Contents

[Cyber Insecurity 2](#_Toc110245025)

[Incidence Detection and Response 2](#_Toc110245026)

[Goal 3](#_Toc110245027)

[Related Studies 4](#_Toc110245028)

[Information Privacy 4](#_Toc110245029)

[SQL Injections 5](#_Toc110245030)

[Deep Learning and Cyber Security 5](#_Toc110245031)

[Deep Learning Process 5](#_Toc110245032)

[Analysis Approaches 7](#_Toc110245033)

[Data 7](#_Toc110245034)

[Data Preprocessing 7](#_Toc110245035)

[Deep Learning Models 8](#_Toc110245036)

[Model Validation 8](#_Toc110245037)

[Findings 9](#_Toc110245038)

[Conclusion 11](#_Toc110245039)

[Study Limitations and Future Studies 11](#_Toc110245040)

[References 12](#_Toc110245041)

# Cyber Insecurity

In 2021, the cost of a data breach was approximately USD 4.24 million which is a 10% increase from USD 3.86 million that was incurred in 2020 (IBM Security, 2021). In 2022, the global average cost of cyber-attacks is forecasted to peak at 6 trillion dollars and rise to 10.5 trillion in 2025 (Ireland, 2022). According to Tunggal & Sen (2022), most of the reported cases are related to compromised credentials which constituted 20% of all the data breaches in 2021. Compromised credentials were mainly obtained through (1) Business Email Compromise (BEC) - $5.01 million, (2) Phishing - $4.65 million, (3) Malicious insiders - $ 4.61 million, and (4) Social engineering - $4.47 million (Tunggal & Sen, 2022).

Almost every system being used today faces the threat of cyberattacks, necessitating that the architecture of the system allows the integration of security features and functions as key components of the underlying system (Borky & Bradley, 2018). In their study on information security, Borky & Bradley (2018) argue that systems with many users, those that are stationed in geographically distributed locations, as well as those with networked access are especially vulnerable.

Based on the preceding observations, it is relatively safe to argue that the cost of cyber-attacks is too high to be ignored. The question however is, which methods are appropriate for detecting and preventing cyber-attacks?

## Incidence Detection and Response

Incidence detection and response is the key aspect of cybersecurity for organizations that use IT and in particular, those that depend on cloud infrastructure. Essentially, devoid of the ability to notice network intruders or other malicious opponents, IT security analysts can not adopt an effective response to security events or appropriately mitigate the resulting damage (Vishalini, et al., 2016).

#### Data and Cyber Security

Various methods have been proposed in the never-ending battle to subdue criminals, hackers, terrorists, foreign intelligence services, and deranged individuals who obtain perverse gratification from releasing viruses, trojans, worms, etcetera into computer systems. Some of the methods include machine learning, evolutionary algorithms, and statistical approaches (Ibor, et al., 2018).

## Goal

Deep learning also identified as Deep Neural Networks (DNN) consists of machine learning techniques that allow the corresponding network model to learn from both supervised and unsupervised data and generate predictions and solutions to complex problems (Dixit & Silakari, 2021). The current study proposes a deep learning-based approach to detecting cyber-attacks i.e., long short-term memory (LSTM). In particular, the study seeks to examine the applicability of various deep learning models in detecting a potential SQL injection.

To address the research objective, the following question is expected to be answered:

1. What is the applicability of deep learning models in predicting an incident of SQL injections in a web server?

Ideally, optimally performing models based on the general characteristics of the user activities will be considered applicable in the detection of SQL injections.

# Related Studies

## Information Privacy

Privacy is a central concept in the various aspects of cyber security. Tobin (2021) defines information/data privacy as the handling of critical personal information, such as "personally identifiable information" (PII) as well as "personal health information" (PHI). Such information includes but is not limited to social security numbers, health records, and financial data, including bank account and credit card numbers. This definition is supported by (Crocetti, et al., 2021) who define data privacy as the process of safeguarding important information from corruption, compromise, or loss. Primarily, the lack of access control regarding personal information can put individuals at risk for fraud and identity theft (Tobin, 2021). One of the most adopted methods for protecting private information is authentication (Maayan, 2022). In a report published in (TechWeb, 2021) on authentication methods for servers, it is noted that during authentication, the user or computer has to prove its identity to the server or client.

Various methodologies have been proposed for server authentication including passwords and biometric methods. In most cases, authentication by a server comprises the use of a user name and password (TechWeb, 2021). Biometric authentication can also be used for server access through the use of cards, retina scans, voice recognition, and fingerprints among other physical features of an individual (Rountree, 2013). Other tools for authentication are multi-factor authentication, certificate-based authentication, and token-based authentication (Maayan, 2022).

While there are various authentication methods for web applications, SQL injection is one of the main threats to web application security. During SQL injection attacks, perpetrators attempt to obtain unauthorized access to the database, which harbors vital and private information of the application users.

### SQL Injections

The main usage of SQL is to work with data in the database so that the data can be manipulated by interacting with SQL in the database. So that the intruders use malicious SQL queries to steal sensitive information from the database server which is executed over a web-based application. Most databases and especially those in the banking, finance industry, health care, and employee information constitute the most targeted vulnerable web-based application attacks. There are various types of attacks ranging from String SQL Injection, Numeric SQL Injection, Comments attack, Blind SQL injection, Timing attacks, to Command union SQL Injection (Shobana, et al., 2021).

## Deep Learning and Cyber Security

Regarding the question of solving cyber security challenges, Choi, et al. (2020) observe that deep learning could potentially overcome the challenges faced by machine learning algorithms including the need for extensive feature engineering. Besides, some deep learning algorithms tend to attain relatively high classification accuracy with minimum domain knowledge (Choi, et al., 2020).

Deep learning models like Convolutional Neural Network (CNN), Auto Encoder (AE), Deep Belief Network (DBN), Recurrent Neural Network (RNN), Generative Adversal Network (GAN) as well as Deep Reinforcement Learning (DIL) have been proposed in the application of cyber security (Dixit & Silakari, 2021).

### Deep Learning Process

The deep learning process as described by (Choi, et al., 2020) follows four main steps including the collection of raw data, data preprocessing, representation learning, and classifier learning (*see figure 1*).

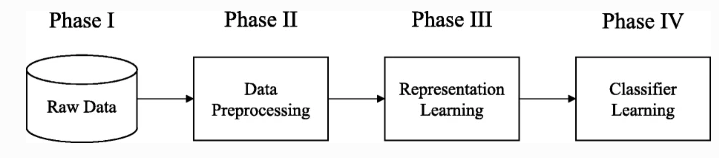


Figure 1: General deep learning process, source: [www.cybersecurity.springeropen.com/](https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00055-5/figures/1)

According to (Choi, et al., 2020), in phase 1, relevant raw data is obtained from the storage repository. The raw data includes uniquely identified events that are set to be used as either input, target, or excluded features during modeling. Both phases II and III seek to extract and create a representation of useful information that is contained in the raw data except that phase III is dedicated toward representation learning i.e., using processes such as extracting text patterns from data while phase II is dedicated to information extraction and data processing operations such as data merging, data cleaning, aggregation which is not representation learning. Phase IV is concerned with building classifiers and other predictors using deep learning models.

(Jothi, et al., 2021) used a multilayer perceptron (MLP) model to detect SQL injections and, attained a cross-validated accuracy of 98% with a precision of 98% and recall of 97%. Other studies have been conducted that apply deep learning techniques in detecting SQL injections. (Zhang, et al., 2022) propose a multi-hidden layer DNN model with ReLU function i.e., the LSTM model which achieved a classification accuracy of 96%. According to (Zhang, et al., 2022), the LSTM model solves the problem of overfitting that is encountered in traditional machine learning algorithms. Hassan, et al. (2021) compare the performance of Support Vector Machines (SVMs) and Random Forest (RF) models with deep learning-based methods. The SVM and RF models attain a classification accuracy of approximately 97.33% while the deep learning model attained a classification accuracy of 98.04%.

# Analysis Approaches

The current study adopted the deep learning implementation approach proposed by (Choi, et al., 2020) as shown in figure 1.

## Data

Since the objective is to propose a deep learning model that detects whether an event is an SQL injection or an authentic request, historical data related to SQL queries were obtained. Table 1 below provides an overview of the general characteristics of the raw data.

Table 1: General data characteristics

|  |  |
| --- | --- |
| Data Question | Response |
| Source of the data | The data was collected from Kaggle and can be accessed through the following link:  <https://www.kaggle.com/competitions/wallarm-ml-hackathon/data> |
| Number of variables | Variables = 3 with 1 input (text) feature where the input variable is textual, target variable, and ID variable.  Injection (target) = two class labels—left and not left, labeled 1 and 0 respectively.  Missing observations = there are no missing observations in the data |
| Number of observations | 65,854 |

### Data Preprocessing

Data used was originally stored in separate files. The original approach was to combine the target and the feature input using the *ID* attribute during the data preprocessing phase. During initial data exploration, it was observed that the text attribute which contained the SQL statements that were executed by users contained entries with no semantic structure. Therefore, the statements were preprocessed using character-level tokenization during which 10 additional features were generated. Character-level tokenization was conducted during representation learning.

## Deep Learning Models

The LSTM model was proposed using a varying number of parameters and *ReLu*, *Tanh*, and *Linear* activations. In this case, the objective is to determine the effect of the number of parameters and type of activation on the performance of the DNN model. Besides, an MLP model was implemented which is a neural network model that consists of multiple layers of nodes that are fully connected to the subsequent nodes.

### Model Validation

The preprocessed data were split into train and test sets using a 70:30 ratio. Subsequently, the train data were used for training the models while the test data was used for model evaluation. During the model evaluation process, the classification accuracy of each of the models was computed and used for comparison of the effectiveness of the models to predict potential SQL injections.

# Findings

#### Common entries in the SQL Statements

Figure 2 below provides an overview of the commonly used entries in the SQL injections. As noted, some of the sensible entries are ‘*select’* and ‘*union’*.



Figure 2: Common entries

Essentially, the SELECT statement is passed when a user wants to select data from a database. The resulting data is the result-set. On the other hand, the UNION statement is used to combine the result-set of two or more SELECT statements. Therefore, it can be assumed that most of the queries are related to database manipulation.

#### Model Performance

The DNN models were evaluated based on two aspects, i.e., the number of parameters and activation functions. As noted in table 2 below, increasing the number of trainable parameters in the DNN models led to an increase in the classification accuracy of the corresponding model with the model that 11281 trainable parameters have the highest classification accuracy (90.98%). However, the type of activation used was also noted to influence the performance of the LSTM model. For instance, when the DNN model was trained with 11281 parameters but using Linear, Tanh, and ReLu activation functions, it was observed that the model attained a classification accuracy of approximately 90.94%, 75.00%, and 90.98% (*see table 2*) indicating that an LSTM model with Relu activation had the best classification accuracy in detecting SQL injections using character-level features.

Table 2: Performance Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| Model | Accuracy | Number of parameters | Activation |
| 3 | 90.98 | 11281 | Relu |
| 5 | 90.94 | 11281 | Tanh |
| Random Forest | 90.24 | None | None |
| Multi-Layer Perceptron | 89.39 | None | None |
| 2 | 83.67 | 805 | Relu |
| 1 | 81.59 | 69 | Relu |
| 4 | 75.13 | 11281 | linear |

Overall, the LSTM model with *Relu* activation outperforms both the Random Forest and Multilayer Perceptron models which have a classification accuracy of 90.24% and 89.39% respectively. Figure 3 below shows the learning curve of the optimally performing DNN model.

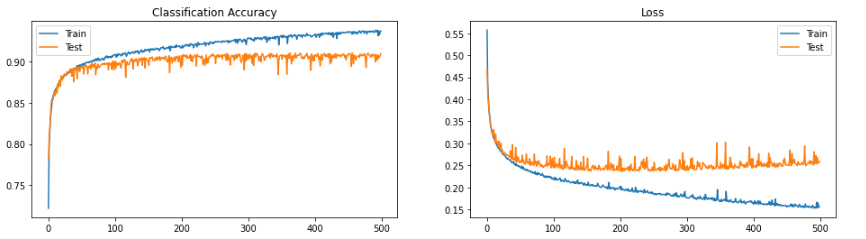


Figure 3: Model Learning Performance

As shown in figure 3 above, the performance of the LSTM model tends to improve as the number of epochs increases.

# Conclusion

Cyber security is a pressing problem that requires the adoption of dynamic approaches if organizations are to protect themselves against the loss of their most critical assets, information. While different digital assets carry varying weights in terms of loss in the event of successful cyber-attacks, the aspect of security elements in each asset cannot be overlooked. Based on the findings of this study, it can be argued that most of the users are interested in extracting database information which supports the argument that organizations that use web applications ought to prioritize the securing of information using appropriate intrusion detection and prevention systems.

Regarding the original research question, i.e., the applicability of deep learning models in predicting an incident of SQL injections in a web server, it can be argued that using the proposed optimal DNN model, it is possible to predict whether a query by a user is an SQL injection or legitimate, ≈91% of the time indicating that the model predicts 91 correct predictions out of 100 total examples. Therefore, the model can be observed to have relatively excellent applicability in the detection of SQL injections.

## Study Limitations and Future Studies

The SQL statements that were captured during data collection are largely gibberish and preprocessing them using methods such as word-embeddings could prove fatal. While character-level tokenization helps obtain general characteristics of the statements, the depth of the features is fairly basic which might have affected the performance of the models.

For future studies, additional model hyperparameter optimization techniques are proposed for consideration. This will enable the researchers to optimize the performance of the deep learning models.

# References

Borky, J. & Bradley, T., 2018. Protecting Information with Cybersecurity. *Effective Model-Based Systems Engineering,* 9(20), pp. 345-404.

Choi, Y.-H.et al., 2020. Using deep learning to solve computer security challenges: a survey. *Cybersecurity,* 3(15).

Crocetti, P., Peterson, S. & Hefner, K., 2021. *What is data protection and why is it important,* s.l.: TechTarget.

Dixit, P. & Silakari, S., 2021. Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. *Computer Science Review,* 39(2021).

Hassan, M. M., Ahmad, R. B. & Ghosh, T., 2021. SQL Injection Vulnerability Detection Using Deep Learning: A Feature-based Approach. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),* 9(3), pp. 702-718.

IBM Security, 2021. *Cost of a Data Breach Report,* s.l.: IBM.

Ibor, A. E., Oladeji, F. A. & Okunoye, O. B., 2018. A Survey of Cyber Security Approaches for Attack Detection,Prediction, and Prevention. *International Journal of Security and Its Applications,* 12(4), pp. 15-28.

Ireland, S., 2022. *Revealed: The True Cost of Rising Cyber Attacks,* s.l.: CEOWorld Magazine.

Jothi, K. R. et al., 2021. *An Efficient SQL Injection Detection System Using Deep Learning.* s.l., IEEE Explore.

Maayan, G. D., 2022. *5 User Authentication Methods that Can Prevent the Next Breach,* s.l.: IDRND.

Rountree, D., 2013. Chapter 2 - What Is Federated Identity?. In: D. Rountree, ed. *Federated Identity Primer.* s.l.:Syngress, pp. 13-36.

Shobana, R., Suriakala, D. M. & Phil, M., 2021. A Thorough Study On Sql Injection Attack-Detection And Prevention Techniques And Research Issues. *Journal of Information and Computational Science,* 10(5).

TechWeb, 2021. *Understanding Authentication, Authorization, and Encryption,* s.l.: Boston University Information Services & Technology.

Tobin, D., 2021. *What is Data Privacy—and Why Is It Important?.* s.l.:Integrate.

Tunggal, A. T. & Sen, K., 2022. *What is the Cost of a Data Breach in 2022?,* s.l.: UpGuard.

Vishalini, P., Rani, K. & Vimala, C., 2016. Cyber Attack Detection Techniques – Solutions. *(IJCSIT) International Journal of Computer Science and Information Technologies,* 7(2), pp. 799-801.

Zhang, W. et al., 2022. Deep Neural Network-Based SQL Injection Detection Method. *Security and Communication Networks,* 2022(Article ID 4836289).