan, the mission of which is to ensure the operation of a company’s infrastructure and applications in case of a major outage.

Risk lurks in all corners of any business: from operational, financial, and strategic risk, to IT and security risk. The potential consequences of those risks include loss of revenue and possible legal action, to application outages, and inability to deliver key customer services. To address these issues, enterprises typically use a range of approaches - from the non-technical (such as business risk assessments) to the highly specialized, such as deploying vulnerability scanners and code inspectors.

First and foremost, organizations must identify the potential risks points within their enterprise networks. The key to this is identifying all firewalls and routers in the network, and then conducting an in-depth examination of each device including all the policies and rules that each device supports. When done manually, this is an extremely time-consuming process of mapping and documenting flows; it can be accelerated dramatically with an automated security management solution.
Once every device’s policies and rules are fully documented and traffic flows mapped, it is then possible to identify the risks that exist within the network and security infrastructure – which will generally speak fall into one of three categories.
The first of these is incorrect device configuration, which occurs when IT teams fail to ensure that each network security device is configured in accordance with vendor guidelines.
Risk is also introduced into the security fabric in instances where it fails to support the compliance and regulatory requirements of the organization, either in terms of the capabilities of the solutions deployed, or the rule sets that must be implemented.

The final risk category is where security is not configured in accordance with industry best practices, such as utilizing good network segmentation.

7.3 PLANNING RECOVERY ACTIVITIES

A network disaster recovery plan is a set of procedures designed to prepare an organization to respond to an interruption of network services during a natural or manmade catastrophe.
Voice, data, internet access, and other network services often share the same network resources. A network disaster recovery (DR) plan ensures that all resources and services that rely on the network are back up and running in the event of an interruption within certain a certain specified time frame.
Such a plan usually includes procedures for recovering an organization's local area networks (LANs), wide area networks (WANs), and wireless networks. It may cover network applications and services, servers, computers, and other devices, along with the data at issue.
Network services are critical to ensuring uninterrupted internal and external communication and data sharing within an organization. A network infrastructure can be disrupted by any number of disasters, including fire, flood, earthquake, hurricane, carrier issues, hardware or software malfunction or failure, human error, and cybersecurity incidents and attacks.
Any interruption of network services can affect an organization's ability to access, collect or use data and communicate with staff, partners, and customers. Interruptions put business continuity (BC) and data at risk and can result in huge customer service and public relations problems. A contingency plan for dealing with any sort of network interruption is vital to an organization's survival.
Some important caveats to consider when preparing a network disaster recovery plan include the following:

- Use business continuity standards. There are nearly two dozen BC/DR standards and they are a useful place to start when creating a contingency plan.
- Determine recovery objectives. Before starting on a plan, the organization must determine its recovery time objective (RTO) and recovery point objective (RPO) for each key service and data type. RTO is the time an organization has to make a function or service available following an interruption. RPO determines the acceptable age of files that an organization can recover from its backup storage to successfully resume operations after a network outage. RPO will vary for each type of data.
- Stick to the basics. A network DR plan should reflect the complexity of the network itself and should include only the information needed to respond to and recover from specific network-related incidents.
- Test and update regularly. Once complete, a network DR plan should be tested at least twice a year and more often if the network configuration changes. It should be reviewed regularly to ensure it reflects changes to the network, staff, potential threats, as well as the organization's business objectives.
- Stay flexible. No one approach to creating a network disaster recovery plan will work for every organization. Check out different types of plan templates and consider whether specialized network DR software or services might be useful.

Network disaster recovery planning provides guidelines for restoring network services and normal operations following a disaster. The plan outlines resources needed to perform network recovery procedures, such as equipment suppliers and information on data storage.
A network disaster recovery plan also identifies specific issues or threats related to an organization's network operations. These can include interruptions caused by loss of voice or data connectivity as a result of network provider problems or disasters caused by nature or human activities.
Like any other disaster recovery plan, this one should include information about contacting key staff members in case an emergency occurs after business hours, such as late at night or on weekends.
Some specific sections that should be included in a network disaster recovery plan include the following:

- Emergency contacts and actions. List the IT network emergency team members and their contact information at the front of the plan for fast access. A list of initial emergency response actions should also be up front.
- Purpose and scope. Outline the purpose of the plan and its scope, along with assumptions, team descriptions, and other background information.
- Instructions for activating the plan. Describe the circumstances under which the contingency plan will be activated, including outage time frames, who declares a disaster, who is contacted and all communication procedures to be used.
- Policy information. Include any relevant IT BC/DR policies, such as data backup policies.
- Emergency management procedures. Provide step-by-step procedures on how networks will be reconfigured and data accessed, what outside help might be needed and how staff will be accommodated for each different kind of potential disaster.
- Checklists and diagrams. Include checklists that prioritize hardware and software restoration and network flow diagrams that make it easy for technical support staff to quickly access the information they may need.
- Data collection. Describe the information that might be needed before officially declaring a network disruption, including network performance data and staff and first responder reports.
- Disaster declaration. Identify actions to take once the network emergency team determines it's necessary to declare a network disaster, including how the decision is communicated, who is contacted, and what additional damage assessments are needed.
- Disaster recovery. Provide instructions on restoring network operations, connectivity, devices, and related activities.
- Appendices. Provide names and contact information of IT and non-IT emergency teams, as well as information on internet service providers and other key vendors, alternate network configuration data, forms that emergency response teams will need, and other relevant information.

The network disaster recovery plan doesn't exist in a vacuum, but rather is part of an organization's broader IT disaster recovery plan. Data backup is a key part of both the overall IT plan and the network plan, and information on an organization's backup policies and procedures should be included in DR planning.

Options for data backup range from having dual data centers in different locations, each of which can handle all of an organization's data processing needs. The data centers run in parallel and synchronize or mirror data between them. Operations can be shifted from one data center to another in an emergency. Dual data centers are not an option open to every organization. Leased colocation facilities are an alternative.

Other options include backing up data to dedicated backup disk appliances with management software that's either integrated in the appliance or run on a separate server. The backup software runs the data copying process and enforces backup policies for an organization. A backup appliance is an effective option as long as it's located where it won't be hit by the same disasters as an organization's original data.

Cloud backup and cloud-based disaster recovery are other options, either in-house or through a cloud data backup service. Cloud storage as a service provides low-cost, scalable capacity and eliminates the need to buy and maintain backup hardware. However, cloud providers fees vary depending on the types of services and accessibility required. And cloud services can require organizations to encrypt data and take other steps to secure the information they're sending to the cloud.

Cloud-to-cloud data backup is an emerging alternative. It uses software as a service (SaaS) platforms, such as Salesforce and Microsoft Office 365, to protect data. This data often exists only in the cloud. Backed up SaaS data is copied to another cloud from where it can be restored in an emergency.

7.4 COMMUNICATION SYSTEMS

You'll be dead in the water and losing clients if you don't have a way to continue consumer engagement during a calamity. Many businesses have basic disaster recovery strategies in place. Unfortunately, many of those same businesses do not include telecom in their disaster recovery plans.

Why is it necessary to use hosted VoIP?
There are a variety of advantages to using VoIP. Of course, the biggest benefit is that you will always be able to keep communication lines up, even in the event of a natural disaster. All that is necessary is access to the Internet. As a result, if your office loses Internet access for any reason, all you have to do is go to another location with an Internet connection, whether it's your home or somewhere else. This will ensure that your business continues to operate. You'll be able to easily reach your staff, ensuring their safety while also reducing operational disturbance by keeping lines of communication open.

In the event of an emergency, you'll also have a sound backup plan. You may lose data if there is a power outage or if your Internet goes down for any reason. If there is a data breach, this is also true. However, because hosted VoIP is cloud-based, recovering from such situations is much easier. Early detection tools are also provided by real-time monitoring capabilities. This ensures that your plan can be implemented before your operations are seriously harmed. With VoIP, tracking and monitoring suspicious activities is much easier. You'll be able to see a breach right away.

7.5 HUMAN RESOURCES

The most important factors to consider when creating an HR business continuity strategy
There are two major factors to consider while creating an HR business continuity plan: 2) talent and 1) furniture, fixtures, and equipment (commonly known as FF&E). Businesses are generally extremely excellent at designing plans to safeguard their FF&E; the difficult part is putting the talent component of the strategy together. And here is where human resources' input is crucial. Here are some things to think about

1. Include human resources in the development of the plan and as a member of the response team. This is also a moment when job descriptions are less crucial than having people who are capable and willing to complete the work. Being a member of any form of emergency response team necessitates flexibility and dedication. Anyone requested to take on this responsibility will need to buy-in from the organization.

2. Examine current emergency communications best practices within your organization. There's no need to start again with your plans. Some of the organization's current communication tactics for hurricanes, snowstorms, flooding, and other disasters might be applied here as well. A critical examination of what currently works and is deemed a true best practice is required.

3. Establish a central location for staff to get information. One of the things that every employee is seeking for during any type of disaster is information. HR case management software can be used to manage employee questions and streamline the flow of information. Employees can self-serve through a knowledge portal, and HR can route-specific situations to the appropriate professionals more quickly.

4. Keep HR technology up to date. Keeping the HR department operational is critical to providing employees with timely information. HR departments, for example, were considered important corporate operations under COVID-19. Even if HR teams work from home, digital file management ensures that files are safe and available from any location, allowing HR to keep employees informed.

7.6 IT SYSTEMS SOFTWARE ARCHITECTURE RECOVERY

Based on the research gaps identified in previous techniques, we have provided an architecture for securing systems towards network-based attacks. Our proposed network intrusion detection system is an architecture that presents an autoencoder based anomaly detection model for intrusion detection, we use the NSL-KDD dataset, this dataset is a benchmark for machine learning-based intrusion detection, however, it suffers from several inefficiencies such as class imbalance, where for instance in the NSL-KDD training dataset only 0.04% of the samples belong to the u2r attack type making it severely underrepresented, the case is similar for the r2l and probe attack types whereas the majority of attack records are representing the DDOS attack type, this fact made it difficult for classifiers to detect these underrepresented types resulting in poor accuracy. Another issue is that this dataset is unrealistic, in reality, most traffic in a network is benign and only a small percentage might be malicious, while in the NSL-KDD training set, for example, attack samples compose 80% of the entire dataset which makes the models trained using this dataset ineffective in real-life situations. Our autoencoder-based approach attempts to overcome these problems.

The 37 attack types available in the dataset can be clustered into four general attack types

- Denial of service attacks
- Remote to Local attacks
- User to Root
- Probe attacks

Our model will perform binary classification of the data to two classes indicating whether the traffic is normal or an Attack, however, we will use the four attack types to analyze the results and calculate performance metrics for each general attack type.
The next section replaces the current outcome field with a Class field that has one of the following values:

- Normal
- Dos
- R2L
- U2R
- Probe

In order to avoid the imbalance of the samples representing each attack type in the training data, and to avoid the model's inability to learn about new attack types by observing existing ones, we present an approach that utilizes autoencoders and reconstruction error to detect anomalies.
In this approach we implemented a sparse autoencoder with dropout on the inputs, it consists of an input layer of 122 neurons due to the fact that the number of features for each sample is 122 followed by a dropout layer and a hidden layer of 8 neuron units so the hidden representation of the autoencoder has a compression ratio of 122/8 forcing it to learn interesting patterns and relations between the features, finally, there is an output layer of 122 units, the activation of both the hidden layer and the output layer is the relu function.
The autoencoder was trained to reconstruct its input, in other words, it learns the identity function, the model was trained using only the samples labeled "Normal" in the training dataset allowing it to capture the nature of normal behavior, this was accomplished by training the model to minimize the mean squared error between its output and its input.
The regularization constraints enforced over the autoencoder prevent it from simply copying the input to the output and overfitting the data, furthermore, the dropout presented on the inputs makes the autoencoder a special case of a denoising autoencoder, this kind of autoencoders is trained to reconstruct the input from a distorted corrupted version of itself, forcing the autoencoder to learn even more properties of the data.

The model is trained for 10 epochs using an Adam optimizer with a batch size of 100, furthermore, we held out 10% of the normal training samples to validate the model.

The model performs anomaly detection by calculating the reconstruction error of samples, since the model was trained using normal data samples only the reconstruction error of samples that represent attacks should be relatively high compared to the reconstruction error of normal data samples, this intuition allows us to detect attacks by setting a threshold for the reconstruction error, if a data sample has a reconstruction error higher than the preset threshold then the sample is classified as an attack, otherwise, it's classified as normal traffic.

For the choice of a threshold two values can be helpful for guiding the process, the model loss over the training data and over the validation data, we found by experiment that a choice around these values produces acceptable results, for our experiments we use the model loss over the training data as a threshold.

Due to the nature of this approach, it can only be used for 2-Class classification as it is purely for anomaly detection and not classification.

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

BCI 3002: Disaster Recovery and Business Continuity Management (DRBCM)

Slot: A1+TA1

Research Paper

TITLE: PREVENTION OF ATTACKS USING ONE CLASS CLASSIFICATION AND AUTOENCODERS

29th November 2021

Team Leader:
Rohan Allen 18BCI0247

Team Members:
Rakshith Sachdev 18BCI0109
Harshita Pundir 18BCI0192

ABSTRACT

In this paper, we represent how one-class classifiers are prepared to utilize generous information to recognize ordinary and dangerous traffic redirected to an endpoint device. In this venture, the framework is prepared to utilize unsupervised / one-class-based demonstrating approaches by which the framework would comprehend the issues that we would confront day by day, and the preparation will be useful for what's to come. After the preparation of the framework, the framework can be utilized in reality to confront ongoing, new difficulties and by gaining from the past experiences it can develop as indicated by the users' issues, weaknesses, dangers, and conditions

KEYWORDS

Autoencoders, feature generation, machine Learning, malware detection, malware profiling, network protection, one-class classification,

INTRODUCTION

With today’s day and age rapidly becoming digital, the network and endpoint devices become a target for attacks and exploitation; thus, the systems have long been associated with issues related to security. Therefore, making systems secure and safe is of extreme importance. As per the 2020 Unit 42 Threat Report, practically all traffic is decoded, implying that the majority of classified and indiIntrusion detection using deep sparse auto-encoder and self-taught learning, Qureshi by A. S., visual user information in the network is highly powerless against cyber attacks. Network security is utilized to delay unintentional harm which can be done to the network's private information, its users, or its devices. The main aim of network security is to secure the network running and for every single authentic client.

The objective of this project is to use machine learning to teach our system to distinguish between malicious network traffic, which could contain a virus or malware, and regular network data. The model has also been taught to detect and avoid fake data and the deployment of any specific software while there is a threat of an attack, which results in dramatically reducing the financial stress on an organization and prevents tarnishing their reputation. The major goal is to offer the most accurate findings possible by utilizing methods such as unsupervised learning/one-class-based modeling, thereby lowering processing time substantially.

In this model, we are using one-class classifications and autoencoders so that the system can detect bad traffic more accurately. With the help of this model, we can predict false data, and therefore, we can prevent the installation of software at the time of any risks to decrease the cost.

LITERATURE SURVEY

TITLE, AUTHOR, AND JOURNAL	OBJECTIVE	METHODOLOGY USED	LIMITATION
Khan, A., Shamim, N., & Durad, M. H. (2019) Neural Computing and Applications (2019). [1]	This paper gives the idea of self-education figuring out how to prepare the deep neural network for network intrusion detection.	In the proposed strategy, a Self Taught based Transfer Learning(DST-TL) is used to remove the highlights from the NSL-KDD dataset a relapse-related pre-prepared network is utilized.	This system cannot classify the different types of attacks as deep neural networks are not used.
A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems by Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) 2019 11th International Conference on Knowledge and Systems Engineering (KSE). IEEE, 2019. [2]	This paper provides the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder(SAE) to lessen the limitations in handling the datasets.	In the proposed method, the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder is used to detect the anomalies occurring in the network. With the help of this method, datasets can also be handled properly.	It failed to extend these works by using better clustering algorithms and other metrics to find a suitable number of clusters in the data.
A Modular Multiple Classifier System for the Detection of Intrusions in Computer Networks Giorgio Giacinto, Fabio Roli, Luca Didaci Department of Electrical and Electronic Engineering, University of Cagliari, Italy. [3]	This paper provides a strategy to use Intrusion Detection Systems (IDS) and pattern recognition to increase the level of security on computer networks. The authors later discuss and evaluate the effectiveness of the IDS on the security of the network.	Utilizing IDS and example acknowledgment ways to deal with network intrusion detection dependent on the combination of numerous classifiers. Specifically, the author centers around Modular Multiple Classifier engineering plans where every	This study presents an extensive report on how IDS and pattern recognition can be used to provide higher levels of network security. The paper includes a descriptive report on how the authors' used methods like machine learning in their implementation and

		module in the design can identify intrusions against the administrations offered by the secured network.	design and also compared different training sets on the data to conclude which model is most effective. Although this paper is detailed, our methodology of achieving a system that can differentiate between good and bad networks containing viruses and malware includes methods and techniques using One-Class Classification and Auto Encoders.
A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) In 2019 11th International Conference on Knowledge and Systems Engineering (KSE) (pp. 1-5). IEEE. [4]	A detailed examination and investigation of different AI procedures have been completed to discover the reason for issues related to different AI strategies in identifying intrusive exercises.	AI methods have been examined and looked at as far as their recognition ability for distinguishing the different classes of assaults. Limits related to every classification of them are additionally talked about. Different data mining apparatuses for AI have additionally been remembered for the paper.	Existing literature is described which is based on similar techniques with most of the popular datasets as on date to generalize our observations. All the techniques have not been implemented to evaluate the performance to ensure that results are reproducible.

A novel statistical analysis and autoencoder-driven intelligent intrusion detection approach. Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). Neurocomputing, 387, 51-62. [5]	Statistical examination and autoencoder (AE) driven insightful intrusion detection (IDS) framework is acquainted with recognizing and alleviating the dangers of programmers growing much more complex and risky malware assaults that make intrusion detection a troublesome assignment.	Initially, the NSLKDD dataset is cleaned from anomalies and the min-max standardization procedure is utilized to scale data inside the range 0 and 1. Subsequently, the one-hot-encoding is applied to change over symbolic (or categorized) features into numeric quantities. At that point, the 38 numeric attributes are investigated statistically to choose the most associated features. At last, shallow (MLP, L-SVM, Q-SVM, LDA, QDA) and deep (AE, LSTM) networks are created to quantify the detection execution both in parallel and multi-classification situations.	The advancement of more precise deep architectures that can oversee continuous real-time data streams like NSL-KDD examples to recognize malicious attacks progressively can build its proficiency. Also, to misuse long-term learning, quicker choice models along with decreased computational complexity for constant needs to execute in this system.

J. K. Chahal, V. Gandhi, P. Kaushal, K. R. Ramkumar, A. Kaur and S. Mittal, "KAS-IDS: A Machine Learning based Intrusion Detection System," *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, 2021.[6]	Regrettably, the majority of commercial IDSs are based on abuse and are only designed to detect known threats. These require frequent signature updates and have a limited capacity for detecting new assaults. As a result, this study proposes an anomaly-based IDS as a viable solution to this challenge.	KAS-IDS, or K-Means and Adaptive SVM-based Intrusion Detection System, is the approach proposed in this study. K-Means were used in the first stage to creating data clusters, and adaptive SVM was used in the second step to classify the data.	As part of the current technique, the data is split into two categories: normal and abnormal data and correct findings are obtained using the NSL-KDD dataset, which can also be used for real-time traffic analysis. Apart from that, the intelligent agents of clustering and classification algorithms can improve their performance in real-time traffic analysis.
G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021[7].	The main purpose of this project is to compare and assess the effectiveness of neural network models on a data set.	To identify intrusion rates, the suggested application uses the SVM (Support Vector Machine) and ANN (Artificial Neural Networks) algorithms. Each algorithm is used to determine if the data being requested is allowed or includes any irregularities. These techniques employed feature selection algorithms based on correlation and Chi-Squared to decrease the dataset by removing unnecessary data.	Another dataset with a larger number of characteristics might be used to improve this research. Because ANN provides greater accuracy but slower calculations, we can apply alternative efficient algorithms in the future that may provide greater accuracy while also computing faster, allowing it to be employed in real-time applications.

D. Xuan, H. Hu, B. Wang and B. Liu, "Intrusion Detection System Based on RF-SVM Model Optimized with Feature Selection," 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 2021.[8]	The goal of this research is to improve network intrusion detection using machine learning. The two-stage IDS suggested in this research is based on machine learning algorithms RF and SVM that are tuned with the Feature Ranking CFS.	In this research, they present a two-stage IDS based on machine learning models RF and SVM tuned with the CFS method, and they tested it on NSL-KDD benchmark datasets, contrasting it to the RF and SVM modeling.	We plan to develop the IDS in the future with the goal of increasing the detection precision of low-frequency assaults, which is a common difficulty in IDS. Furthermore, the capacity of an IDS to identify unknown forms of threats is taken into account. We'd want to increase the accuracy of detecting unknown forms of assaults.
A. Aljohani and A. Bushnag, "An Intrusion Detection System Model in a Local Area Network using Different Machine Learning Classifiers," *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 2021.[9]	The article presents a security control for an IDS that is used to identify known and unknown attacks in order to avoid security concerns in LANs.	The suggested system uses Neural Network and Support Vector Machine (SVM) models for intrusion detection to avoid security risks in a Local Area Network (LAN). The KDD99 dataset is used to test the suggested method. The KDD99 is an anomaly-based detection benchmark. This method detects assaults quickly and effectively.	In future research, the KDD99 dataset may be used to classify threat categories to see which machine learning classifier performs better.

H. Elbahadır and E. Erdem, "Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks," 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021.[10]	An intrusion detection system (IDS) is modeled in this work to assure WSN security. Because signature, misuse, and anomaly-based intrusion detection approaches are insufficient to offer security on their own, a hybrid model is presented in which these methods are combined.	Anomaly criteria were created for attack detection, and the BayesNet, J48, and Random Forest machine learning algorithms were employed to categorize normal and anomalous traffic in the hybrid model.	Application of alternative efficient algorithms in the future that may provide greater accuracy while also computing faster, allowing it to be employed in real-time applications.
S. T. Zargar, J. Joshi, and D. Tipper, ‘‘A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,’’ IEEECommun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, Mar. 2013. [11]	This paper describes the developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during, and after an actual attack.	The paper provides the knowledge required about the attacks as this project works on the prevention of attacks. It stimulates our research into understanding how the attacks occur which in turn helps with solutions to prevent them.	Existing literature is described which is based on similar techniques with most of the popular datasets as on date to generalize our observations. All the techniques have not been implemented to evaluate the performance to ensure that results are reproducible.
V. Balamurugan and R. Saravanan, ‘‘Enhanced intrusion detection and prevention system on cloud environment using hybrid classification andOTS generation,’’ Cluster Comput., vol. 22, pp. 1–13, Nov. 2017. [12]	The proposed system in this paper is directed on intrusion detection systems and it uses cloudlet controller, trust authority, and virtual machine management in cloud environments.	The proposed classifier in this paper effectively detects the attackers which are experimentally proved by comparing with existing classification models which provide a very good insight.	Application of alternative efficient algorithms in the future that may provide greater accuracy while also computing faster, allowing it to be employed in real-time applications.

J. Yan, D. Jin, C. W. Lee, and P. Liu, ‘‘A comparative study of off-line deep learning based network intrusion detection,’’ in Proc. 10th Int. Conf.Ubiquitous Future Netw. (ICUFN), Jul. 2018, pp. 299–304. [13]	It intends to answer some of the research questions specified in and random forest classifiers, which are shallow. The authors indicated that their approach could reduce the SVM’s training and testing times in both binary and multiclass classifications and improve the prediction accuracy of the SVM.	They used ISCX 2012 dataset and achieved ten features from it by using an auto-encoder and feeding it to the SVM for its training. The authors indicated the benefits of their method regarding metrics like Kappa statistics, detection rate, accuracy, and FPR.	It is only able to conduct the binary classification and cannot handle the multiclass attack traffics.
M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, ‘‘Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,’’ IEEE Access, vol. 6, pp. 52843–52856, 2018. [14]	This paper proposes a scheme that uses the self-taught learning framework for the learning of features and reduction of dimension. This IDS model benefits from a sparse auto-encoder for unsupervised reconstructing a new feature representation.	The authors indicated that their approach could reduce the SVM’s training and testing times in both binary and multiclass classificationsand improves the prediction accuracy of the SVM.	The efficiency of this approach in binary and multiclass classifications is evaluated against the naive random forest classifiers, which are shallow.
B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, ‘‘Deep learning for classification of malware system call sequences,’’ in Proc. Australas.Joint Conf. Artif. Intell., 2016, pp. 137–149. [15]	The authors used recurrent and convolutional network layers to construct an ANN model and by using one recurrent layer and two convolutional layers, they detect various malware.	This model achieves good accuracy for multiclass intrusion detection with both datasets. Also, FAR and the execution time of this scheme are low.	This scheme should be further evaluated on the other imbalanced datasets,in which some of their attack classes have much fewer data records than others, to verify the detection rate of the minority class security attacks.

Khan et. al.[1] in this paper gives the idea of self-education figuring out how to prepare the profound neural network for network intrusion detection. In the proposed strategy, a Self Taught based Transfer Learning(DST-TL) is used to remove the highlights from the NSL-KDD dataset a relapse-related pre-prepared network is utilized. The limit of this system cannot classify the different types of attacks as deep neural networks are not used. Bui et. al.[2] in this paper provides the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder(SAE) to lessen the limitations in handling the datasets. In the proposed method, the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder is used to detect the anomalies occurring in the network. With the help of this method, datasets can also be handled properly. The limit of the system is that it failed to extend these works by using better clustering algorithms and other metrics to find a suitable number of clusters in the data.

Giacinto et. al. [3] in this paper provide a strategy to use Intrusion Detection Systems (IDS) and pattern recognition to increase the level of security on computer networks. The authors later discuss and evaluate the effectiveness of the IDS on the security of the network. Utilizing IDS and example acknowledgment ways to deal with network intrusion detection dependent on the combination of numerous classifiers. Specifically, the author centers around Modular Multiple Classifier engineering plans where every module in the design can identify intrusions against the administrations offered by the secured network. The limit of this study presents an extensive report on how IDS and pattern recognition can be used to provide higher levels of network security. The paper includes a descriptive report on how the authors used methods like machine learning in their implementation and design and also compared different training sets on the data to conclude which model is most effective. Although this paper is detailed, our methodology of achieving a system that can differentiate between good and bad networks containing viruses and malware includes methods and techniques using One-Class Classification and Auto Encoders. Bui et. al. [4]do a detailed examination and investigation of different AI procedures have been completed to discover the reason for issues related to different AI strategies in identifying intrusive exercises.AI methods have been examined and looked at as far as their recognition ability for distinguishing the different classes of assaults. Limits related to every classification of them are additionally talked about. Different data mining apparatuses for AI have additionally been remembered for the paper. The limit of the existing literature is described which is based on similar techniques with most of the popular datasets as on date to generalize our observations. All the techniques have not been implemented to evaluate the performance to ensure that results are reproducible

Ieracitano et. al. [5] statistical examination and autoencoder (AE) driven insightful intrusion detection (IDS) framework is acquainted with recognizing and alleviating the dangers of programmers growing much more complex and risky malware assaults that make intrusion detection a troublesome assignment. Initially, the NSLKDD dataset is cleaned from anomalies and the min-max standardization procedure is utilized to scale data inside the range 0 and 1. Subsequently, the one-hot-encoding is applied to change over symbolic (or categorized) features into numeric quantities. At that point, the 38 numeric attributes are investigated statistically to choose the most associated features. At last, shallow (MLP, L-SVM, Q-SVM, LDA, QDA) and deep (AE, LSTM) networks are created to quantify the detection execution both in parallel and multi-classification situations. The limit of the advancement of more precise deep architectures

that can oversee continuous real-time data streams like NSL-KDD examples to recognize malicious attacks progressively can build its proficiency. Also, to misuse long-term learning, quicker choice models along with decreased computational complexity for constant needs to execute in this system. Chahal et.al. [6] talk about machine learning-based IDS for anomaly detection. Intrusion detection systems (IDS) serve an important role in detecting intrusions. This paper introduces a hybrid strategy that combines K-Means and Adaptive SVM, concluding that the combined results are superior to the individual results of K-Means and Adaptive SVM. Furthermore, when compared to other methodologies, this algorithm is quite accurate.The hybrid technology correctly distinguishes between normal and attack data, and this approach is 99.54 percent more accurate than solo techniques. As a result, employing this approach in real-time results in an extremely high detection rate of assaults. Furthermore, this method is easy and effective, especially when it comes to lowering the false-positive ratio and increasing the false negative ratio.

Yedukondalu et.al. [7] To identify intrusion rates, the suggested application uses the SVM (Support Vector Machine) and ANN (Artificial Neural Networks) algorithms. Each algorithm is used to determine if the data being requested is allowed or includes any irregularities. While the IDS examines the requested data, if it detects any malicious material, the request is dropped. These techniques employed feature selection algorithms based on correlation and Chi-Squared to decrease the dataset by removing unnecessary data. The preprocessed dataset is trained and evaluated with the models to generate notable findings, which improves prediction accuracy. The experiment was conducted using the NSL KDD dataset. Finally, the SVM algorithm obtained a 48 percent accuracy, while the ANN method achieved a 97 percent accuracy. On this dataset, the ANN model performs better than the SVM. Xuan et.al. [8] IDS is a good way to cope with the ever-changing nature of network attacks. In this research, we present a two-stage IDS based on machine learning models RF and SVM optimized with the CFS method, and we tested it on NSL-KDD benchmark datasets, comparing it to the RF and SVM models. The following is a summary of the key findings: (1) Our two-stage IDS outperformed RF and SVM, increasing Precision by 4.31 percent, Recall by 3.39 percent, and F1-measure by 5.56 percent to 11.08 percent; (2) the feature selection algorithm CFS, which we used in this paper, improved accuracy by 1.50 percent while reducing the time by 8.07 percent; and (3) our approach reduced Test Set prediction time by 93.84 percent compared to SVM.

Aljohani et.al. [9] The suggested system uses Neural Network and Support Vector Machine (SVM) models for intrusion detection to avoid security risks in a Local Area Network (LAN). The KDD99 dataset is used to test the suggested method. The KDD99 is an anomaly-based detection benchmark. This method detects assaults quickly and effectively. A comparison of the SVM and Neural Network models' performance is carried out. In terms of classification accuracy, the findings demonstrate that the Neural Network outperformed all SVM kernel models. The SVM linear kernel outperforms the SVM Gaussian kernel by a small margin, and the SVM polynomial kernel by a large margin. Elbahadır et.al. [10] An intrusion detection system (IDS) is modeled in this work to assure WSN security. Because signature, misuse, and anomaly-based intrusion detection approaches are insufficient to offer security on their own, a hybrid model is presented in which these methods are combined. Anomaly criteria were created for attack detection, and the BayesNet, J48, and Random Forest machine learning algorithms were employed to categorize normal and anomalous traffic in the hybrid model. The findings

revealed that the generated model has a high level of accuracy and a low percentage of false alarms.

Zargar et.al. [11] This paper describes the developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during, and after an actual attack. The paper provides the knowledge required about the attacks as this project works on the prevention of attacks. It stimulates our research into understanding how the attacks occur which in turn helps with solutions to prevent them. Balamurugan et.al. [12] The proposed system in this paper is directed on intrusion detection systems and it uses cloudlet controller, trust authority, and virtual machine management in cloud environments. The proposed classifier in this paper effectively detects the attackers which are experimentally proved by comparing with existing classification models which provide a very good insight.

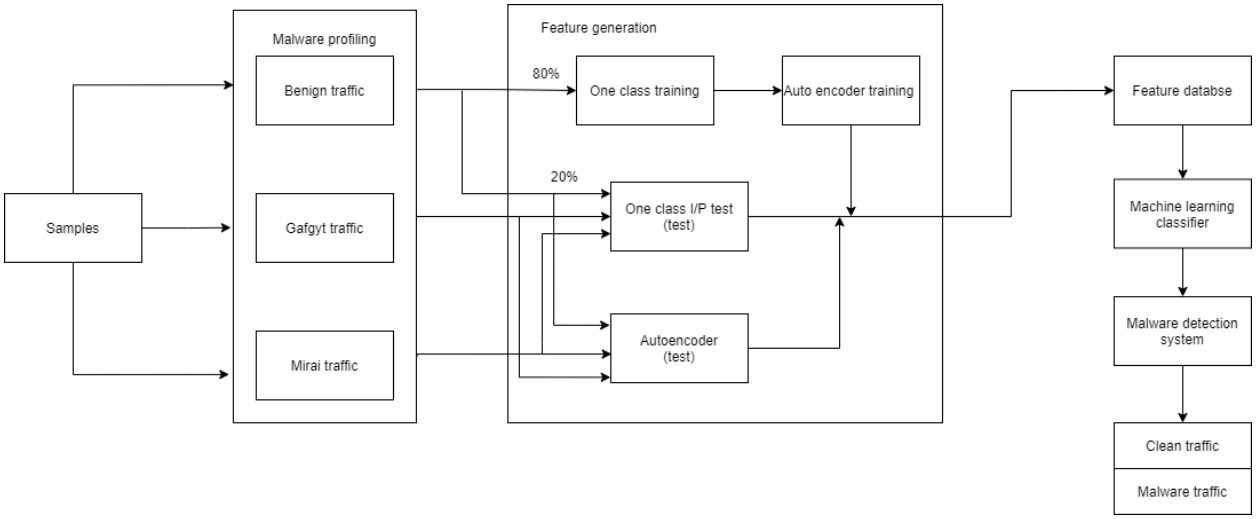
Yan et.al. [13] intends to answer some of the research questions specified in and random forest classifiers, which are shallow. The authors indicated that their approach could reduce the SVM's training and testing times in both binary and multiclass classifications and improve the prediction accuracy of the SVM. They used ISCX 2012 dataset and achieved ten features from it by using an auto-encoder and feeding it to the SVM for its training. The authors indicated the benefits of their method regarding metrics like Kappa statistics, detection rate, accuracy, and FPR. Al-Qatf et.al. [14] This paper proposes a scheme that uses the self-taught learning framework for the learning of features and reduction of dimension. This IDS model benefits from a sparse auto-encoder for unsupervised reconstructing a new feature representation. The authors indicated that their approach could reduce the SVM's training and testing times in both binary and multiclass classificationsand improve the prediction accuracy of the SVM.

Kolosnjaji et.al. [15] The authors used recurrent and convolutional network layers to construct an ANN model and by using one recurrent layer and two convolutional layers, they detect various malware. This model achieves good accuracy for multiclass intrusion detection with both datasets. Also, FAR and the execution time of this scheme are low.

METHODOLOGY

ONE CLASS SVM: One-class SVM is an unsupervised algorithm that learns a decision work for curiosity identification: ordering new information as comparative or diverse to the preparation set. One-class classification algorithms are often used for binary classification tasks with a severely skewed class distribution. These techniques are used to fit on the input examples from the huge class within the training dataset, then evaluated on the remaining test dataset. Albeit not designed for these types of problems, one-class classification methods are frequently successful for unbalanced classification datasets with no or few instances of the minority class, or datasets with no cohesive structure to distinguish the classes that a supervised algorithm would learn. The SVM algorithm, which was originally designed for classification tasks, is frequently employed for one-class classification.

AUTOENCODERS: An autoencoder neural network is a type of unsupervised machine learning technique that uses backpropagation to adjust the target values to the inputs. Autoencoders have a habit of condensing the dimensions of our inputs into a more compact representation. If the first data is required, the condensed data will be used to recreate it. The purpose of an autoencoder is to train the model to ignore signal noise in order to discover a symbol for a set of knowledge, generally to reduce dimensions. They work by condensing the input into a latent-space description and then reconstructing the outcome from there. We'll visualize our findings and results as part of the analysis once both of these models have been implemented and trained, and we'll try and compare the trained models to see which one gives an exact result.



There are three different types of datasets available as input: innocuous traffic (40,395 records), Mirai traffic (652,100 records), and Gafgyt traffic (316,650 records). Benign traffic is clean data flow, whereas Gafgyt and Mirai traffic both contain harmful data, resulting in malware traffic. Each record in the dataset has 115 attributes that were generated by the dataset's publishers using the raw characteristics of network traffic. Because both Gafgyt and Mirai traffic is generated from attack activity, they are combined to create the malicious data (968,750 records).

For training the model, 80 percent of the benign traffic data is fed into the one-class classifier. This means that the model was trained using 32,316 data, and the model's performance was evaluated with (40,395 – 32,316) + (652,100 + 316,650) = 976,829 records.

This is also further given as input for the training of the autoencoder model. The rest 20% of the benign traffic data is sent to the testing phase of both the one-class classifier and autoencoder model. This is also used as an input for the autoencoder model's training. The remaining 20% of the benign traffic data is supplied to the one-class classifier and autoencoder models for testing.

The Gafgyt and Mirai traffic data, which contains harmful data, are combined with 20% of the benign traffic data to see if the one-class classifier and autoencoder models can help sort traffic into clean and malware traffic.

Data is pre-processed in order to increase the quality of the datasets involved. Because there are various datasets to consider, functions are built to ensure that they are loaded and entered into the needed model.

Getting examples of cases with good traffic which displays benign behavior is simpler and easier to get in comparison with malware traffic that displays malicious behavior. This can be due to the fact that obtaining malware traffic can come at a cost or in some cases, impractical like the days with no attacks thus containing only good traffic. Other explanations regarding this could be on the basis of privacy, law, and ethics. But, despite all this, it can be easily convinced that corrupted traffic data can be used first to build models like the two-class classifier. But it cannot be assured that all scenarios involving bad traffic data can be replicated. This issue can be addressed using the unsupervised one-class classifier methodology approach here.

So, in this project, the training model is created only using benign instances, and this trained model is then implemented to detect any unknown/new cases of traffic using machine-learning and other statistical methods. If the data targeted shows considerable diversion according to predetermined calculations, it will be labeled as out-of-class. Thus, one-class classifiers that may belong to different families are examined here under the criterion of performance. One-Class Support Vector Machine from the conventional ML family and Autoencoder from the deep learning family are the two one-class classifiers and their related families illustrated here. In this case, we're investigating how benign occurrences vary from corrupted occurrences in terms of structure. The Autoencoder model is built on the basis of this base composition.

Through training sets comprising only examples of that class, one-class classifiers may distinguish instances of a given class from all other instances. This is a benign class that is being explored. There are various types of one-class classifiers that examine opposing examples to refine the categorization limit.

Other purposes that a one-class classifier can fulfill are in cases of binary and imbalanced classification datasets. In the scenarios where binary classification is to be done but the majority of the dataset overpowers the minority, the training set is modeled based on the majority category of data, before being jointly evaluated in the testing phase. Because one-class classifiers are not built for cases involving unbalanced categorization datasets where the minority may be non-existent or not evident enough, supervised machine learning approaches will need to be used.

Even though it's designed for binary classification, the support vector machine, or SVM, the technique may be used for one-class classification. Before using one-class classifiers, scaled and conventional support vector machines can be applied to the dataset in circumstances of unbalanced classification. For one-class classification, the approach aids in sizing up the density of the majority class and classifies outliers on either side of the probability density. A one-class support vector machine is a variant of the SVM classifier.

Autoencoder neural network is an unsupervised ML algorithm that incorporates backpropagation by keeping the required values the same as the inputted values. This helps decrease the size of

the input into reduced representation. The original data can be reassembled from the compressed data. The primary goal of autoencoders is to learn the representation of a dataset, mainly for the simplification of dimensionality, by training it to overlook noise data. The input is compressed and put into a latent-space representation and the autoencoders then reconstruct the output out of this.

The autoencoder comprises an encoder, code, and decoder. The encoder helps compress the input into the latent space. The input image is encoded here as the compressed representation with a simplified dimensionality. Thus, this compressed version will be distorted in comparison to the original. The code part shows the input that was compressed which is loaded into the decoder. Finally, the decoder helps decode the compressed image back into the original version with the original dimension, resulting in a lossy reconstruction of the original from the latent space.

The features extracted through the above algorithms are then registered and stored in a database called the feature database. The machine learning classifiers included in the project are explained above. Thus, malware detection can be directly implemented resulting in the allowance of the benign traffic to be sent and received through the device and removal of any transmission back and forth of malicious data found due to the presence of Gafgyt and Mirai datasets

RESULTS AND DISCUSSION

Dataset

1. The dataset comprises three types of web traffic data, benign traffic containing 40, 395 records, Mirai traffic containing 652,100 records, and Gafgyt traffic containing 316,650 records.
2. Each record contains 115 features that were created by the distributors of the dataset utilizing crude credits of network traffic. As both Gafgyt and Mirai traffic delivered by the attack movement, the two information sources were joined to develop the general arrangement of noxious information (968,750 records) for this activity.
3. It tends to contend that a definitive objective of a model in that setting is to permit benign traffic to pass to and from the device, dispose of transmission, and gathering of malevolent data, a one-class classifier prepared utilizing benign data would satisfactorily suit the reason.
4. We utilized 80% of the benign records to assemble our model. This implies that 32, 316 records were utilized to prepare the model and (40,395 – 32,316) + (652,100 + 316,650) = 976,829 records were utilized to assess the presentation of the model.

Test Beds

In this project, we have used Jupyter Notebook for the compilation of the work. The testing and training part is written in R studio and the visualization is done on Anaconda Navigator using Python. Jupyter notebook is used to compile the Python as well as the R code to get the desired graph and outputs. Not only that, in the code part, many libraries were used like NumPy, Pandas, matplotlib, Keras, scikit-learn, and TensorFlow.

Expected Result

The result which is expected is 100% accuracy in detecting a bad traffic network with some virus, malware to the system, or any other type and normal network using machine learning and

deep learning. The output is determined using the confusion matrix. The model also predicts false data which helps in the prevention of installation of software during risks to minimize the cost.

ONE CLASS SVM MODEL EVALUATION

Model Evaluation

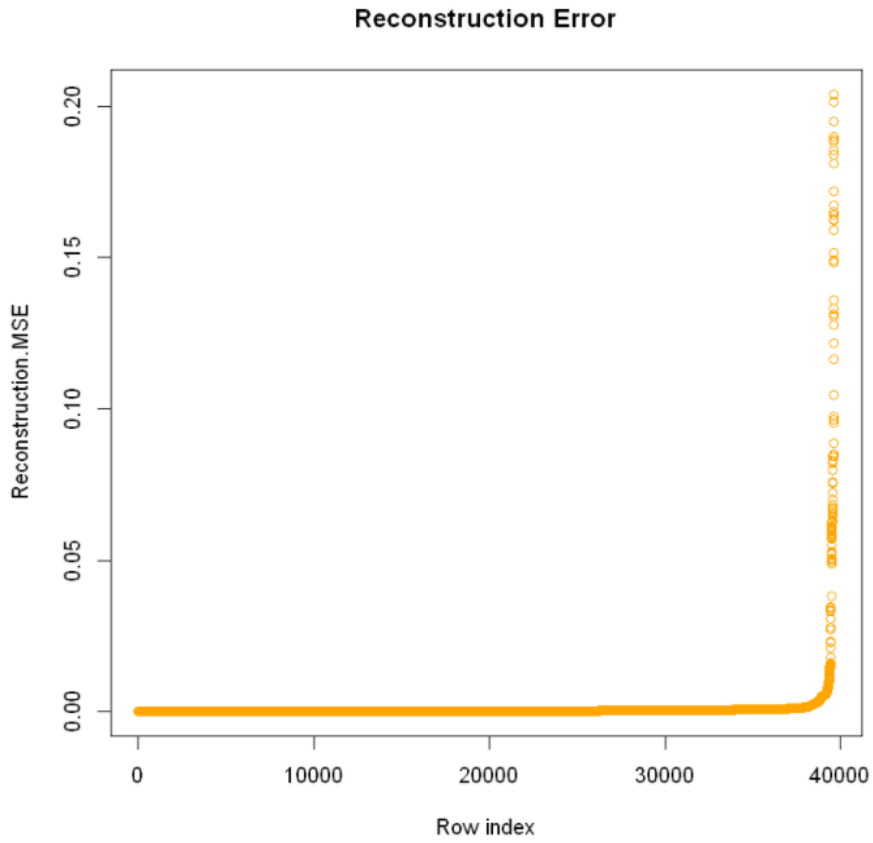
In [11]:
```
predictions <- predict(fit, testSet[,1:(ncol(testSet)-1)], type="response") # make predictions
```

In [12]:
```
confusionMatrix(data=as.factor(predictions),reference=as.factor(testSet$Type))
```

```
Confusion Matrix and Statistics

          Reference
Prediction  FALSE   TRUE
     FALSE 725065   2018
     TRUE       0   7891

               Accuracy : 0.9973
                 95% CI : (0.9971, 0.9974)
    No Information Rate : 0.9865
    P-Value [Acc > NIR] : < 2.2e-16

                  Kappa : 0.8853

 Mcnemar's Test P-Value : < 2.2e-16

            Sensitivity : 1.0000
            Specificity : 0.7963
         Pos Pred Value : 0.9972
         Neg Pred Value : 1.0000
             Prevalence : 0.9865
         Detection Rate : 0.9865
   Detection Prevalence : 0.9893
      Balanced Accuracy : 0.8982

       'Positive' Class : FALSE
```

AUTOENCODER IMPLEMENTATION

```
In [26]: plot(sort(err[,1]), main='Reconstruction Error',xlab="Row index", ylab="Reconstruction.MSE",col="orange")
```



reconstruction.MSE plot helps us to see where the model reconstructs the original records. Model was previously not able to learn patterns for those anomaly points. Reconstruction.MSE infer that at approximately 0.02 MSE, the data starts to become sparse, and therefore, including data above a 0.02 MSE will not be useful. Thus, we introduce a threshold value of 0.02 in the AutoEncoder model.

Defining the threshold based on Reconstruction. We randomly take 50% records of test instances due to the memory constraints and summarise (average) the results to approximate the accuracy if our computer has low computation resources. Then, we converted data to h20 compatible and calculated MSE across observations.

AUTOENCODER MODEL EVALUATION

```
In [41]: prediction <- err$Reconstruction.MSE<=threshold
```

```
In [42]: confusionMatrix(data=as.factor(prediction),reference=as.factor(newtestSet$Type))
```

```
Confusion Matrix and Statistics

          Reference
Prediction  FALSE   TRUE
     FALSE 483435     20
     TRUE       0   4959

               Accuracy : 1
                 95% CI : (0.9999, 1)
    No Information Rate : 0.9898
    P-Value [Acc > NIR] : < 2.2e-16

                  Kappa : 0.998
 Mcnemar's Test P-Value : 2.152e-05

            Sensitivity : 1.0000
            Specificity : 0.9960
         Pos Pred Value : 1.0000
         Neg Pred Value : 1.0000
             Prevalence : 0.9898
         Detection Rate : 0.9898
   Detection Prevalence : 0.9898
      Balanced Accuracy : 0.9980

       'Positive' Class : FALSE
```

Once the data has been fit into the model, the testset and the MSE threshold can be used to predict and show the performance of the AutoEncoder model. We can analyze the confusion matrix and infer the accuracy is now 100% with zero false negatives. This is a great improvement from the One-Class SVM model implemented above.

The 37 attack types mentioned in the dataset can be clustered into four general attack types as listed below:

- Denial of service attacks
- Remote to Local attacks
- User to Root
- Probe attacks

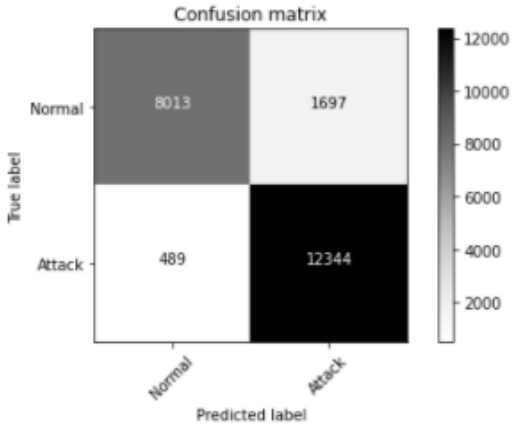
Our model will perform binary classification of the data to two classes indicating whether the traffic is normal or is a malicious attack, however, we will use the four attack types to analyze the results and calculate performance metrics for each general attack type. The next section replaces the current outcome field with a Class field that has one of the following values:

- Normal
- Dos
- R2L
- U2R
- Probe

PLOTTING CONFUSION MATRIX AND VIOLIN PLOTS

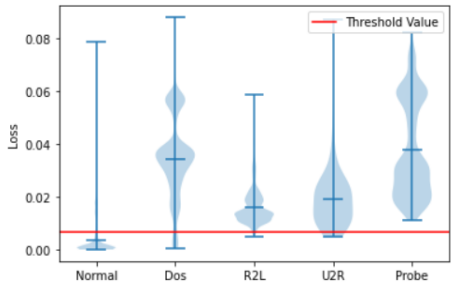
Plotting confusion matrix

In [21]:
```
def plot_confusion_matrix(cm, classes,
                          normalize=False,
                          title='Confusion matrix',
                          cmap=plt.cm.Greys):
    """
    This function prints and plots the confusion matrix.
    Normalization can be applied by setting `normalize=True`.
    """


    plt.imshow(cm, interpolation='nearest', cmap=cmap)
    plt.title(title)
    plt.colorbar()
    tick_marks = np.arange(len(classes))
    plt.xticks(tick_marks, classes, rotation=45)
    plt.yticks(tick_marks, classes)

    fmt = '.2f' if normalize else 'd'
    thresh = cm.max() / 2.
    for i, j in itertools.product(range(cm.shape[0]), range(cm.shape[1])):
        plt.text(j, i, format(cm[i, j], fmt),
                 horizontalalignment="center",
                 color="white" if cm[i, j] > thresh else "black")

    plt.tight_layout()
    plt.ylabel('True label')
    plt.xlabel('Predicted label')
c = confusion_matrix(y0_test,testing_set_predictions)
plot_confusion_matrix(c,["Normal","Attack"])
```



Violin plot

```
In [22]: plt.ylabel('Loss')
         plt.xticks(np.arange(0,5), classes)
         plt.violinplot([test_losses[np.where(y_test==class_)] for class_ in classes],np.arange(0,len(classes)),showmeans =True )
         plt.axhline(y=threshold,c='r',label="Threshold Value")
         plt.legend();
```



The violin plot shows the distribution of reconstruction loss values for the testing dataset values and clearly infer that the loss values of attacks are mostly higher than the threshold value, the opposite is true for the normal dataset.

CONCLUSION

The one class classifiers we used in the project were used for both training and testing set with which it will segregate malicious and good traffic which comes through the network. To increase the efficiency of the one-class classifiers we implemented a model using autoencoders which use deep learning neural networks. By the use of both algorithms we increased the efficiency of the project and we also attempted to overcome the problems that exist in the datasets, namely the class imbalance issue and the data being unrealistic, by avoiding the attacks data during training, the model was trained only using normal traffic, so it was not affected by the class imbalance of the dataset. Another strength of this approach is its simplicity, it consists of only a single hidden layer of 8 neurons making it very easy to train and especially suitable for online learning. During the evaluation, we avoided human manipulation of the threshold in order to achieve reproducible results without human interference.

REFERENCES

1. Intrusion detection using deep sparse auto-encoder and self-taught learning, Qureshi by A. S., Khan, A., Shamim, N., & Durad, M. H. (2019) Neural Computing and Applications (2019)
2. A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems by Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) 2019 11th International Conference on Knowledge and Systems Engineering (KSE). IEEE, 2019.
3. A Modular Multiple Classifier System for the Detection of Intrusions in Computer Networks Giorgio Giacinto, Fabio Roli, Luca Didaci Department of Electrical and Electronic Engineering, University of Cagliari, Italy

4. A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) In 2019 11th International Conference on Knowledge and Systems Engineering (KSE) (pp. 1-5). IEEE.
5. A novel statistical analysis and autoencoder-driven intelligent intrusion detection approach Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). Neurocomputing, 387, 51-62.
6. J. K. Chahal, V. Gandhi, P. Kaushal, K. R. Ramkumar, A. Kaur and S. Mittal, "KAS-IDS: A Machine Learning based Intrusion Detection System," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 90-95, doi: 10.1109/ISPCC53510.2021.9609402.
7. G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021, pp. 1224-1230, doi: 10.1109/ICIRCA51532.2021.9544717.
8. D. Xuan, H. Hu, B. Wang and B. Liu, "Intrusion Detection System Based on RF-SVM Model Optimized with Feature Selection," 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 2021, pp. 1-5, doi: 10.1109/CCCI52664.2021.9583206.
9. A. Aljohani and A. Bushnag, "An Intrusion Detection System Model in a Local Area Network using Different Machine Learning Classifiers," *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 2021, pp. 483-488, doi: 10.1109/ACIT52158.2021.9548421.
10. H. Elbahadır and E. Erdem, "Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks," 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021, pp. 401-406, doi: 10.1109/UBMK52708.2021.9558928.
11. S. T. Zargar, J. Joshi, and D. Tipper, ‘‘A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,’’ IEEECommun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, Mar. 2013.
12. V. Balamurugan and R. Saravanan, ‘‘Enhanced intrusion detection and prevention system on cloud environment using hybrid classification andOTS generation,’’ Cluster Comput., vol. 22, pp. 1–13, Nov. 2017.
13. J. Yan, D. Jin, C. W. Lee, and P. Liu, ‘‘A comparative study of off-line deep learning based network intrusion detection,’’ in Proc. 10th Int. Conf.Ubiquitous Future Netw. (ICUFN), Jul. 2018, pp. 299–304
14. M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, ‘‘Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,’’ IEEE Access, vol. 6, pp. 52843–52856, 2018.
15. B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, ‘‘Deep learning for classification of malware system call sequences,’’ in Proc. Australas.Joint Conf. Artif. Intell., 2016, pp. 137–149.

Plagiarism Checker X Originality Report

Similarity Found: 11%

Date: Monday, November 29, 2021
Statistics: 693 words Plagiarized / 6142 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

BCI 3002: Disaster Recovery and Business Continuity Management (DRBCM) Slot: A1+TA1 Research Paper TITLE: PREVENTION OF ATTACKS USING ONE CLASS CLASSIFICATION AND AUTOENCODERS 29th November 2021 Team Leader: Rohan Allen 18BCI0247 Team Members: Rakshith Sachdev 18BCI0109 Harshita Pundir 18BCI0192 ABSTRACT In this paper, we represent how one-class classifiers are prepared to utilize generous information to recognize ordinary and dangerous traffic redirected to an endpoint device.

In this venture, the framework is prepared to utilize unsupervised / one-class-based demonstrating approaches by which the framework would comprehend the issues that we would confront day by day, and the preparation will be useful for what's to come. After the preparation of the framework, the framework can be utilized in reality to confront ongoing, new difficulties and by gaining from the past experiences it can develop as indicated by the users' issues, weaknesses, dangers, and conditions KEYWORDS Autoencoders, feature generation, machine Learning, malware detection, malware profiling, network protection, one-class classification, INTRODUCTION With today’s day and age rapidly becoming digital, the network and endpoint devices become a target for attacks and exploitation; thus, the systems have long been associated with issues related to security.

Therefore, making systems secure and safe is of extreme importance. As per the 2020 Unit 42 Threat Report, practically all traffic is decoded, implying that the majority of classified and indiIntrusion detection using deep sparse auto-encoder and self-taught learning, Qureshi by A. S., visual user information in the network is highly powerless against cyber attacks.

Network security is utilized to delay unintentional harm which can be done to the network's private information, its users, or its devices. The main aim of network security is to secure the network running and for every single authentic client. The objective of this project is to use machine learning to teach our system to distinguish between malicious network traffic, which could contain a virus or malware, and regular network data.

The model has also been taught to detect and avoid fake data and the deployment of any specific software while there is a threat of an attack, which results in dramatically reducing the financial stress on an organization and prevents tarnishing their reputation. The major goal is to offer the most accurate findings possible by utilizing methods such as unsupervised learning/one-class-based modeling, thereby lowering processing time substantially. In this model, we are using one-class classifications and autoencoders so that the system can detect bad traffic more accurately.

With the help of this model, we can predict false data, and therefore, we can prevent the installation of software at the time of any risks to decrease the cost. LITERATURE SURVEY TITLE, AUTHOR, AND JOURNAL OBJECTIVE METHODOLOGY USED LIMITATION Khan, A., Shamim, N., & Durad, M. H. (2019) Neural Computing and Applications (2019).

[1] This paper gives the idea of self-education figuring out how to prepare the deep neural network for network intrusion detection. In the proposed strategy, a Self Taught based Transfer Learning(DST-TL) is used to remove the highlights from the NSL-KDD dataset a relapse related pre-prepared network is utilized This system cannot classify the different types of attacks as deep neural networks are not used.

A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems by Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) 2019 11th International Conference on Knowledge and Systems Engineering (KSE). IEEE, 2019. [2] This paper provides the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder(SAE) to lessen the limitations in handling the datasets.

In the proposed method, the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder is used to detect the anomalies occurring in the network. With the help of this method, datasets can also be handled properly It failed to extend these works by using better clustering algorithms and other metrics to find a suitable number of clusters in the data A Modular Multiple Classifier System for the Detection of Intrusions in Computer Networks Giorgio Giacinto, Fabio Roli, Luca Didaci Department of Electrical and Electronic Engineering, University of Cagliari, Italy.

[3] This paper provides a strategy to use Intrusion Detection Systems (IDS) and pattern recognition to increase the level of security on computer networks. The authors later discuss and evaluate the effectiveness of the IDS on the security of the network. Utilizing IDS and example acknowledgment ways to deal with network intrusion detection dependent on the combination of numerous classifiers.

Specifically, the author centers around Modular Multiple Classifier engineering plans where every module in the design can identify intrusions against the administrations offered by the secured network. This study presents an extensive report on how IDS and pattern recognition can be used to provide higher levels of network security. The paper includes a descriptive report on how the authors used methods like machine learning in their implementation and design and also compared different training sets on the data to conclude which model is most effective.

Although this paper is detailed, our methodology of achieving a system that can differentiate between good and bad networks containing viruses and malware includes methods and techniques using One-Class Classification and Auto Encoders. A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems Bui, T. C., Hoang, M., & Nguyen, Q. U.

(2019, October) In 2019 11th International Conference on Knowledge and Systems Engineering (KSE) (pp. 1-5). IEEE. [4] A detailed examination and investigation of different AI procedures have been completed to discover the reason for issues related to different AI strategies in identifying intrusive exercises. AI methods have been examined and looked at as far as their recognition ability for distinguishing the different classes of assaults.

Limits related to every classification of them are additionally talked about. Different data mining apparatuses for AI have additionally been remembered for the paper Existing literature is described which is based on similar techniques with most of the popular datasets as on date to generalize our observations.

All the techniques have not been implemented to evaluate the performance to ensure that results are reproducible A novel statistical analysis and autoencoder-driven intelligent intrusion detection approach. Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). Neurocomputing, 387, 51-62. [5] Statistical examination and autoencoder (AE) driven insightful intrusion detection (IDS) framework is acquainted with recognizing and alleviate the dangers of programmers growing much more complex and risky malware assaults that make intrusion detection a troublesome assignment Initially, the NSLKDD dataset is cleaned from anomalies and the min-max

standardization procedure is utilized to scale data inside the range 0 and 1.

Subsequently, the one-hot-encoding is applied to change over symbolic (or categorized) features into numeric quantities. At that point, the 38 numeric attributes are investigated statistically to choose the most associated features. At last, shallow (MLP, L-SVM, Q-SVM, LDA, QDA) and deep (AE, LSTM) networks are created to quantify the detection execution both in parallel and multi-classification situations.

The advancement of more precise deep architectures that can oversee continuous real-time data streams like NSL-KDD examples to recognize malicious attacks progressively can build its proficiency. Also, to misuse long-term learning, quicker choice models along with decreased computational complexity for constant needs to execute in this system. J. K.

Chahal, V. Gandhi, P. Kaushal, K. R. Ramkumar, A. Kaur and S. Mittal, "KAS-IDS: A Machine Learning based Intrusion Detection System," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021.[6] Regrettably, the majority of commercial IDSs are based on abuse and are only designed to detect known threats.

These require frequent signature updates and have a limited capacity for detecting new assaults. As a result, this study proposes an anomaly-based IDS as a viable solution to this challenge. KAS-IDS, or K-Means and Adaptive SVM based Intrusion Detection System, is the approach proposed in this study.

K-Means were used in the first stage to create data clusters, and adaptive SVM was used in the second step to classify the data. As part of the current technique, the data is split into two categories: normal and abnormal data, and correct findings are obtained using the NSL-KDD dataset, which can also be used for real-time traffic analysis.

Apart from that, the intelligent agents of clustering and classification algorithms can improve its performance in real-time traffic analysis. G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021[7]. The main purpose of this project is to compare and assess the effectiveness of neural network models on a data set.

To identify intrusion rates, the suggested application uses the SVM (Support Vector Machine) and ANN (Artificial Neural Networks) algorithms. Each algorithm is used to determine if the data being requested is allowed or includes any irregularities. These techniques employed feature selection algorithms based on correlation and

Chi-Squared to decrease the dataset by removing unnecessary data.

Another dataset with a larger number of characteristics might be used to improve this research. Because ANN provides greater accuracy but slower calculations, we can apply alternative efficient algorithms in the future that may provide greater accuracy while also computing faster, allowing it to be employed in real-time applications. D. Xuan, H. Hu, B. Wang and B.

Liu, "Intrusion Detection System Based on RF-SVM Model Optimized with Feature Selection," 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 2021.[8] The goal of this research is to improve network intrusion detection using machine learning. The two-stage IDS suggested in this research is based on machine learning algorithms RF and SVM that are tuned with the Feature Ranking CFS.

In this research, they present a two-stage IDS based on machine learning models RF and SVM tuned with the CFS method, and they tested it on NSL-KDD benchmark datasets, contrasting it to the RF and SVM modeling. We plan to develop the IDS in the future with the goal of increasing the detection precision of low-frequency assaults, which is a common difficulty in IDS.

Furthermore, the capacity of an IDS to identify unknown forms of threats is taken into account. We'd want to increase the accuracy of detecting unknown forms of assaults. A. Aljohani and A. Bushnag, "An Intrusion Detection System Model in a Local Area Network using Different Machine Learning Classifiers," 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), 2021.[9] The article presents a security control for an IDS that is used to identify known and unknown attacks in order to avoid security concerns in LANs.

The suggested system uses Neural Network and Support Vector Machine (SVM) models for intrusion detection to avoid security risks in a Local Area Network (LAN). The KDD99 dataset is used to test the suggested method. The KDD99 is an anomaly-based detection benchmark. This method detects assaults quickly and effectively. In future research, the KDD99 dataset may be used to classify threat categories to see which machine learning classifier performs better. H. Elbahadir and E.

Erdem, "Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks," 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021.[10] An intrusion detection system (IDS) is modeled in this work to assure WSN security. Because signature, misuse, and anomaly-based intrusion

detection approaches are insufficient to offer security on their own, a hybrid model is presented in which these methods are combined.

Anomaly criteria were created for attack detection, and the BayesNet, J48, and Random Forest machine learning algorithms were employed to categorize normal and anomalous traffic in the hybrid model. Application of alternative efficient algorithms in the future that may provide greater accuracy while also computing faster, allowing it to be employed in real-time applications. S. T. Zargar, J. Joshi, and D. Tipper, ''A survey of defense mechanisms against distributed denial of service (DDoS) ?ooding attacks,'' IEEECommun.

Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, Mar. 2013. [11] This paper describes the developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack. The paper provides the knowledge required about the attacks as this project works on prevention of attacks.

It stimulates our research into understanding how the attacks occur which in turn help with solutions to prevent them. Existing literature is described which is based on similar techniques with most of the popular datasets as on date to generalize our observations. All the techniques have not been implemented to evaluate the performance to ensure that results are reproducible. V. Balamurugan and R.

Saravanan, ''Enhanced intrusion detection and prevention system on cloud environment using hybrid classi?cation andOTS generation,'' Cluster Comput., vol. 22, pp. 1–13, Nov. 2017. [12] The proposed system in this paper is directed on intrusion detection systems and it uses cloudlet controller, trust authority and virtual machine management in cloud environments.

The proposed classifier in this paper effectively detects the attackers which are experimentally proved by comparing with existing classification models which provides a very good in sight. Application of alternative efficient algorithms in the future that may provide greater accuracy while also computing faster, allowing it to be employed in real-time applications. J. Yan, D. Jin, C. W. Lee, and P. Liu, ''A comparative study of off-line deep learning based network intrusion detection,'' in Proc. 10th Int. Conf.Ubiquitous Future Netw. (ICUFN), Jul. 2018, pp. 299–304. [13] It intends to answer some of the research questions speci?ed in and random forest classi?ers, which are shallow.

The authors indicated that their approach could reduce the SVM's training and testing

times in both binary and multiclass classi?cations and improves the prediction accuracy of the SVM. They used ISCX 2012 dataset and achieved ten features from it by using an auto-encoder and fed it to the SVM for its training. Theauthors indicated the bene?ts of their method regarding met-rics like Kappa statistics, detection rate, accuracy, and FPR.

It is only able to conduct the binary classi?cation and cannot handle the multiclass attack traf?cs M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, ''Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,'' IEEE Access, vol. 6, pp. 52843–52856, 2018. [14] This paper proposes a scheme that uses the self-taught learning framework for the learning of features and reduction of dimension.

This IDS model bene?ts from a sparse auto-encoder for unsupervised reconstructing a new feature representation. The authors indicated that their approach could reduce the SVM's training and testing times in both binary and multiclass classi?cationsand improves the prediction accuracy of the SVM. The ef?ciency of this approach in binary and multiclass classi?cations is evaluated against the naive random forest classi?ers, which are shallow.

B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, ''Deep learning for classi?cation of malware system call sequences,'' in Proc. Australas.Joint Conf. Artif. Intell., 2016, pp. 137–149. [15] The authors used recurrent and convolutional network layers to construct an ANN model and by using one recurrent layer and two convolutional layers, they detect various malware. This model achieves good accuracy for multiclass intrusion detection with both datasets. Also, FAR and the execution time of this scheme are low.

This scheme should be further evaluated on the other imbalanced datasets,in which some of their attack classes have much fewer data records than others, to verify the detection rate of the minority class security attacks. Khan et. al.[1] in this paper gives the idea of self-education figuring out how to prepare the profound neural network for network intrusion detection.

In the proposed strategy, a Self Taught based Transfer Learning(DST-TL) is used to remove the highlights from the NSL-KDD dataset a relapse-related pre-prepared network is utilized. The limit of this system cannot classify the different types of attacks as deep neural networks are not used. Bui et. al.[2] in this paper provides the hybrid model of the K-Means clustering algorithm and Shrink AutoEncoder(SAE) to lessen the limitations in handling the datasets.

In the proposed method, the hybrid model of the K-Means clustering algorithm and

Shrink AutoEncoder is used to detect the anomalies occurring in the network. With the help of this method, datasets can also be handled properly. The limit of the system is that it failed to extend these works by using better clustering algorithms and other metrics to find a suitable number of clusters in the data. Giacinto et. al.

[3] in this paper provide a strategy to use Intrusion Detection Systems (IDS) and pattern recognition to increase the level of security on computer networks. The authors later discuss and evaluate the effectiveness of the IDS on the security of the network. Utilizing IDS and example acknowledgment ways to deal with network intrusion detection dependent on the combination of numerous classifiers.

Specifically, the author centers around Modular Multiple Classifier engineering plans where every module in the design can identify intrusions against the administrations offered by the secured network. The limit of this study presents an extensive report on how IDS and pattern recognition can be used to provide higher levels of network security.

The paper includes a descriptive report on how the authors used methods like machine learning in their implementation and design and also compared different training sets on the data to conclude which model is most effective. Although this paper is detailed, our methodology of achieving a system that can differentiate between good and bad networks containing viruses and malware includes methods and techniques using One-Class Classification and Auto Encoders. Bui et. al.

[4]do a detailed examination and investigation of different AI procedures have been completed to discover the reason for issues related to different AI strategies in identifying intrusive exercises.AI methods have been examined and looked at as far as their recognition ability for distinguishing the different classes of assaults. Limits related to every classification of them are additionally talked about.

Different data mining apparatuses for AI have additionally been remembered for the paper. The limit of the existing literature is described which is based on similar techniques with most of the popular datasets as on date to generalize our observations. All the techniques have not been implemented to evaluate the performance to ensure that results are reproducible Ieracitano et. al.

[5] statistical examination and autoencoder (AE) driven insightful intrusion detection (IDS) framework is acquainted with recognizing and alleviating the dangers of programmers growing much more complex and risky malware assaults that make intrusion detection a troublesome assignment. Initially, the NSLKDD dataset is cleaned

from anomalies and the min-max standardization procedure is utilized to scale data inside the range 0 and 1.

Subsequently, the one-hot-encoding is applied to change over symbolic (or categorized) features into numeric quantities. At that point, the 38 numeric attributes are investigated statistically to choose the most associated features. At last, shallow (MLP, L-SVM, Q-SVM, LDA, QDA) and deep (AE, LSTM) networks are created to quantify the detection execution both in parallel and multi-classification situations.

The limit of the advancement of more precise deep architectures that can oversee continuous real-time data streams like NSL-KDD examples to recognize malicious attacks progressively can build its proficiency. Also, to misuse long-term learning, quicker choice models along with decreased computational complexity for constant needs to execute in this system. Chahal et.al.

[6] talk about machine learning-based IDS for anomaly detection. Intrusion detection systems (IDS) serve an important role in detecting intrusions. This paper introduces a hybrid strategy that combines K-Means and Adaptive SVM, concluding that the combined results are superior to the individual results of K-Means and Adaptive SVM. Furthermore, when compared to other methodologies, this algorithm is quite accurate.The hybrid technology correctly distinguishes between normal and attack data, and this approach is 99.54 percent more accurate than solo techniques.

As a result, employing this approach in real-time results in an extremely high detection rate of assaults. Furthermore, this method is easy and effective, especially when it comes to lowering the false-positive ratio and increasing the false negative ratio. Yedukondalu et.al. [7] To identify intrusion rates, the suggested application uses the SVM (Support Vector Machine) and ANN (Artificial Neural Networks) algorithms.

Each algorithm is used to determine if the data being requested is allowed or includes any irregularities. While the IDS examines the requested data, if it detects any malicious material, the request is dropped. These techniques employed feature selection algorithms based on correlation and Chi-Squared to decrease the dataset by removing unnecessary data.

The preprocessed dataset is trained and evaluated with the models to generate notable findings, which improves prediction accuracy. The experiment was conducted using the NSL KDD dataset. Finally, the SVM algorithm obtained a 48 percent accuracy, while the ANN method achieved a 97 percent accuracy. On this dataset, the ANN model performs better than the SVM. Xuan et.al. [8] IDS is a good way to cope with the ever-changing

nature of network attacks.

In this research, we present a two-stage IDS based on machine learning models RF and SVM optimized with the CFS method, and we tested it on NSL-KDD benchmark datasets, comparing it to the RF and SVM models. The following is a summary of the key findings: (1) Our two-stage IDS outperformed RF and SVM, increasing Precision by 4.31 percent, Recall by 3.39 percent, and F1-measure by 5.56 percent to 11.08 percent; (2) the feature selection algorithm CFS, which we used in this paper, improved accuracy by 1.50 percent while reducing the time by 8.07 percent; and (3) our approach reduced Test Set prediction time by 93.84 percent compared to SVM. Aljohani et.al.

[9] The suggested system uses Neural Network and Support Vector Machine (SVM) models for intrusion detection to avoid security risks in a Local Area Network (LAN). The KDD99 dataset is used to test the suggested method. The KDD99 is an anomaly-based detection benchmark. This method detects assaults quickly and effectively. A comparison of the SVM and Neural Network models' performance is carried out.

In terms of classification accuracy, the findings demonstrate that the Neural Network outperformed all SVM kernel models. The SVM linear kernel outperforms the SVM Gaussian kernel by a small margin, and the SVM polynomial kernel by a large margin. Elbahadir et.al. [10] An intrusion detection system (IDS) is modeled in this work to assure WSN security.

Because signature, misuse, and anomaly-based intrusion detection approaches are insufficient to offer security on their own, a hybrid model is presented in which these methods are combined. Anomaly criteria were created for attack detection, and the BayesNet, J48, and Random Forest machine learning algorithms were employed to categorize normal and anomalous traffic in the hybrid model. The findings revealed that the generated model has a high level of accuracy and a low percentage of false alarms. Zargar et.al.

[11] This paper describes the developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack. The paper provides the knowledge required about the attacks as this project works on prevention of attacks. It stimulates our research into understanding how the attacks occur which in turn help with solutions to prevent them. Balamurugan et.al.

[12] The proposed system in this paper is directed on intrusion detection systems and it uses cloudlet controller, trust authority and virtual machine management in cloud

environments. The proposed classifier in this paper effectively detects the attackers which are experimentally proved by comparing with existing classification models which provides a very good in sight. Yan et.al. [13] It intends to answer some of the research questions speci?ed in and random forest classi?ers, which are shallow.

The authors indicated that their approach could reduce the SVM's training and testing times in both binary and multiclass classi?cations and improves the prediction accuracy of the SVM. They used ISCX 2012 dataset and achieved ten features from it by using an auto-encoder and fed it to the SVM for its training. Theauthors indicated the bene?ts of their method regarding met-rics like Kappa statistics, detection rate, accuracy, and FPR. Al-Qatf et.al.

[14] This paper proposes a scheme that uses the self-taught learning framework for the learning of features and reduction of dimension. This IDS model bene?ts from a sparse auto-encoder for unsupervised reconstructing a new feature representation. The authors indicated that their approach could reduce the SVM's training and testing times in both binary and multiclass classi?cationsand improves the prediction accuracy of the SVM. Kolosnjaji et.al.

[15] The authors used recurrent and convolutional network layers to construct an ANN model and by using one recurrent layer and two convolutional layers, they detect various malware. This model achieves good accuracy for multiclass intrusion detection with both datasets. Also, FAR and the execution time of this scheme are low. METHODOLOGY ONE CLASS SVM: One-class SVM is an unsupervised algorithm that learns a decision work for curiosity identification: ordering new information as comparative or diverse to the preparation set. One-class classification algorithms are often used for binary classification tasks with a severely skewed class distribution.

These techniques are used to fit on the input examples from the huge class within the training dataset, then evaluated on the remaining test dataset. Albeit not designed for these types of problems, one-class classification methods are frequently successful for unbalanced classification datasets with no or few instances of the minority class, or datasets with no cohesive structure to distinguish the classes that a supervised algorithm would learn.

The SVM algorithm, which was originally designed for classification tasks, is frequently employed for one-class classification. AUTOENCODERS: An autoencoder neural network is a type of unsupervised machine learning technique that uses backpropagation to adjust the target values to the inputs. Autoencoders have a habit of condensing the dimensions of our inputs into a more compact representation.

If the first data is required, the condensed data will be used to recreate it. The purpose of an autoencoder is to train the model to ignore signal noise in order to discover a symbol for a set of knowledge, generally to reduce dimensions. They work by condensing the input into a latent-space description and then reconstructing the outcome from there.

We'll visualize our findings and results as part of the analysis once both of these models have been implemented and trained, and we'll try and compare the trained models to see which one gives an exact result. There are three different types of datasets available as input: innocuous traffic (40,395 records), Mirai traffic (652,100 records), and Gafgyt traffic (316,650 records). Benign traffic is clean data flow, whereas Gafgyt and Mirai traffic both contain harmful data, resulting in malware traffic.

Each record in the dataset has 115 attributes that were generated by the dataset's publishers using the raw characteristics of network traffic. Because both Gafgyt and Mirai traffic are generated from attack activity, they are combined to create the malicious data (968,750 records). For training the model, 80 percent of the benign traffic data is fed into the one-class classifier.

This means that the model was trained using 32,316 data, and the model's performance was evaluated with (40,395 – 32,316) + (652,100 + 316,650) = 976,829 records. This is also further given as input for the training of the autoencoder model. The rest 20% of the benign traffic data is sent to the testing phase of both the one-class classifier and autoencoder model.

This is also used as an input for the autoencoder model's training. The remaining 20% of the benign traffic data is supplied to the one-class classifier and autoencoder models for testing. The Gafgyt and Mirai traffic data, which contains harmful data, are combined with 20% of the benign traffic data to see if the one-class classifier and autoencoder models can help sort traffic into clean and malware traffic. Data is pre-processed in order to increase the quality of the datasets involved.

Because there are various datasets to consider, functions are built to ensure that they are loaded and entered into the needed model. Getting examples of cases with good traffic which displays benign behavior is simpler and easier to get in comparison with malware traffic that displays malicious behavior.

This can be due to the fact that obtaining malware traffic can come at a cost or in some cases, impractical like the days with no attacks thus containing only good traffic. Other

explanations regarding this could be on the basis of privacy, law, and ethics. But, despite all this, it can be easily convinced that corrupted traffic data can be used first to build models like the two-class classifier.

But it cannot be assured that all scenarios involving bad traffic data can be replicated. This issue can be addressed using the unsupervised one-class classifier methodology approach here. So, in this project, the training model is created only using benign instances, and this trained model is then implemented to detect any unknown/new cases of traffic using machine-learning and other statistical methods.

If the data targeted shows considerable diversion according to predetermined calculations, it will be labeled as out-of-class. Thus, one-class classifiers that may belong to different families are examined here under the criterion of performance. One-Class Support Vector Machine from the conventional ML family and Autoencoder from the deep learning family are the two one-class classifiers and their related families illustrated here. In this case, we're investigating how benign occurrences vary from corrupted occurrences in terms of structure.

The Autoencoder model is built on the basis of this base composition. Through training sets comprising only examples of that class, one-class classifiers may distinguish instances of a given class from all other instances. This is a benign class that is being explored. There are various types of one-class classifiers that examine opposing examples to refine the categorization limit.

Other purposes that a one-class classifier can fulfill are in cases of binary and imbalanced classification datasets. In the scenarios where binary classification is to be done but the majority of the dataset overpowers the minority, the training set is modeled based on the majority category of data, before being jointly evaluated in the testing phase.

Because one-class classifiers are not built for cases involving unbalanced categorization datasets where the minority may be non-existent or not evident enough, supervised machine learning approaches will need to be used. Even though it's designed for binary classification, the support vector machine, or SVM, the technique may be used for one-class classification.

Before using one-class classifiers, scaled and conventional support vector machines can be applied to the dataset in circumstances of unbalanced classification. For one-class classification, the approach aids in sizing up the density of the majority class and classifies outliers on either side of the probability density. A one-class support vector

machine is a variant of the SVM classifier.

Autoencoder neural network is an unsupervised ML algorithm that incorporates backpropagation by keeping the required values the same as the inputted values. This helps decrease the size of the input into reduced representation. The original data can be reassembled from the compressed data. The primary goal of autoencoders is to learn the representation of a dataset, mainly for the simplification of dimensionality, by training it to overlook noise data.

The input is compressed and put into a latent-space representation and the autoencoders then reconstruct the output out of this. The autoencoder comprises an encoder, code, and decoder. The encoder helps compress the input into the latent space. The input image is encoded here as the compressed representation with a simplified dimensionality.

Thus, this compressed version will be distorted in comparison to the original. The code part shows the input that was compressed which is loaded into the decoder. Finally, the decoder helps decode the compressed image back into the original version with the original dimension, resulting in a lossy reconstruction of the original from the latent space. The features extracted through the above algorithms are then registered and stored in a database called the feature database.

The machine learning classifiers included in the project are explained above. Thus, malware detection can be directly implemented resulting in the allowance of the benign traffic to be sent and received through the device and removal of any transmission back and forth of malicious data found due to the presence of Gafgyt and Mirai datasets RESULTS AND DISCUSSION Dataset 1.

The dataset comprises three types of web traffic data, benign traffic containing 40, 395 records, Mirai traffic containing 652,100 records, and Gafgyt traffic containing 316,650 records. 2. Each record contains 115 features that were created by the distributors of the dataset utilizing crude credits of network traffic. As both Gafgyt and Mirai traffic delivered by the attack movement, the two information sources were joined to develop the general arrangement of noxious information (968,750 records) for this activity. 3.

It tends to contend that a definitive objective of a model in that setting is to permit benign traffic to pass to and from the device, dispose of transmission, and gathering of malevolent data, a one-class classifier prepared utilizing benign data would satisfactorily suit the reason. 4. We utilized 80% of the benign records to assemble our model.

This implies that 32, 316 records were utilized to prepare the model and (40,395 – 32,316) + (652,100 + 316,650) = 976,829 records were utilized to assess the presentation of the model. Test Beds In this project, we have used Jupyter Notebook for the compilation of the work. The testing and training part is written in R studio and the visualization is done on Anaconda Navigator using Python.

Jupyter notebook is used to compile the Python as well as the R code to get the desired graph and outputs. Not only that, in the code part, many libraries were used like NumPy, Pandas, matplotlib, Keras, scikit-learn, and TensorFlow. Expected Result The result which is expected is 100% accuracy in detecting a bad traffic network with some virus, malware to the system, or any other type and normal network using machine learning and deep learning. The output is determined using the confusion matrix.

The model also predicts false data which helps in the prevention of installation of software during risks to minimize the cost. ONE CLASS SVM MODEL EVALUATION Model Evaluation AUTOENCODER IMPLEMENTATION reconstruction.MSE plot helps us to see where the model reconstructs the original records. Model was previously not able to learn patterns for those anomaly points. Reconstruction.MSE infer that at approximately 0.02 MSE, the data starts to become sparse, and therefore, including data above a 0.02 MSE will not be useful. Thus, we introduce a threshold value of 0.02 in the AutoEncoder model. Defining the threshold based on Reconstruction.

We randomly take 50% records of test instances due to the memory constraints and summarise (average) the results to approximate the accuracy if our computer has low computation resources. Then, we converted data to h20 compatible and calculated MSE across observations. AUTOENCODER MODEL EVALUATION Once the data has been fit into the model, the testset and the MSE threshold can be used to predict and show the performance of the AutoEncoder model. We can analyze the confusion matrix and infer the accuracy is now 100% with zero false negatives.

This is a great improvement from the One-Class SVM model implemented above. The 37 attack types mentioned in the dataset can be clustered into four general attack types as listed below: ? Denial of service attacks ? Remote to Local attacks ? User to Root ? Probe attacks Our model will perform binary classification of the data to two classes indicating whether the traffic is normal or is a malicious attack, however, we will use the four attack types to analyze the results and calculate performance metrics for each general attack type.

The next section replaces the current outcome field with a Class field that has one of the following values: ? Normal ? Dos ? R2L ? U2R ? Probe PLOTTING CONFUSION MATRIX

AND VIOLIN PLOTS Plotting confusion matrix Violin plot The violin plot shows the distribution of reconstruction loss values for the testing dataset values and clearly infer that the loss values of attacks are mostly higher than the threshold value, the opposite is true for the normal dataset.

CONCLUSION The one class classifiers we used in the project were used for both training and testing set with which it will segregate malicious and good traffic which comes through the network. To increase the efficiency of the one-class classifiers we implemented a model using autoencoders which use deep learning neural networks. By the use of both algorithms we increased the efficiency of the project and we also attempted to overcome the problems that exist in the datasets, namely the class imbalance issue and the data being unrealistic, by avoiding the attacks data during training, the model was trained only using normal traffic, so it was not affected by the class imbalance of the dataset.

Another strength of this approach is its simplicity, it consists of only a single hidden layer of 8 neurons making it very easy to train and especially suitable for online learning. During the evaluation, we avoided human manipulation of the threshold in order to achieve reproducible results without human interference.

<1% - www.researchgate.net › publication › 273213434_K-SVM
<1% - digitalcommons.latech.edu › cgi › viewcontent
<1% - www.sciencedirect.com › traffic-analysis
<1% - toc.proceedings.com › 60511webtoc
<1% - socialsciences.cornell.edu › research-incubation
<1% - www.ijettjournal.org › volume-3 › issue-4
<1% - www.researchgate.net › publication › 318279418_An
<1% - jis-eurasipjournals.springeropen.com › articles › 10
<1% - www.researchgate.net › publication › 355026200_An
<1% - www.wunu.edu.ua › en › 10216-11th-international
<1% - www.ai.rug.nl › ~mwiering › GROUP
<1% - ijana.in › papers › V6I4-10
<1% - www.sciencedirect.com › intrusion-detection-system
<1% - www.ifsecglobal.com › uncategorized › signature
<1% - aijsh.com › wp-content › uploads
<1% - dl.acm.org › doi › 10
<1% - www.ijert.org › analysis-of-denial-of-services-dos
<1% - www.researchgate.net › figure › KEY-TERMS-APPEARED
<1% - www.researchgate.net › publication › 328766118_HyINT
<1% - www.hindawi.com › journals › scn
<1% - www.researchgate.net › publication › 221533942
<1% - www.researchgate.net › publication › 349531131_A
<1% - www.scribd.com › document › 430024136
<1% - www.ncbi.nlm.nih.gov › pmc › articles
<1% - downloads.hindawi.com › journals › mpe
<1% - www.checkpoint.com › cyber-hub › network-security
<1% - www.researchgate.net › publication › 12413257_New
<1% - serokell.io › blog › classification-algorithms
<1% - machinelearningmastery.com › one-class
<1% - blockgeni.com › classification-algorithms-for
<1% - cse.iitkgp.ac.in › ~sudeshna › courses
<1% - iq.opengenus.org › types-of-autoencoder
1% - github.com › Putting-data-into-action › IoT-Security
1% - www.irjet.net › archives › V8
<1% - www.mdpi.com › 2079/9292/10-21 › 2696
<1% - www.irjet.net › archives › V5
<1% - link.springer.com › chapter › 10
<1% - course.ccs.neu.edu › cs5100f11 › resources
<1% - ufldl.stanford.edu › tutorial › unsupervised
<1% - towardsdatascience.com › deep-inside-autoencoders

<1% - deepai.org › publication › autoencoders
<1% - www.researchgate.net › publication › 337811525
<1% - machinelearningmastery.com › lstm-autoencoders
<1% - www.academia.edu › 30688608 › K_Means_Cluster_based
<1% - pt.scribd.com › document › 464972254