National College of Ireland

Information Security and Data protection: A review of challenges and influencing factor faced in IT

MSc Research Project
Programme Name

Deepika Porkodian Suganraj
Student ID: 22185712

School of Computing
National College of Ireland

Supervisor: Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Deepika Porkodian Suganraj
Student ID:	22185712
Programme:	Masters in Cybersecurity **Year:** 2023
Module:	Msc Research Project
Supervisor:	Jawad Salahuddin
Submission Due Date:	31/1/2024
Project Title:	Information Security and Data Protection: A Review of Challenges and Influencing Factor Faced In IT
Word Count:	6687 **Page Count** 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Deepika Porkodian Suganraj
Date:	31/1/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Information Security and Data Protection: A Review of Challenges and Influencing Factor Faced In IT

Deepika Porkodian Suganraj
22185712

Abstract

Information security and data protection are critical concerns in IT Systems, due to a rising risk of data breaches, abnormal network activity, human error, and privacy violations. The aim of this study is to examine the method and approach that may be employed to successfully lower the risks related to data breaches, anomalous network activity, and privacy violations in IT systems. A survey was also carried out among IT professionals to effectively find their understanding on data handling, incident reporting, information security, and other aspects on security, resulting in Intrusion detection systems (IDS) as the proposed approach to reduce the risks of privacy violations and data leaks in IT systems. The Deep Belief Network-Gated Recurrent Unit (DBN-GRU) architecture-based novel intrusion detection system makes use of a machine learning algorithm and the NSL-KDD99 dataset to identify intrusions. The method includes extensive data pre-processing to improve the quality of the data, such as binary encoding, data scaling, and Min-Max normalisation. Combining the sequential pattern recognition of GRUs with the hierarchical characteristic learning of DBNs, the hybrid DBN-GRU model provides a comprehensive method for stimulating complex information connections in network data. TensorFlow and Keras libraries are utilised to create and train the neural network model. Three crucial steps in the training process are progressive backpropagation, hyperparameter adjustment, and regularisation. A 98.92% accuracy rate in categorising incoming data as either normal or abnormal network activity is achieved by the model, according to an independent dataset evaluation. Compared to baseline methods like Random Forest, SVM, and GNB, this is a significantly better approach. The results of the study demonstrate how well the suggested strategy works to identify intrusions and enhance network protection. Python is used as a software tool throughout the implementation, which improves the approaches' dependability and efficiency. This work offers a helpful tool for enhancing network security through the creation of distinctive hybrid architecture by accurately detecting and classifying intrusion attempts. The approach, outcomes, and conclusions of the study offer significant insights into how intrusion detection systems and machine learning can be used in IT systems to secure data and maintain information security.

1 Introduction

In today's digital world, information security plays a critical role in preventing unauthorised access, disclosure, and modification of sensitive data. Strong information security measures are essential given the increasing focus on networked technology and online resources (Abdalzaher et al, 2022). It includes availability, confidentiality, and integrity—also referred to as the "CIA trinity"—which together form the foundational principles of information security (William et al, 2022). According to (Prabhakar et al, 2022), firewalls, encryption, access controls, and incident response protocols are essential components in the fight against a variety of online threats.

Organisations invest in threat intelligence, vulnerability assessments, and penetration testing to find and fix potential weaknesses in their systems as information security threats change (Tsao et al, 2022). To protect information assets and handle matters such as employee training and incident response, it is imperative to establish thorough security policies that encompass guiding concepts, procedures, and legal requirements (Ghillani et al, 2022). Following industry-specific rules and regulations is frequently mandated by legislation, indicating a dedication to data security and reducing legal risks (Ghelani et al, 2022). Businesses need to take a proactive approach in the constantly evolving field of information security, which involves enhancing security measures on a regular basis, keeping aware of technical advancements, and creating a work climate that prioritises security (Zhang et al, 2022). According to (Kanade et al, 2022), current trends include the development of zero-trust architectures, improvements in security technologies, and a greater emphasis on cloud environment security. Data protection is essential for effective information management in the age of digital data. It includes policies, processes, and norms to guarantee that private rights are respected when handling sensitive and private data (Alshurideh et al, 2023). Key ideas that integrate privacy considerations from the outset and proactively manage privacy issues are privacy by design and privacy impact assessments (Rathore et al, 2022). To prevent unauthorised access, disclosure, or alteration of data, data security measures are put in place, such as encryption, access controls, and secure communication channels (Jakka et al, 2022).

The study's principal goal is to minimise the risk that IT systems would experience in privacy violations, data leaks, anomalous network activity, and human error. The suggested method provides an enhanced solution for detecting network intrusions and developing network security technologies by utilising a hybrid DBN-GRU architecture within Intrusion Detection Systems (IDS) to improve accuracy, precision, recall, and F1-score.

The unique hybrid architecture intrusion detection system that combines Gated Recurrent Units (GRU) and Deep Belief Networks (DBN) is a significant contribution presented in this research. In order to provide a complete network security solution that captures both temporal dependencies and structural characteristics, this special combination makes use of DBN's hierarchical feature learning and GRU's sequential pattern understanding. In order to improve data quality for security-related assessments, the study uses data pre-processing techniques such binary encoding and normalisation. An objective dataset is used to assess the robustness of the intrusion detection model through a thorough training and optimisation procedure that includes hyperparameter tuning, regularisation, and backpropagation.

The arrangement of the remaining content is as follows. The literature on different approaches of data protection and information security is illustrated in Section 2. The suggested method for protecting data and information security is covered in Section 3. The suggested method's design specification is provided in Section 4. Data on the use of the suggested approach is provided in Section 5. In Section 6, the effectiveness of the approach is compared to earlier approaches, and the performance metrics are illustrated along with a summary of the findings. The final section provides an overview of the findings and subsequent initiatives.

2 Literature Survey

Within the field of data protection and information security, recent studies have investigated how contextual elements and machine learning collaborate to influence the opinions of individuals of their security skills. In one research, workers at a multinational pharmaceutical business were surveyed. Machine learning techniques were used to categorize the participants according to the chance that they would demonstrate insecurity in their security expertise. In a

different study, the critical issue of protecting personal data in the big data and Internet of Things age was examined. A machine learning model was suggested as an approach of identifying documents that contain sensitive data. Furthermore, the intersection of blockchain and machine learning technologies has been explored, highlighting its cooperative potential for ensuring data security while promoting data exchange. The use of transfer learning models has also increased, especially in addressing issues like protecting trained models using secret key security and overcoming data shortages in deep learning-based anomaly detection. In addition, methods have been suggested to protect privacy in multi-party learning environments. Together, these connected works add to the changing field of data protection and information security by offering creative answers to problems brought on by shifting technological landscapes and a variety of contextual factors.

2.1 Machine learning Models in Information Security and Data Protection

This study looks at the problem of workers overstating their abilities despite greater resources being spent on workforce security education. The research uses machine learning to classify people according to their tendency towards over-optimism by polling more than 5,000 workers of a multinational pharmaceutical business. Important elements for improving awareness campaigns included employment experience, team size, salary range, and training commitment. According to (Frank et al, 2023), the study's application might be restricted to the pharmaceutical firm's particular organizational context. The study creates a machine learning model to effectively recognize documents containing personal information in the context of big data and linked devices, improving data security. Even while the accuracy of several neural network models is assessed, their generalizability may be limited by their dependence on a dataset from a particular area (Lin et al, 2020).

The combination of blockchain and machine learning is also explored in the study, demonstrating how the two technologies may work together to safely manage and exchange enormous volumes of data. The combination of machine learning's evaluation capabilities and blockchain's decentralized and secure nature makes it possible to develop important data from many sources and create real-time forecasting algorithms. When implementing machine learning algorithms, it is important to consider the constraints of smart contracts in handling sophisticated logic, as noted by (Diwan et al, 2022).

2.2 Transfer learning Models in Information Security and Data Protection

The lack of training data is one of the main issues in deep learning-based network anomaly detection that are discussed in this research. The study suggests a novel solution that combines federated learning with transfer learning to address this problem. During the federated learning phase, users exchange basic data from their training sets, which improves the detection system's performance for a particular assault. In the second learning stage, transfer learning is used to reconstruct and retrain the algorithm. Experiments conducted on the UNSW-NB15 dataset show that this strategy works well, outperforming other baseline approaches when training data is limited. But the strategy's effectiveness depends on the availability of participants with similar training responsibilities, which presents difficulties when there are different or unusual assault types (Zhao et al, 2020). The study also discusses the use of a secret key to protect taught algorithms. The suggested technique uses transfer learning to construct a secure approach by using a small portion of a training set. To generate learnable changed images for algorithmic fine-tuning, the secret key is employed in combination with encryption. Resilience against key estimation assaults is demonstrated by simulations conducted using the ImageNet

dataset, which show that the accuracy of the secured system dramatically drops in the absence of the correct key. Nonetheless, the protection mechanism's efficacy might be impacted by the secret key's length and complexity (AprilPyone & Kiya, 2021). The research also presents a transfer learning method to handle another factor shift in federated learning, allowing numerous parties to collaborate without sharing raw data. Homomorphic cryptography and secret sharing techniques are used by the suggested end-to-end, privacy-preserving multi-party learning strategy to connect the dissimilar characteristic spaces of different information consumers. Hospital mortality forecasting is used to illustrate the method's scalability, security, and effectiveness. Its application is limited in situations where characteristic spaces are entirely disconnected, as it is predicated on the premise that data producers have homogeneous characteristic spaces that overlap (Gao et al, 2019).

2.3 Information, Cyber, Network Attacks

Information, Cyber, Network Attacks: Cyber and information system attacks have a significant impact on system requirements, including the vital concepts of availability, confidentiality, and integrity. Intellectual property breaches, service quality deviations, trespassing or criminal activity, natural disasters, human error or failure, social engineering, information extortion, sabotage or theft, software attacks, technical software or hardware failures or errors and advances in technology are some of the threat categories. These worries are expanded by cyberattacks to include cyber-physical production systems (CPPS), where scenarios involving significant harm, like data alteration, packet dropouts, and the theft of encryption keys and sensitive data, are possible. worm attacks that introduce malicious code at the application layer, sinkhole attacks that interfere with network routing, and malicious node injection attacks that take advantage of hidden node vulnerabilities are a few notable instances. Network security is also subject to active attacks, in which hackers interfere with regular network operations, and passive attacks, in which hackers intercept data. This covers a variety of targeted assaults, each with the potential to alter data, drop packets, or capture confidential information. Examples of these attacks include malicious node injection, worm, and side channel attacks (Alkhudhayr, et al., 2019).Furthermore, a large portion of network security vulnerabilities are caused by human activities, such as visiting malicious websites or downloading malicious files, falling for unsolicited emails, and failing to update antivirus software (Mohan V. Pawar a, 2015).

Security Requirements: The authors examine the cyber security protocols of the Indian government, including the National Informatics Centre (NIC), the Indian Computer Emergency Response Team, and the National Information Security Assurance Programme (NISAP), in order to give security solutions for the cyber system described in (Engg., et al., 2016).

They also offer the following suggestions for cyber security: (1) Adopt a security and assurance policy. (2) As soon as feasible, malicious software should be identified and removed. (3) Provide a range of activities, including workshops and security drills. (4) Enhancements to cyber security expertise through conducting (workshops, research projects, and gatherings). Today’s computing generation is primarily concerned with network security because there are an increasing number of different forms of assaults. Protecting the system's tangible and nontangible objects from unauthorised access and modification from both internal and external sources is a crucial aspect of network security. Tangible objects include the hardware resources of the system, while intangible objects include the information and data stored in the system, both in transition and static states. One way to safeguard hardware resources is to protect: (1) End user items, such as the hardware components of the user interface (keyboard, mouse,

touchscreen, etc.). (2) Network devices, such as hubs, firewalls, switches, routers, and gateways. (3) Network communication channels designed to stop network communications from being intercepted by observers. Safeguarding software resources encompasses safeguarding operating systems, browsers, hardware-based applications, server protocols, and so forth. Although the information describes several cyberthreats and attacks, it does not address the precise ways to prevent privacy violations and data leaks, nor does it go into detail about the implications of the risks or provide countermeasures.

2.4 Information Security Systems Based on the AI and Machine Learning

It is evident that system capabilities in data gathering, processing, and utilization are evolving and eventually heading towards total independence. Although it is currently beyond the reach of technology, autonomous intelligence is expected in the future. As an aspect of artificial intelligence, machine learning uses mathematical models to evaluate input datasets so that algorithms may find patterns, anticipate outcomes, and learn from their mistakes. Regression, classification, clustering, anomaly detection, and size reduction are typical tasks. Inspired by biological processes, neural networks are made up of networked neurons that could analyze, remember, and replicate data. Using multilayer networks trained on large datasets, deep learning combines machine learning and neural networks to translate and transport information between layers for tasks like recognition, prediction, and classification. The paper also explains the various benefits that machine learning brings to the improvement of cybersecurity protocols. Its capacity for large-scale data analysis exceeds that of human analysts who depend on logic rules. With the help of manually created rules, machine learning allows exact data slicing by taking thousands of signals into consideration. Also, by utilizing computational power to react to threats in a matter of seconds, it guarantees faster responses. Machine learning's flexibility is essential since it goes beyond predetermined algorithms and makes judgements through "thinking," which makes it difficult for hackers to get around setup restrictions. Machine learning makes it possible to predict new hazards by recognizing possible risks based on previous occurrences, even when parameters are changed. All things considered; machine learning proves to be a useful tool for strengthening cybersecurity measures. (Tsareva & Voronova, 2022). Although the suggested solution emphasises how machine learning might improve cybersecurity, it doesn't include detailed instructions on how to lower the risk of data leaks, privacy violations, and human error in IT systems.

3 Research Methodology

3.1 Survey Overview

A survey on information security procedures in the IT sector, which included experts from a range of countries and areas , indicating that human error is well-known. All occupational backgrounds have noticeable differences in awareness, nevertheless. Regarding incident reporting, password and access control, and policy adherence in particular, some participants show a lack of awareness. To strengthen defences against emerging cyber threats, the findings highlight the critical need for focused awareness programmes and ongoing education.

3.2 Proposed Architecture Design

Using the extensively used NSL-KDD99 dataset for security intrusion detection system benchmarking, the technique initiates gathering information. This dataset provides a well-documented and often updated set of characteristics, including protocol categories, flags, and network-related statistics. It was inspired by the KDD'99 Cup. The dataset is appropriate for assessing intrusion detection systems because of its 'class' characteristic, which differentiates between typical and unusual network traffic.

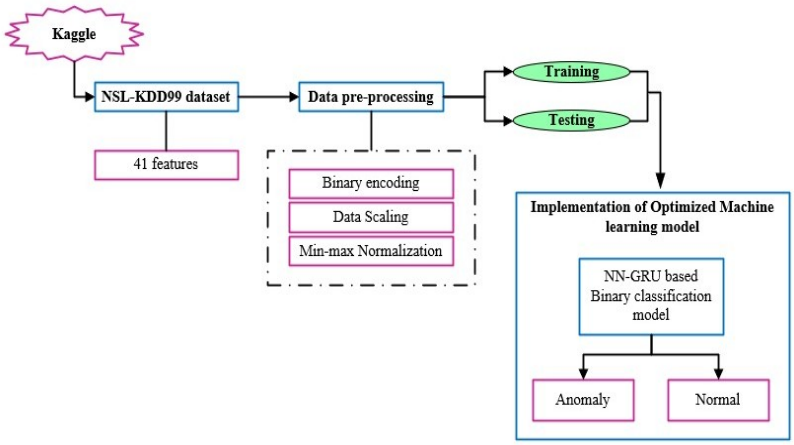

Figure 1: Architecture of the Suggested Model

The next phase is data pre-processing, which includes necessary procedures including binary encoding, information scaling, and Min-Max normalization to improve the information's quality and suitability for further security-related analysis. A comprehensive training and testing procedure, incorporating regularization and hyperparameter optimization, is required for generating an optimal machine learning framework. For binary categorization tasks in network security, the hybrid approach integrating Deep Belief Networks (DBNs) and Gated Recurrent Units (GRUs) is introduced. It provides a comprehensive solution by utilizing the sequential pattern recognition of GRUs and the hierarchical characteristic learning of DBNs. The design and functioning of the hybrid DBN-GRU framework is demonstrated. Utilizing back propagation over time, the method is trained to reduce the binary cross-entropy loss by modifying weights and biases. The model's efficacy is evaluated on an independent dataset, and the improved model demonstrates competence in categorizing incoming information as either abnormal or comparable to typical network activity, therefore establishing itself as an effective tool for detecting attacks inside network security. The general architecture of the suggested model is seen in Figure 1.

3.3 Data Collection

A structured questionnaire was used in a quantitative manner to assess participants' knowledge of information security procedures and the risks associated with human error. With regard to risks like privilege escalation and unauthorised data access, the research attempts to address loopholes and improve information security processes. Based on survey data, ongoing initiatives to raise IT personnel' understanding of information security are prioritised. In network security research, the NSL-KDD99 dataset is often used as a benchmark to assess

system efficacy. The 41-feature dataset, which was inspired by the KDD'99 Cup, offers a thorough representation of network traffic scenarios, facilitating the development and evaluation of intrusion detection systems. Some of the dataset's parameters, such "num_failed_logins","is_guest_login" and "num_file_creations," may point to human mistake inside cybersecurity procedures. This popular dataset, which is accessible on Kaggle, is used as a benchmark for assessing intrusion detection systems in the cybersecurity industry.(*NSL-KDD99 Dataset | Kaggle*, n.d.).

3.4 Data Pre-processing

An essential first step to obtain the initial information prepared to be processed for evaluation or modelling is data pre-processing. Information organization, transformation, and cleansing are all done within the framework of information security to improve the quality and fit of the information for activities associated with security. Making ensuring the information is in a format that machine learning algorithms, anomaly recognition systems, and other security measures can use to their full potential constitutes the objective. Data pre-processing is essential because it may improve the quality and dependability of security-related analysis by addressing problems like noise, inconsistencies, and changes in data.

3.4.1 Binary Encoding

A data pre-processing method used in information security is called binary encoding, which converts categorical information having two distinctive values ('C' and 'D') into binary formats (0 or 1). When producing categorical characteristics for machine learning methods, this strategy can be extremely beneficial. Giving 0 to the characteristic value that relates to 'A' and 1 to the characteristic value that belongs to 'B' provides the encoding value. The encoded value (E) can be stated mathematically as follows:

$$E = \#\begin{matrix} 0,\ if\ characteristics\ value\ is\ C \\ 1,\ if\ characteristics\ value\ is\ D \end{matrix} \quad (1)$$

The key component of binary encoding may be found in equation (1), which provides a simple but effective method to transform categorical information into a binary format that can be used for machine learning and information security.

3.4.2 Data scaling

Information security requires an essential pre-processing approach known as data scaling, particularly when using algorithms that are dependent upon the scale of the input characteristics. Data scaling is used to ensure that numerical characteristics have similar scales by standardizing them. Equation (2) is used to determine a feature's scaled value (S).

$$S = \frac{OV - min}{max - min} \quad (2)$$

The starting value of the characteristic is indicated by OV, its minimum and maximum values in the dataset are represented by min and max, respectively. In information security, scaling is essential for enabling consistent and objective assessments across a variety of

variables in the dataset. This mathematical derivation demonstrates the procedure of scaling, which converts numerical values into a standardized range.

3.4.3 Min-Max Normalization

The Min-Max Normalization approach is frequently utilized in the field of information security to scale numerical characteristic values within a specific range, typically between 0 and 1. Equation (3) provides the formula for Min-Max Normalization.

$$G_{out} = (G_{in} - Min)\frac{newMax - newMin}{Max - Min} + newMin \quad (3)$$

In Equation (3), *"G"* denotes the initial measurement position; min_{new} andmax_{new} stand for the values that are required for the standardized information; max_r andmin_r, for the maximum and minimum values, respectively. The main advantages of Min-Max normalization for managing many information points are its speed and efficacy. To provide more accurate and reliable analyses that increase the overall efficacy of security measures, these data pre-processing approaches together serve a critical role in improving the level of accuracy of input information for information security applications.

3.5 Implementation of Optimized Machine Learning Model

It takes precise training and testing steps to optimise a machine learning model for binary categorization. Using a selective and pre-processed dataset, the model is trained during the training phase. Regularisation techniques are used to prevent overfitting, optimisation techniques like stochastic gradient descent are implemented, and methods like grid or randomised search are used to change the hyperparameters. To improve category differentiating ability, the model seeks to minimise a selected loss function. To ensure resilience, cross-validation is frequently used during the testing phase, which assesses the model's performance on a different dataset. To attain the best possible generalisation to new, unidentified data, the model is iteratively improved depending on test outcomes. Hierarchical neural networks, or Deep Belief Networks (DBNs), are based on Multi-layered Restricted Boltzmann Machines (RBMs). From the input data, each RBM layer—which consists of visible and hidden units—extracts progressively abstract features. DBNs receive training layer by layer, with the network optimised for certain tasks such as binary classification through fine-tuning of the final layer's RBM. In pre-training RBMs, contrastive divergence is used to minimise the difference between observed and recreated data by modifying weights and biases. By identifying patterns and relationships, DBNs seek to decrease feature dimensionality while maintaining pertinent information, improving binary classification's discriminating abilities. Theoretical RBM training and tuning the DBN's parameters for efficient binary categorization are accomplished by stochastic gradient descent and labelled data.

Sequential interactions in data are captured by a particular kind of recurrent neural network (RNN), called Gated Recurrent Units (GRUs). GRUs solve some of the issues with conventional RNNs through the incorporation of gating mechanisms that allow them to actively update and forget data over time. GRUs are useful for circumstances in which the sequence of information points is crucial since they could symbolize sequential patterns and relationships in the setting of a binary categorization. The update and reset gates are included in the fundamental equations that control how a GRU operates. Let y_t be the input at time *t*, s_t the

update gate, h_t the reset gate, and r_t the hidden state at time *t*. Equation (4) computes the update gate.

$$s_t = \sigma(Z_s \cdot [r_{t-1}, y_t]) \quad (4)$$

Where, σ is the activation function of the sigmoid and Z_s is the weight matrix. Similarly, Equation (5) computes the reset gate as follows.

$$h_t = \sigma(Z_h \cdot [r_{t-1}, y_t]) \quad (5)$$

Equation (6) is then used to calculate the candidate hidden state $\bar{r}_t$.

$$\bar{r}_t = \tanh\,(Z_r \cdot [h_t \odot r_{t-1}, y_t] \quad (6)$$

Where, element-wise multiplication is indicated by ⊙. Equation (7) gives the candidate state, which is the result of combining the previously hidden state with the final hidden state.

$$r_t = (1 - s_t) \odot r_{t-1} + s_t \odot \bar{r}_t \quad (7)$$

The last hidden state r_t modifies a GRU for binary categorization by acting as input to a fully linked layer with sigmoid activation. For positive class membership, this layer produces a probability score (0 to 1). The difference between actual labels and expected probabilities is measured using binary cross-entropy loss. The complete network is trained using backpropagation over time, with weights and biases being adjusted. GRU hidden units, batch size, and learning rate are important hyperparameters. Overfitting is avoided using regularization and dropout techniques. To ensure model reliability for binary categorization, stochastic gradient descent optimizes parameters iteratively. Hyperparameters must be fine-tuned and adjusted based on the effectiveness of validation sets.

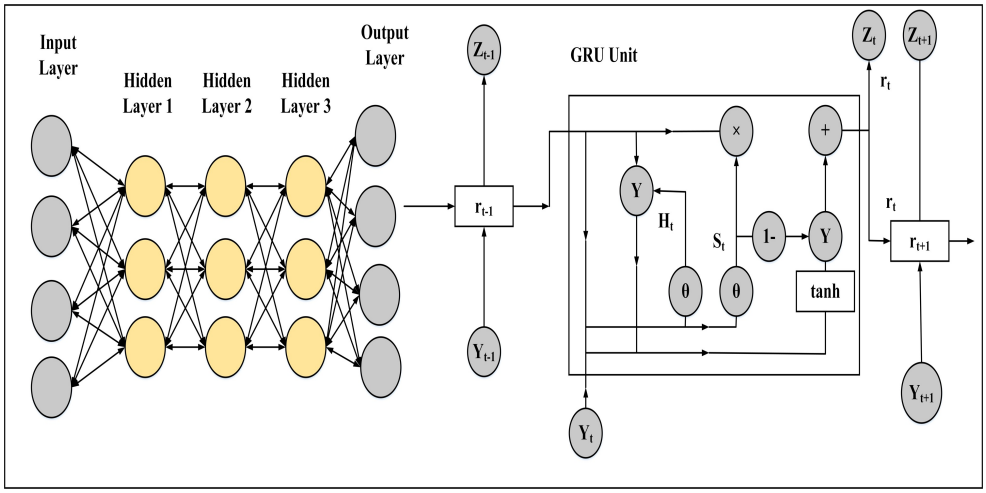

Figure 2: Structure of Hybrid NN-GRU for Binary Classification

The sequential pattern recognition of Gated Recurrent Units and the structured feature extraction of Deep Belief Networks are combined in the Hybrid NN-GRU Structure for Binary Classification. Using multiple-layered Restricted Boltzmann Machines to capture abstract properties, the DBN-GRU hybrid makes use of layer-wise pre-training. The final layer's RBM is modified for binary classification. The sequential linkages are captured by the GRU component, which manages sequential interactions. The hybrid uses the most recent hidden state of the GRU to get a probability estimate. Biases, modified weights, and backpropagation all lessen the loss of binary cross-entropy. Learning rate and batch size are important hyperparameters, and regularization improves outcomes. This hybrid model leverages the characteristics of both architectures for complete information modelling, and it performs exceptionally well in binary categorization, particularly in network security intrusion detection.

4 Design Specification

To improve security, the suggested intrusion detection method combines Deep Belief Networks (DBNs) with Gated Recurrent Units (GRUs) in a hybrid architecture. Hierarchical characteristic learning is facilitated by DBNs, which are machines composed of multiple-layered Restricted Boltzmann Machines (RBMs). RBMs optimise the final layer for binary categorization via layer-by-layer training, lowering dimensionality while maintaining crucial information. GRUs capture sequential interactions and solve problems with traditional RNNs. The benchmark dataset is the 41-character NSL-KDD99 dataset, and data quality is guaranteed by pre-processing techniques. Thorough layer-by-layer pre-training, backpropagation, and hyperparameter optimization for batch size and learning rate are applied to the hybrid DBN-GRU model. A binary categorization probability score is generated by the activation function. To ensure ideal generalization, testing entails evaluation on a different dataset. The model, which focuses on intrusion detection, distinguishes between normal and abnormal network.

5 Implementation

The survey identifies a mixed level of awareness and adherence to password and access management protocols. While some participants report high familiarity, others exhibit a need for improvement in this crucial area, emphasizing the importance of supporting password and access security practices. Professionals display a spectrum of familiarity with security awareness practices, with a notable percentage reporting high awareness. This diversity highlights the varying degrees of emphasis placed on security education within different professional environments. Incident reporting emerges as an area of concern for a subset of respondents, uncovering potential gaps in reporting mechanisms. This finding underscores the need for robust incident reporting systems to address and mitigate security incidents effectively. A diverse set of responses is observed regarding adherence to information security policies and procedures. While the survey provides valuable insights into the current state of information security practices, the research extends its scope to explore the broader landscape of challenges and influencing factors. The study delves into the pivotal role that efficient intrusion detection systems play in safeguarding systems from cyber-attacks. The research introduces an innovative intrusion detection method for detecting the risks of data breaches and privacy violations in IT systems based on hybrid DBN-GRU architecture. Leveraging the NSL-KDD99 dataset, the approach involves meticulous data pre-processing, binary encoding, data scaling, and Min-Max normalization to enhance data quality.

The NSL-KDD99 dataset will be used as a benchmark for the suggested intrusion detection system's implementation. The dataset, which includes features like protocol

classifications, flags, and network-related information, is regularly updated and has extensive documentation. Binary encoding, information scaling, and Min-Max normalization are examples of data pre-processing techniques that improve the quality of information for evaluation linked to security. DBN and GRU are integrated into a hybrid architecture that is used to implement the machine learning model. Regularization, hyperparameter optimization, and long-term back propagation are used in the training and testing stages. Python is used for developing and implementing machine learning algorithms; scikit-learn is used for data pre-processing and evaluation; and well-known libraries like TensorFlow and Keras are used for building and training neural network models. Effective intrusion detection is made possible by the suggested model's implementation, which recognizes temporal correlations and structural elements in network data.

6 Evaluation

The main conclusions of the study are thoroughly analysed in this section, with an emphasis on the consequences for practitioners and researchers. A significant finding in Figure 3 is brought to light by the poll, which compiles opinions from a wide range of IT specialists. Participants' answers to the Data Handling and Security question clearly show differences. A subset of respondents positively recognises awareness and adherence; however, a significant number of respondents negatively reply, suggesting a possible breach in data management procedures. This distribution, when visualised graphically, emphasises the necessity of focused efforts to promote data security standards. Resolving issues brought up by unfavourable comments calls for customised education or awareness efforts to guarantee thorough comprehension and adherence to reliable data handling and security protocols.

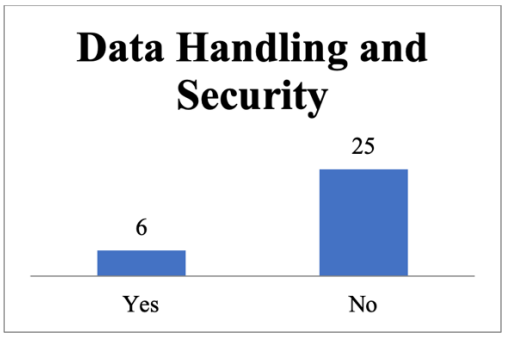

Figure 3: Data Handling and Security

Metrics are required for the assessment of effectiveness in the detection of anomalies. Accuracy measurement is the approach most often employed for this purpose. The number of testing datasets that a pretrained model correctly classifies for a particular dataset serves as a proxy for the model's accuracy. Because obtaining the most relevant conclusions will be impossible if the accuracy measure is the only one used. To assess the strategy's effectiveness, the researchers investigated additional factors. The following criteria were used to assess the effectiveness of the approach used: accuracy, recall, precision, and F1-score. The definitions of each metric are described as follows:

- The quantity of data that has been correctly identified is referred to as T_{Pos} (True Positive).
- F_{Pos} (False Positive) refers to the quantity of reliable data that was interpreted incorrectly.

- False negatives (F_{Ne*}) are situations in which incorrect data has been identified correctly.
- False information values are referred to as T_{Ne*} (True Negative), or erroneous information values.

6.1 Accuracy

Accuracy is used to assess the overall efficacy of the procedure's technique. In essence, it is the presumption that every occurrence will be precisely anticipated. Accuracy is given in Equation (8) (Zeeshan Ahmad, 2020).

$$Accuracy = \frac{T_{Pos}+T_{Neg}}{T_{Pos}+T_{Neg}+F_{Pos}+F_{Neg}} \quad (8)$$

6.2 Precision

Precision describes how comparable two or more calculations are to one another in addition to being accurate. The reliability with which an assessment may be made is demonstrated by the link between accuracy and precision. Equation (9) is frequently applied in precision calculations (Zeeshan Ahmad, 2020).

$$Precision = \frac{T_{Pos}}{T_{Pos}+F_{Pos}} \quad (9)$$

6.3 F1-Score

Accuracy and recall are combined in the F1-Score calculation. Equation (10) uses precision and recall calculating the F1-Score (Zeeshan Ahmad, 2020).

$$F1-score = \frac{2\times precision\times recall}{precision+recall} \quad (10)$$

6.4 Recall

The percentage of all acceptable results that the algorithms effectively sorted is known as recall. The right positive for these numbers is obtained by dividing the true negative values by the ratio of the real positives. It is referenced in Equation (11) (Zeeshan Ahmad, 2020).

$$Recall = \frac{T_{Pos}}{T_{Pos}+F_{Neg}} \quad (11)$$

6.5 AUC & ROC

AUC, or area under the ROC curve, is a prominent evaluation metric for binary categorization problems in deep learning and machine learning methods. The AUC is used to compute the area under the receiver operating characteristic (ROC) curve, a visual representation of the binary identification algorithm's efficacy. The classifier's goal in a binary identified problem is

to determine whether the given data belongs to a positive or negative category. Utilizing the ROC curve, the T_P to the F_P were compared according to various criteria. Greater efficiency is indicated by higher numbers on the AUC scale, which goes from 0 to 1. An entirely random predictor has an AUC of 0.5, whereas the optimal classifier has an AUC of one. Due to the algorithm's consideration of every possible classification level and production of a single value for contrasting the efficacy of different classifiers.

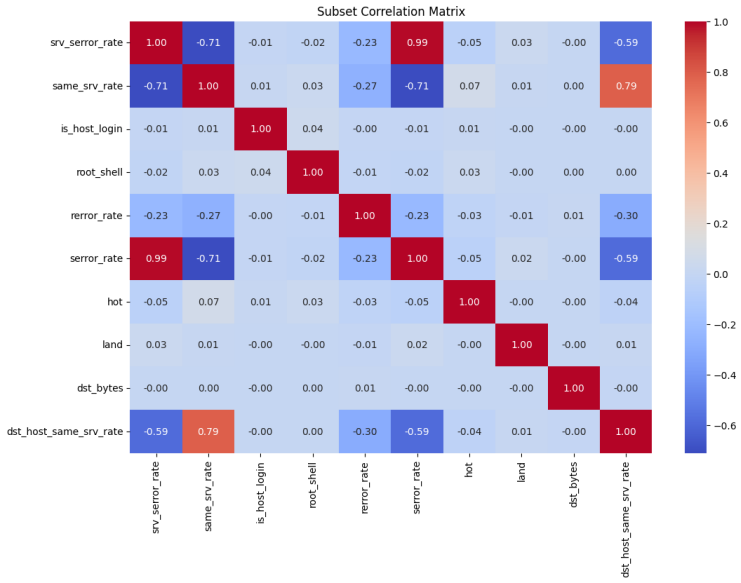

Figure 4: Subset Correlation Matrix

The Subset Correlation Matrix, which was created from ten randomly selected columns in the Data Frame, is shown in Figure 4. Each cell in this matrix represents the correlation coefficient, which is used to show dependencies and pairwise correlations between variables. The coefficient, which has a range of -1 to 1, represents the direction and intensity of associations. The heatmap's color-coded values improve readability, and the annotated matrix values provide quantitative measurements. Through the discovery of patterns and correlations within the numerical subset, this research sheds light on possible multicollinearity—the sharing of information between variables.

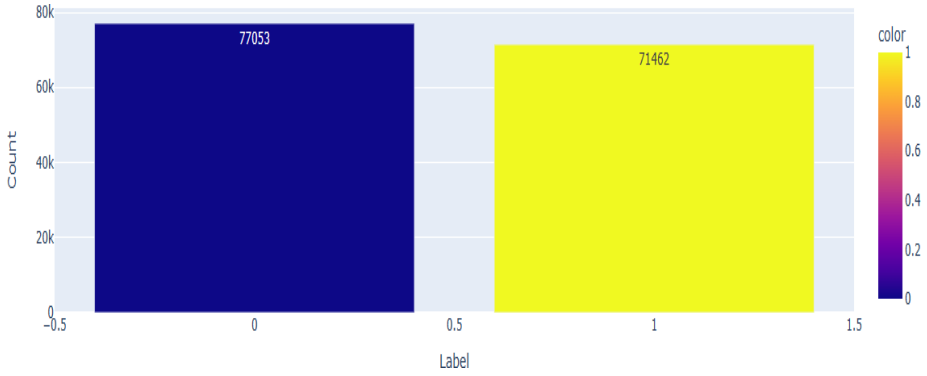

Figure 5: Distribution of Labels

Given in Figure 5, the Distribution of Labels graph shows the frequency of each label in the 'label' column of the concatenated data. The vertical axis shows the count or frequency of each label, while the horizontal bars relate to distinct labels. The distinct labels are distinguished from one another by the color distinction in the bars, which gives an accurate representation of how common they are. The bars' heights correspond to the corresponding numbers; longer bars denote a higher frequency of a certain label. This bar chart provides significant information into the relative representation of each label and is especially helpful for evaluating the class distribution and imbalance within the dataset.

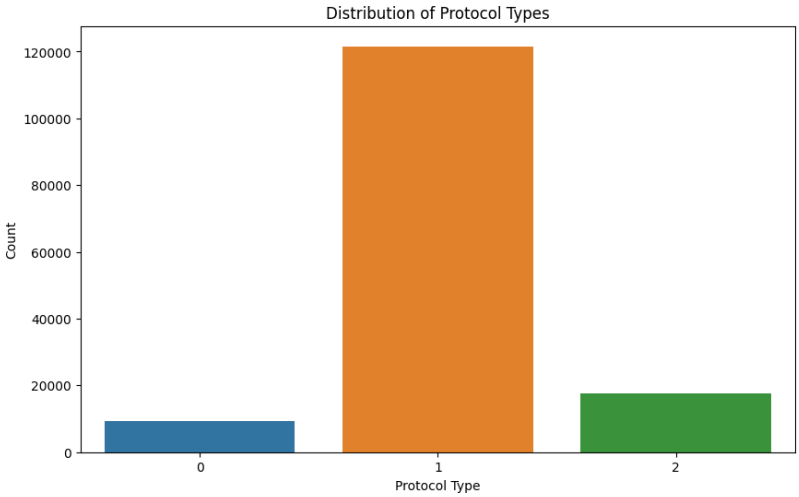

Figure 6: Distribution of Protocol Types

Figure 6 displays the Distribution of Protocol Types plot, which shows the frequency distribution of various protocol types found in the combined information. The horizontal axis denotes different protocol kinds, and the vertical axis shows the percentage of instances or occurrence of a particular protocol type. The distinct bar heights in the plot indicate the number of instances of the numerous protocols in the dataset. This visualization is useful for learning about the relative representation of various communication protocols.

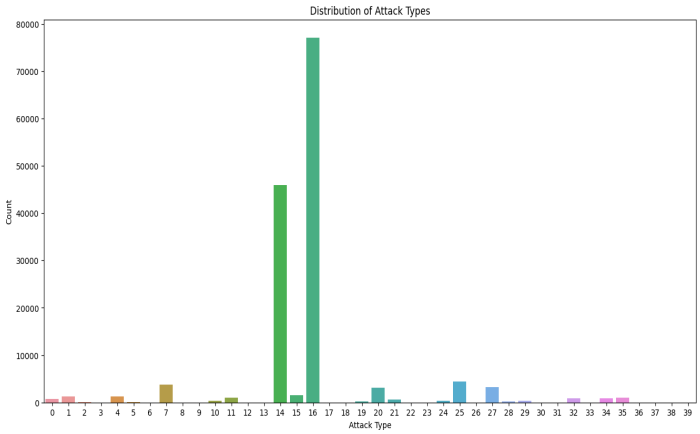

Figure 7: Distribution of Attack Types

The Distribution of Attack Categories, seen in Figure 7, illustrates how different types of attacks show themselves in the aggregated data. The vertical axis shows the number or frequency of each assault type, while each bar on the horizontal axis refers to a specific kind of attack. The distribution of assaults throughout the dataset is clearly shown by the bars' varied

heights. Understanding the frequency of various assault kinds and observing any imbalances or trends in the information depend significantly on this depiction.

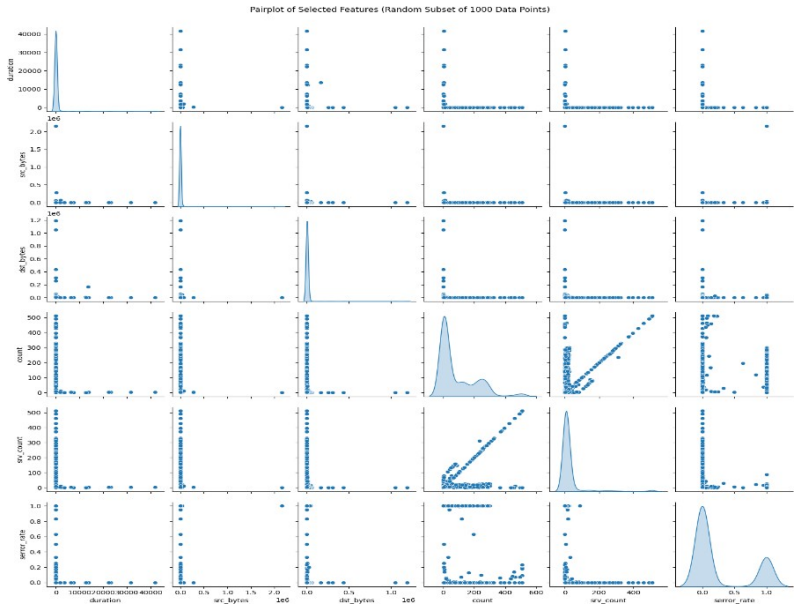

Figure 8: Pairplot of Selected Features

Figure 8 shows the Pairplot of Selected characteristics graph, which offers an extensive visual investigation of the distributions and interactions among a subset of characteristics within the overall information. In particular, a subset of 1000 points of information from the dataset is chosen at random to create the pairplot. Plots of the chosen features—"duration," "src_bytes," "dst_bytes," "count," "srv_count," and "serror_rate"—against one another in a variety of combinations. The diagonal panels provide information on the single-variable distributions of each characteristic by displaying kernel density estimations for every distinct characteristic. In the meanwhile, bivariate connections between pairs of characteristics are displayed in the scatterplots in the bottom and upper triangles, where the data points are represented by markers. Exploratory data analysis can be aided by this visualization's ability to spot trends, correlations, or possible outliers within the chosen subset of characteristics. The pairplot is a useful tool for analysts to identify patterns, evaluate the distribution of values, and develop a visual comprehension of how various factors interact.

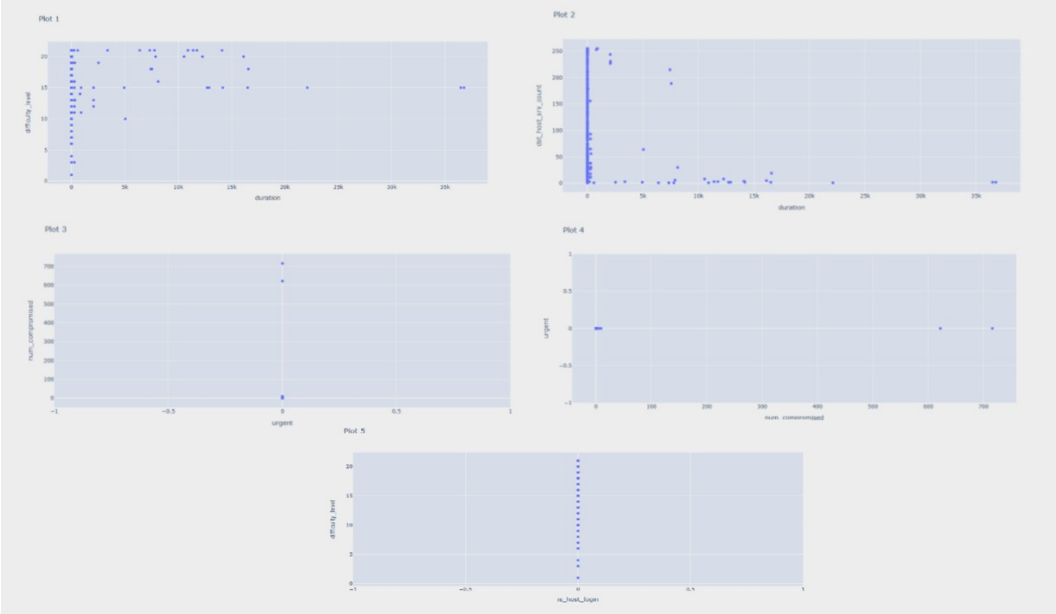

Figure 9: Data Analysis by Randomly Selecting 1000 Data Points

Using 5 scatter plots with 1000 randomly chosen points from the concatenated dataset, Figure 9 presents a qualitative analysis. Each dynamic scatter plot illustrates the relationship between two randomly selected columns using Plotly Express. For evaluation, the "sample_df" DataFrame guarantees a consistent subset. The looping procedure, which is based on the "unique_columns_list," produces a variety of scatter plots that allow for the visual analysis of trends, correlations, or anomalies. To help analysts grasp data linkages, this method provides a dynamic study of possible links between different column pairs in the dataset.

Table 1: **Performance metrics of the Suggested Method are Compared with those of Existing Methods**

Methods	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1Score (%)**
Random Forest (Kumar et al, 2022)	89	87	87.5	87
SVM (Koroniotis et al, 2018)	92	91.6	91.4	91.4
GNB (Panda et al, 2021)	94	93	93	93
Proposed Method	98.92	99	99	99

A comprehensive examination of performance metrics between the recommended technique and the current methods such as Random Forest, SVM, and GNB (Gaussian Naive Bayes) is given in Table 1. Accuracy, Precision, Recall, and F1 Score are among the metrics that were assessed; the results are displayed as percentages. With an outstanding accuracy of 98.92%, the suggested strategy performs much better than the current approaches. The suggested approach also shows outstanding outcomes in terms of Precision, Recall, and F1 Score metrics, which are all consistently at 99%. These metrics demonstrate high precision in correctly recognizing positive cases, robust recall in preserving accurate positive circumstances, and a balanced F1 Score that requires both precision and recall into

consideration. Conversely, the current approaches show outstanding results but generally show significantly lower metrics. This table illustrates the advantages of the proposed method above existing procedures, highlighting its possibilities as a sophisticated and extremely accurate strategy for the problem at hand.

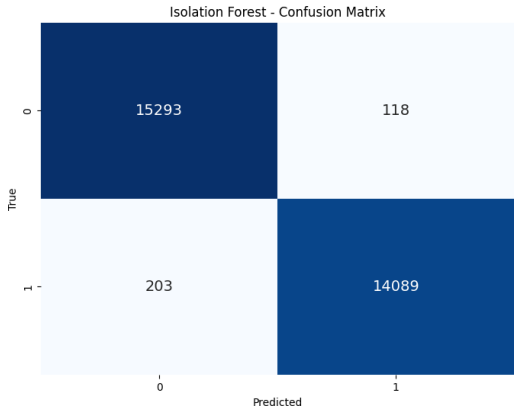

Figure 10: Isolation Forest- Confusion Matrix

To evaluate an Isolation Forest model's performance, Figure 10 generates and displays a confusion matrix. The test set is subjected to the confusion matrix function, and the outcome is shown as a heatmap. True positives, true negatives, false positives, and false negatives all have been prominently displayed in the color-coded matrix. The compatible numbers are displayed in the annotations of each cell, which facilitates the evaluation of the model's accuracy and error kinds.

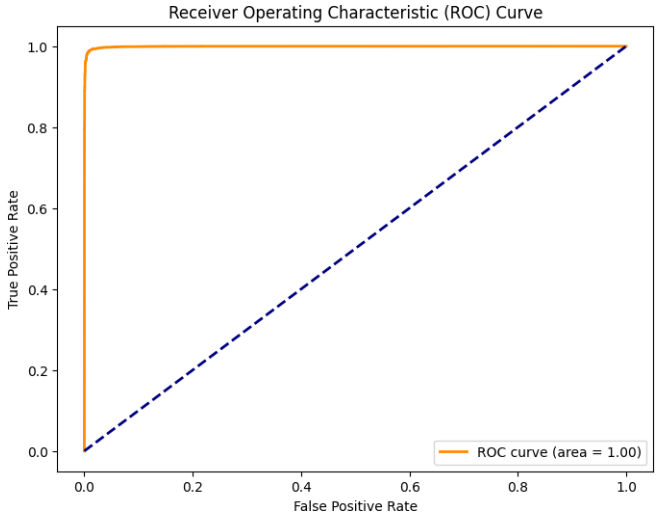

Figure 11: ROC Curve

To evaluate the effectiveness of a binary categorization model, probably developed from a machine learning algorithm, figure 11 creates a ROC curve. A graphical depiction of the trade-off between the true positive rate and the false positive rate across a range of threshold values is called a ROC curve. The projections of the model and the true labels are used by the roc_curve function to calculate the false positive rate, true positive rate, and associated thresholds. The final curve, on which the AUC was computed, represented the capacity for discrimination of the framework.

6.6 Discussion

In a quantitative study of IT professionals' knowledge and understanding of information security, 28 participants disclosed serious gaps in their knowledge and comprehension of data protection and information security. The hybrid DBN-GRU model, which is based on the NSL-KDD99 dataset, the intrusion detection system (IDS) is recommended as a proposed solution to detect them accurately. This model outperformed well-known techniques such as Random Forest, SVM, and GNB, with a 98.92% accuracy rate. Recall, F1-score, and precision were all very high, which is essential for successful intrusion detection. Confusion matrices and ROC curves, among other visualizations, offered thorough insights into the benefits of the model and demonstrated its status as a highly developed and accurate intrusion detection system.

7 Conclusion and Future Work

Using the NSL-KDD99 dataset as a standard, this study concludes by introducing an effective intrusion detection system that can be a valuable measure to reduce and detect the risks of privacy violations, data leaks and anomalous network activity in IT systems built on a hybrid DBN-GRU design to detect them with an accuracy rate of 98.92%, the suggested model is effective in classifying activities as normal or abnormal. The hybrid technique provides a complete solution for modelling complex information relationships in data by combining the advantages of DBNs and GRUs. Python is used in the implementation, which guarantees both scalability and effectiveness. The efficacy of the suggested approach not only handles intrusion detection issues but also provides a useful instrument for augmenting network security. To improve the model's capacity for generalization, future research initiatives may focus on refining hyperparameters and investigating new regularization strategies. Furthermore, broadening the assessment to encompass a range of datasets and authentic network conditions would confirm the model's suitability for a multitude of scenarios. Furthermore, examining the model's resilience to adversarial assaults and developing interpretability techniques to improve the decision-making procedure's transparency may benefit the intrusion detection connection throughout its entirety. The suggested methodology can be easily included into useful cybersecurity frameworks through business partnerships, confirming its applicability in actual situations.

References

Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data privacy preservation and security in smart metering systems. *Energies*, *15*(19), 7419.

William, P., Yogeesh, N., Vimala, S., Gite, P., & others. (2022). Blockchain technology for data privacy using contract mechanism for 5G networks. *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, 461–465.

Prabhakar, P., Arora, S., Khosla, A., Beniwal, R. K., Arthur, M. N., Arias-Gonzáles, J. L., Areche, F. O., & others. (2022). Cyber Security of Smart Metering Infrastructure Using Median Absolute Deviation Methodology. *Security and Communication Networks*, *2022*.

Tsao, K.-Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894.

Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.

Zhang, X., Zhang, W., Sun, W., Sun, X., & Jha, S. K. (2022). A Robust 3-D Medical Watermarking Based on Wavelet Transform for Data Protection. *Computer Systems Science & Engineering*, *41*(3).

Kanade, S., Petrovska-Delacrétaz, D., & Dorizzi, B. (2022). *Enhancing information security and privacy by combining biometrics with cryptography*. Springer Nature.
Alshurideh, M., Alquqa, E., Alzoubi, H., Kurdi, B., & Hamadneh, S. (2023). The effect of information security on e-supply chain in the UAE logistics and distribution industry. *Uncertain Supply Chain Management*, *11*(1), 145–152.

Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., Osamor, J., & Hamdi, M. (2022). A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. *Computers and Electrical Engineering*, *102*, 108205.

Jakka, G., Yathiraju, N., & Ansari, M. F. (2022). Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology*, *6*(3), 6156–6165.

Frank, M., Jaeger, L., & Ranft, L. M. (2023). Using contextual factors to predict information security overconfidence: A machine learning approach. *Computers & Security*, *125*, 103046.

Lin, C.-H., Yang, P.-K., & Lin, Y.-C. (2020). Detecting security breaches in personal data protection with machine learning. *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 1–7.

Diwan, P., Khandelwal, B., & Dewangan, B. K. (2022). Ensuring Data Protection Using Machine Learning Integrating with Blockchain Technology. *International Conference on Innovations in Computer Science and Engineering*, 359–368.

Zhao, Y., Chen, J., Guo, Q., Teng, J., & Wu, D. (2020). Network anomaly detection using federated learning and transfer learning. *International Conference on Security and Privacy in Digital Economy*, 219–231.

AprilPyone, M., & Kiya, H. (2021). Transfer learning-based model protection with secret key. *2021 IEEE International Conference on Image Processing (ICIP)*, 3877–3881.

Gao, D., Liu, Y., Huang, A., Ju, C., Yu, H., & Yang, Q. (2019). Privacy-preserving heterogeneous federated transfer learning. *2019 IEEE International Conference on Big Data (Big Data)*, 2552–2559.

Fatimah Alkhudhayr IT Department, Q. U. Q. S. A., Alfarraj, S., Aljameeli, B. & Elkhdiri, S., 2019. *Information Security:A Review of Information Security Issues and Techniques ,* Saudi Arabia: IEEE.

Mohan V. Pawar a, J. A. b., 2015. *Network Security and Types of Attacks in Network,* Odisha: ScienceDirect.

Engg., S. R. K. C. S. &., Yadav, S. A., Sharma, S. & Singh, A., 2016. *Recommendations for effective cyber security execution ,* Noida: IEEE.

Tsareva, P. E. & Voronova, A. V., 2022. *Information Security Systems Based on the AI and Machine Learning ,* Saint Petersburg, Russian: IEEE.

NSL-KDD99 Dataset | Kaggle. (n.d.). Retrieved December 2, 2023, from https://www.kaggle.com/datasets/kaggleprollc/nsl-kdd99-dataset
Zeeshan Ahmad, A. S. K. C. W. S. J. A. F. A., 2020. *Network intrusion detection system: A systematic study of machine learning and deep learning approaches ,* Malaysia: WILEY.

Kumar, A., Shridhar, M., Swaminathan, S., & Lim, T. J. (2022). Machine learning-based early detection of IoT botnets using network-edge traffic. Computers & Security, 117, 102693.

Koroniotis, N., Moustafa, N., Sitnikova, E., & Slay, J. (2018). Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. *Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings 9*, 30–44

Panda, M., Abd Allah, A. M., & Hassanien, A. E. (2021). Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber attacks. *IEEE Access*, *9*, 91038–91052.