CYSP 2024

THE THIRD CONFERENCE ON

CYBERSPACE

Proceedings

دبیرخانه: قم، ابتدای جاده قدیم تهران، دانشکدگان فارابی دانشگاه تهران، دانشکده مهندسی

تلفن: ۰۲۵-۳۶۱۶۶۶۵۱

Secretariat: Faculty of Engineering, College of Farabi, University of Tehran, Old Qom-Tehran Road, Qom, Iran

Phone Number:(+98-25)36166651

Website: http://cysp2024.ut.ac.ir

E-mail: cysp.conf@ut.ac.ir

Instant Messengers: @cysp_conf

بسم الله الرحمن الرحیم

IN THE NAME OF ALLAH

CYSP 2023

THE THIRD CONFERENCE ON

CYBERSPACE

Proceedings

University of Tehran
29-31 October 2024

.

Proceedings of
The Third Conference on Cyberspace (CYSP 2024)
Organizer: University of Tehran

Preparation: *Kazim Fouladi-Ghaleh*
with: *Sadjad Shokooh, Hussein Azimi, Seyyed Ali Faghih Mousavi Golpayegani, Alireza Zeini*

Publisher: Faculty of Engineering, College of Farabi, University of Tehran
Printing: Matris Publishing Co.
Publishing Year: 2024

Secretariat Address: Faculty of Engineering, College of Farabi, University of Tehran, Old Qom-Tehran Road, Qom, Iran, Postal Code: 3718117469.
Telephone: 025-36166651
Fax: 025-36166652
E-mail: `cysp.conf@ut.ac.ir`
Web: `http://cysp2024.ut.ac.ir`
Messengers: `@cysp_conf`
All links in one: `http://conf.cysp.ir/links`

Table of Papers

[1048] **Using Machine Learning for Detecting and Preventing SQL Injection Attacks**
- Ahamd Farid Aseel 1

[1059] **Advancing Intelligence-Led Cybersecurity: An Architecture for Cyber Security Intelligence Center**
- Mehran Mahboubian - Amir Hossein Pourshams - Mohammad Mahdi Abdian 15

[1098] **Migration Aware Virtual Network Embedding in Software Define Networks**
- Arezoo Jahani 25

[1102] **The Future of Artificial Intelligence, From Cognitive Science to Superintelligence**
- Mohammad Taha Ghaempanah 37

[1112] **An Ensemble Deep Model for Deceptive Opinion Detection Based on Opinion Text: For English and Persian Languages**
- Mahmoud Ali-Arab - Kazim Fouladi-Ghaleh 53

[1116] **The Importance of Modern SEO in the Success of Online Businesses**
- Yashar Abri - Faezeh Khadem 71

[1119] **Cyberattack Defense in Smart Cities: Leveraging Quantum Neural Networks for Secure Route Planning in ADAS**
- Mahdi Seyfipoor - Mohammad Javad Samii Zafarqandi - Siamak Mohammadi 85

[1120] **Vision-based Efficient Traffic Control and Scheduling System for Smart City Intersections with Emphasis on Emergency Vehicles**
- Mahdi Seyfipoor - Sayyed Muhammad Jaffry - Siamak Mohamadi 101

Table of Authors

- Amir Hossein Pourshams (pg. 15)
- Ahamd Farid Aseel (pg. 1)
- Arezoo Jahani (pg. 25)
- Faezeh Khadem (pg. 71)
- Kazim Fouladi-Ghaleh (pg. 53)
- Mahdi Seyfipoor (pg. 85)
- Mahdi Seyfipoor (pg. 101)
- Mahmoud Ali-Arab (pg. 53)
- Mehran Mahboubian (pg. 15)
- Mohammad Javad Samii Zafarqandi (pg. 85)
- Mohammad Mahdi Abdian (pg. 15)
- Mohammad Taha Ghaempanah (pg. 37)
- Mohammad Taha Ghaempanah (pg. 37)
- Sayyed Muhammad Jaffry (pg. 101)
- Siamak Mohammadi (pg. 101)
- Siamak Mohammadi (pg. 85)
- Yashar Abri (pg. 71)

.

English Full Papers

Using Machine Learning for Detecting and Preventing SQL Injection Attacks

Ahamd Farid Aseel[1] [1]*M.Sc. Student, Information Technology Engineering, Faculty of Engineering, College of Farabi, University of Tehran, Iran*
faridaseel.4all@gmail.com

Abstract

This paper investigates SQL Injection attacks and the use of machine learning algorithms as a novel approach to prevent such attacks in databases. It begins by explaining various types of SQL Injection attacks and then introduces the concepts and algorithms of machine learning. The goal of this research is to provide effective solutions for detecting and preventing these attacks. Through examples and practical results, this paper addresses the enhancement of database security through machine learning algorithms. The results show that employing these algorithms can significantly improve database security and contribute to increasing awareness about innovative methods for combating SQL Injection attacks.

Keywords: *SQL Injection, Machine learning, Cybersecurity, Cyber-attack, Artificial intelligence.*

1 Introduction

SQL Injection attacks are one of the oldest and most dangerous threats to web applications. In this type of attack, the attacker injects unreliable inputs into the application, resulting in alterations to the database commands or queries. These alterations can lead to data theft, data loss, and compromise of data integrity.

In essence, in these types of attacks, the attacker sends inappropriate and unreliable inputs to the application. These inputs affect a portion of the command or query and modify the execution of the program. Most vulnerabilities in these types of attacks stem from the validation of inappropriate user inputs [1, 2].

The significance of this issue lies in the fact that attackers can extract sensitive information such as user data, passwords, and financial information from the database, or by altering SQL commands, they can destroy data or even lead to system destruction. However, the attacker may simply aim to gain control of the system without intending to destroy it [3].

Figure 1: SQL Injection Attack

The structure of this text is such that it initially describes various types of SQL Injection attacks, then, while examining past work, various machine learning methods related to the subject will be mentioned. Finally, an evaluation of the effectiveness of machine learning algorithms for detecting intrusions will be addressed.

2 SQL Injection Attacks

SQL Injection attack, as one of the prevalent threats in the digital world, employs malicious SQL codes to manipulate data in databases to gain access to information that was not intended to be accessed. This type of attack, by exploiting vulnerabilities present in database systems and injecting malicious codes, can easily jeopardize online systems. When an attacker successfully exploits SQL Injection, they can fraudulently obtain sensitive information and even gain full control over the database, leading to serious repercussions for organizations and online systems [2, 3].

This section of the article focuses on examining various types of SQL Injection attacks. A comprehensive study regarding the penetration methods of these attacks and their different forms is discussed herein. The aim of this section is to provide an explanation and extensive understanding of SQL Injection attacks to better comprehend cyber threats and raise awareness regarding possible countermeasures against such attacks.

3 Types Of SQL Injection Attacks (SQLIA)

In web applications, most activities involve accessing information from databases. If the data entered by users is not properly validated and authenticated, individuals can gain

Table 1: Example of Injection

admin	admin is Username
`' OR 'x'='x`	`SELECT name FROM member WHERE username='admin' AND password= ' ' OR 'x'='x'`
`' OR 'x'='x ' OR 'x'='x`	`SELECT name FROM member WHERE username =' ' OR 'x'='x' AND password=' ' OR 'x'='x'`
`'OR 'x'='x' - -`	`SELECT name FROM member WHERE username =' ' OR 'x'='x' - - ' AND password=' '`

access to information they were not intended to see. Various methods exist to execute SQL Injection attacks [9].

3.1 Tautologies

Tautology is a type of SQL data structure tampering attack wherein hackers attempt to bypass validations, identify input parameters, and/or extract information from the desired database using WHERE clause conditions that are always true in every interpretation. For instance: `"WHERE password = 'x' OR 'x' = 'x'"` or `"WHERE password = 'x' OR 1=1"`. Therefore, possible signatures for this type of attack include string terminator `" ' "`, `OR`, `=`, `LIKE`, and `SELECT`. Mitigating tautology attacks in SQL data structure tampering attacks can be achieved by precise validation of user inputs on the user side and blocking queries containing tautological conditions in WHERE clauses on the database side [5, 6].

This query is always true because it is augmented with the tautology expression (`'x'='x'`). The double dashes `"--"` indicate to the SQL interpreter software that the rest of the statement is a comment and should not be executed as part of the new command sent to the database or in the execution of stored procedures. It is worth noting that many databases do not require a special character to separate distinct queries, so essentially checking for exceptional or special characters is not an effective

way to prevent these types of attacks.

3.2 Inference

In this type of attack, attackers design queries that, when executed, alter the behavior of the application or database. They use the responses received from the database to modify the query method. This type of attack is based on a rewrite that is executed based on the correct or incorrect response to a question about data values in the database. Typically, attackers target a site that appears to be sufficiently secure, so that when injection is successful, sufficient information is not available through database error messages. Therefore, attackers use various methods to obtain responses from the database. They inject their commands into the site and observe the website's reaction behavior to determine whether these changes indicate any vulnerabilities in the site's parameters or not. This method allows the attacker to gain access to database data and identify vulnerable parameters.

Two well-known attack techniques based on inference that allow attackers to extract data from the database and identify vulnerable parameters are Blind Injection and Timing attacks [5, 6, 7].

3.3 Blind Injection

Developers remove details of error messages. These messages help attackers to infiltrate databases. In this case, attackers attempt to penetrate the database using vulnerability query statements that have logical results. Then, they analyze the differences based on program responses [6, 4].

3.4 Timing Attacks

A timing attack allows an attacker to extract information from a database by observing time delays in the database response. This type of attack is very similar to blind injection but employs a different method. To conduct a timing attack, attackers structure their injection query as an if/then statement, where the conditional branches relate to unknown information about the database content. In one of the branches, the attacker uses an SQL structure that requires a specific time to execute (such as a watch key that causes a delay in the database response). By measuring the increase or decrease in database response time, the attacker can infer which branch in their injection has been executed, and therefore what the injected query's response is [4, 6, 8].

Now, let's consider Table 2. In the first scenario, we have a secure program, and inputs for system entry are properly validated. In this case, both injections return a system login error message, and the attacker understands that the system entry parameter is not vulnerable. In the second scenario, we have an insecure program, and the system entry parameter is injectable. The attacker sends the first query, and due

Table 2: Code Example

```
SELECT accounts FROM users WHERE login='legalUser' and 1=0 -
' AND pass='' AND pin=0
```

```
SELECT accounts FROM users WHERE login='legalUser' and 1=1 -
' AND pass='' AND pin=0
```

to the always-evaluating false condition, the program returns a system login error message. However, at this point, the attacker does not know whether this is because the program properly validated the input and blocked the attack attempt or if the attack itself caused the system login error. The attacker then sends the second query, which is always evaluated as true. If the system login error message is not needed in this case, the attacker realizes that the attack has been successful, and the system entry parameter is injectable.

3.5 Malformed Queries

In this method, when an attacker exploits incorrect or insufficient symbols in the SQL command, an error message is returned from the database containing useful information for troubleshooting. This error message enables attackers to accurately identify vulnerable parameters in the program and the overall database structure. This situation is exploited due to SQL commands designed by attackers or incomplete inputs that result in syntax errors, data type problems, or logical errors in the database. Syntax errors are used to identify injectable parameters. Also, data type errors may be used to infer specific information types or to delete used information. Logical errors may also reveal table names or features that cause errors or mistakes [8].

3.6 Union Query

In this technique, attackers merge an invalid statement with a valid query using the UNION keyword. This merging involves appending a query statement with the structure `"UNION <injected query>"` to the end of a valid statement as much as possible. This action causes the program to retrieve information from both the original query results and another table. Then, a statement with a double dash `"--"` as a comment existing within the query is deactivated. In this query, the original query returns an empty set while the manipulated query statement retrieves data from the same table [11, 8].

Table 3: Code Example

```
SELECT name FROM member WHERE username=''UNION
SELECT password FROM member WHERE username='admin' -- AND password=''
```

Table 4: Code Example

```
SELECT accounts FROM users WHERE login='admin' AND
pass=''  - ' AND pin=123; DROP table users
```

4 Piggy-backed Queries

In this type of attack, the attacker attempts to inject additional queries into the main query. We distinguish this type from others because attackers in this case are not seeking to modify the main query; instead, they try to add new and distinct queries piggybacked onto the main query. The result of this action is the execution of multiple SQL queries by the database. The first query is the main query that is executed normally; subsequent queries are the injected queries that are executed in addition to the main query. This type of attack can be highly destructive. Upon success, attackers can insert almost any type of SQL command, including stored procedures, into the additional queries and execute them along with the main query. Vulnerability to this type of attack usually depends on the configuration of the database allowing multiple commands to be received in a supplementary string [13].

Example: If the attacker enters the text `"'; drop table users --"` into the password field, the program generates the following query (table 4).

After executing the first query, the database recognizes the boundary marker (`";"`) and proceeds to execute the injected second query. The result of executing the second query is the deletion of the users table, potentially removing valuable information. Other types of queries may involve inserting new users into the database or executing stored procedures. Note: Many databases do not require a specific symbol to separate distinct queries, so searching only for a query separator is not an effective way to prevent this type of attack [10, 6, 5].

4.1 Stored Procedures

Due to the extensive capabilities provided by stored procedures in the database, SQL Injection Attack intrusion attempts of this type seek to execute these procedures in the database. Many database vendors provide standard stored procedures that extend database capabilities and provide interaction with the operating system. Therefore,

Table 5: Code Example

```
SELECT name FROM member WHERE username=''; SHUTDOWN; - - password=''
```

Table 6: Code Example

```
SELECT accounts FROM users WHERE login='legalUser';
exec(char(0x73687574646f776e)) -- AND pass='' AND pin=
```

whenever an attacker identifies which development the database is using, they can specifically design SQL Injection Attack intrusions to execute the stored procedures offered by that database, even procedures that interact with the operating system.

There is a common misconception that using stored procedures to write web applications protects them against SQL Injection Attack intrusions. Developers are often surprised that their stored procedures are vulnerable to attacks just like regular programs. Additionally, because stored procedures are often written in specific scripting languages, they may be susceptible to other types of vulnerabilities such as buffer overflows, allowing attackers to execute arbitrary code on the server or elevate their privileges [4, 12, 6, 8].

4.2 Alternate encoding

Alternate encoding SQL Injection attack is a type of attack where hackers attempt to conceal their injection commands using encoding techniques such as ASCII, hexadecimal, and Unicode. Thus, possible signatures for this attack include: exec(), Char(), ASCII(), BIN(), HEX(), UNHEX(), BASE64(), DEC(), ROT13(), and similar methods. Accurate validation of user inputs on the user side, for example, prohibiting the use of any metacharacters such as `"()Char"` and interpreting all metacharacters as regular characters on the database side, can prevent alternate encoding SQLi attacks. In terms of violating the three elements of the CIA triad, SQLi inference attack and alternate encoding are among the different classifications of SQLi. For example, the inference attack does not compromise information security but rather involves an initial data gathering operation by the attacker. Alternate encoding is a method to conceal SQLi attacks from other types. All the aforementioned attacks along with their signatures and prevention methods are listed in Table 1 [4]. Related works on SQLi attacks, detection, and prevention will be discussed in the next section [12].

This example utilizes the ()char function and hexadecimal encoded ASCII. The () char function, by taking an integer or hexadecimal encoded character, returns an instance of that character. The sequence of numbers in the injection part represents the hexadecimal encoding of the ASCII for the string `"SHUTDOWN"`. Therefore, when

interpreted by the database, the query concludes with the execution of the SHUTDOWN command by the database [6].

5 Related Works

A considerable number of studies and research have been conducted in the field of SQL injection penetration and its detection using various methods, including static and dynamic analysis, a combination of techniques, machine learning, hash techniques, etc. [15].

Static analysis examines whether each flow from a source to a precise location depends on confirming the information and also investigates the input sanitation method [15]. Meanwhile, dynamic analysis involves developing advanced query structure extraction for each data and identifying attacks by comparing them with the actual query structure given by the user [17].

AMNESIA, as an integrated method, is a model-based approach that integrates static and dynamic analysis for detecting and preventing SQL injection attacks. It utilizes static analysis to create SQL query models at the time of database access. It then utilizes dynamic analysis before sending queries to the database and compares them with the static models previously created. However, there are query generation methods and specific code snippets that reduce the efficiency of this model and increase the error rate [18].

The Hidden Markov Model (HMM) has been introduced for detecting malicious queries using machine learning in two phases: training and execution. The first phase focuses on collecting known malicious and benign queries, while the second phase concentrates on detecting injection attacks. The author themselves have stated that WHERE clauses and piggybacked queries cannot be identified by this model [19, 21].

Lambert et al. [20, 22] proposed a model that utilizes tokenization technique for detecting SQL injection attacks, hence queries containing aliases, samples, and set operations can also be blocked at the entry point. It examines whether the query generated based on user input yields its desired result and compares the results by applying tokenization technique on a main query and an input query. If the results are the same, there is no injection attack; otherwise, the attack is present. Balasundaram et al. [23] proposed a technique using ASCII-based string matching for detecting SQL injection attacks. This technique utilizes static and dynamic analysis to examine user input fields to identify and prevent SQL injection attacks.

6 Machine Learning Classification Based Modeling

Classification is a supervised learning technique extensively used for modeling cyber-attacks based on various attack categories. In supervised learning, data is always labeled before training. During the training phase, the classifier learns labels so that it can

accurately predict for data that has not been seen before during the testing phase. In our analysis, commonly used machine learning techniques for various purposes are implemented. Several techniques can be summarized as follows.

6.1 Naive Bayes

Naive Bayes is a type of Bayesian network and a common machine learning algorithm [26]. It is a basic probability-based technique that calculates the probability of classifying or predicting the class of a cyber attack in the given dataset. This method assumes that the value of each feature is independent and does not consider the correlation or relationship between features [27]. Naive Bayes consists of two probabilities: conditional probability and class probability. The class probability is determined by dividing the frequency of each class instance by the total number of instances. The conditional probability is the ratio of the repetition of each feature for a given class and the repetition of instances for that class. Naive Bayes is faster than other classifiers.

6.2 Decision Trees

Decision Tree is one of the most popular algorithms for classification and prediction in machine learning. ID3, proposed by J. R. Quinlan [29], is a common top-down approach for building decision trees. Based on this, the C4.5 algorithm [30], and later the BehavDT method [30], the IntruDTree model [32] have been developed for generating decision trees. A decision tree is a tree-like structure in which an internal node represents features, branches indicate outcomes, and leaves represent a class label. These algorithms create decision rules for predicting outcomes for unseen test cases. They provide high accuracy and better interpretability. Decision trees can handle both continuous and discrete data.

6.3 Random Forest

Random Forest is a classifier composed of decision trees as a team learning method [33, 34]. Breiman and his colleagues proposed this method.

6.4 SVM

Support Vector Machine operates by maximizing the distance between data points from the separator boundary, known as the margin. The SVM algorithm can classify with high accuracy and can be used for classification and regression tasks [35].

6.5 Artificial Neural Network

Additionally, in parallel with classical machine learning techniques above, we consider an artificial neural network learning model. The most common architecture of an artificial neural network is a multi-layer perceptron consisting of an input layer with multiple

inputs, one or more hidden layers typically using sigmoid activation functions, and an output layer for attack prediction. This approach utilizes backpropagation for network construction [36].

7 Experimental Evaluation

This section defines performance metrics in the field of intrusion detection and examines the results by conducting experiments on cybersecurity datasets with various attack categories. If TP refers to true positives, FP to false positives, TN to true negatives, and FN to false negatives, then the formal definition of the following metrics is as follows.

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$F1score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{3}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

8 Dataset

The most critical part of detecting SQL injection attacks is the data and dataset. This section plays a crucial role in detecting and predicting SQL injection attacks. The data used in this section must be very accurate and meaningful, containing SQL injection attack queries. In this article, the dataset available on Kaggle has been utilized. This dataset consists of two main fields, namely Query and Label. In the Query field, malicious queries and legitimate commands are included. Out of all queries, 11,331 of them are labeled as one, indicating SQL injection attacks, while the remaining 19,595 are labeled as zero, representing harmless queries.

9 Experimental Results and Discussion

In this section, the effectiveness of machine learning algorithms for detecting intrusions has been investigated. For this purpose, an analysis has been conducted on various classification techniques, including Artificial Neural Networks (ANN), Naive Bayes (NB), Support Vector Machine (SVM), Decision Trees (DT), and Random Forest (RF). Additionally, values for precision, recall, F1 score, and accuracy for each of the examined classification models have been evaluated.

To evaluate the performance of each of the classification models in intrusion detection systems, Figures 2 and 3 respectively compare accuracy, precision, recall, and F1 score.

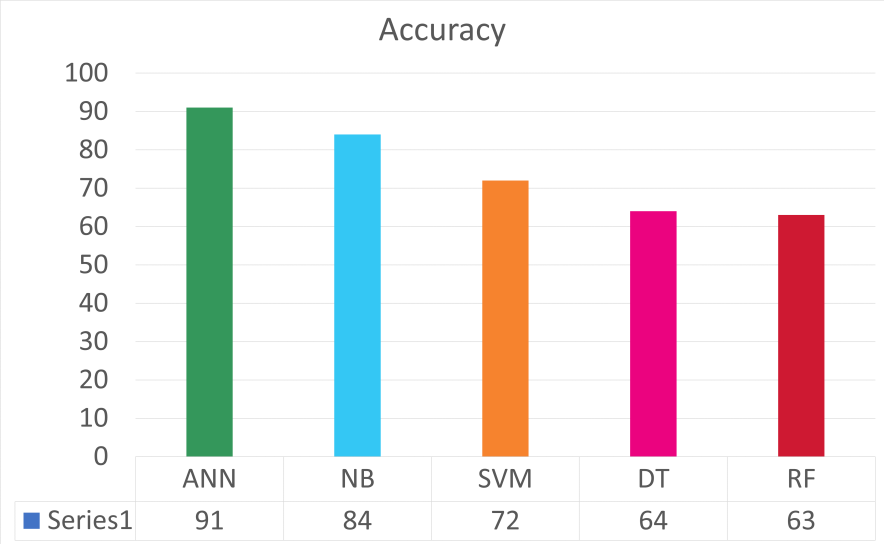

Figure 2: Performance Comparison Results in Terms of Accuracy for Machine Learning-Based Models in Intrusion Detection Systems

For evaluation, the same set of training and testing data is used for each machine learning-based classification model in intrusion detection systems.

Figures 2 and 3 show that the artificial neural network-based intrusion detection model consistently outperforms other classifiers in detecting intrusions. Specifically, artificial neural network achieves the best results in terms of accuracy, precision, recall, and F-score. The reason for this is that the neural network classifier initially creates several neural networks, and for each different network, a set of inference rules is derived. Each neural network in the artificial neural network model acts as a different machine learning classification technique, and considering the majority voting of these networks, more logical rules are generated. Therefore, the artificial neural network model performs better in terms of accuracy, recall, F-score, and precision. Overall, the machine learning-based intrusion detection model discussed above focuses entirely on the data and reflects behavioral patterns of various cyber attacks.

10 Comparison of Traditional Methods and Machine Learning In SQL Attack Prevention

Traditional methods such as static and dynamic analysis discussed in the Related Works section rely heavily on examining predefined and fixed patterns, but they have limitations when dealing with more complex or evolving attacks, as seen with AMNESIA and HMM. These methods often face efficiency issues when confronted with advanced attacks. In contrast, machine learning-based models discussed in the Machine Learning Classification Based Modeling section offer greater flexibility in detecting emerging

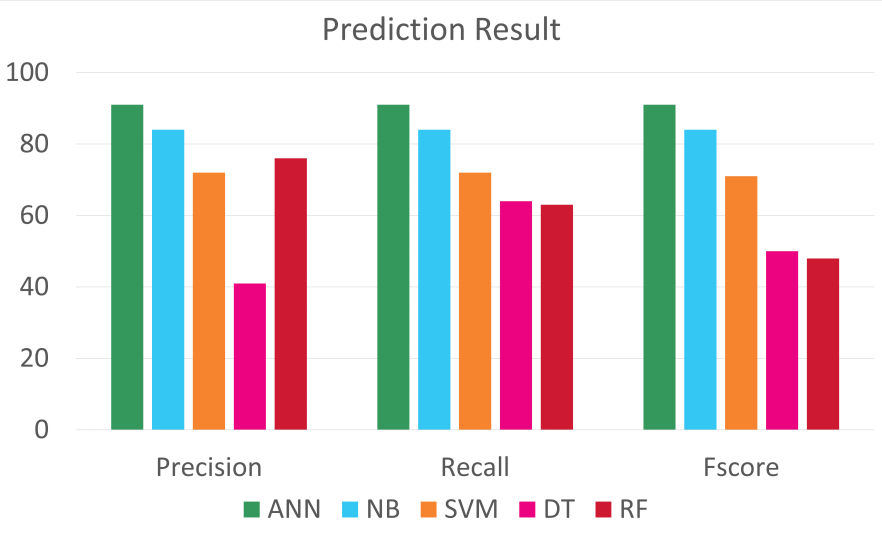

Figure 3: Performance Comparison Results in Terms of Accuracy, Recall, and F-score for Machine Learning-Based Classification Models in Intrusion Detection Systems

threats. Models like Artificial Neural Networks (ANN), due to their ability to learn from data and adapt to new patterns, outperform traditional methods in detecting complex attacks and demonstrate higher accuracy.

11 Conclusion

The capability and efficiency of a machine learning-based intrusion detection model is one of the most fundamental concerns for individuals active in the field of IT, e-commerce, and application developers from a security perspective. In general, cyber-security datasets comprise various types of cyber attacks along with their associated features. Therefore, some classification models may not perform optimally in terms of accuracy and true prediction rates based on diverse attack categories and various features. In this article, we have investigated the performance of data-based intrusion detection models considering well-known classification techniques in the field of machine learning. Additionally, performance metrics such as accuracy, recall, F-score, and overall precision have been evaluated. Our future plans include expanding cybersecurity datasets and designing a data-based intrusion detection system that benefits from a combination of various intrusion detection models. This composite system aims to provide automated security services to the cybersecurity community.

References

[1] A. F. Aseel and Y. Abri, "Vulnerability Analysis of Social Media Accounts Against Cyber Attacks", in Proc. 2nd Conference on Cyberspace, University of Tehran, Iran, 2023, pp. 29-36.

[2] S. S. A. Krishnan, A. N. Sabu, P. P. Sajan, and A. L. Sreedeep, 'SQL injection detection using machine learning', vol, vol. 11, p. 11, 2021.

[3] T. Muhammad and H. Ghafory, 'SQL Injection Attack Detection Using Machine Learning Algorithm', Mesopotamian journal of cybersecurity, vol. 2022, pp. 5–17, 2022.

[4] N. M. Sheykhkanloo, 'SQL-IDS: evaluation of SQLi attack detection and classification based on machine learning techniques', in Proceedings of the 8th International Conference on Security of Information and Networks, 2015, pp. 258–266.

[5] U. Farooq, 'Ensemble machine learning approaches for detection of sql injection attack', Tehnički glasnik, vol. 15, no. 1, pp. 112–120, 2021.

[6] W. G. Halfond, J. Viegas, A. Orso, and Others, 'A classification of SQL-injection attacks and countermeasures', in Proceedings of the IEEE international symposium on secure software engineering, 2006, vol. 1, pp. 13–15.

[7] B. A. Cumi-Guzman, A. D. Espinosa-Chim, M. G. Orozco-del-Castillo, and J. A. Recio-García, "Counterfactual explanation of a classification model for detecting SQL injection attacks", Tecnológico Nacional de México / IT de Mérida, Mérida, México, 2024.

[8] Z. C. S. S. Hlaing and M. Khaing, 'A detection and prevention technique on sql injection attacks', in 2020 IEEE Conference on Computer Applications (ICCA), 2020, pp. 1–6.

[9] W. G. J. Halfond and A. Orso, 'Detection and prevention of SQL injection attacks', in Malware Detection, Springer, 2007, pp. 85–109.

[10] M. Kumar, L. Indu, "Detection and Prevention of SQL Injection Attack", International Journal of Computer Science and Information Technologies, vol. 5, no. 1, pp. 374-377, 2014.

[11] G. Yigit, M. Amavutoglu, "SQL Injection Attacks Detection & Prevention Techniques", International Journal of Computer Theory and Engineering, vol. 9, no. 5, pp. 351-356, October 2017

[12] M. Ŝtamper, "Inferential SQL Injection Attacks", International Journal of Network Security, vol 18, no. 2, pp. 316-325, Mar 2016.

[13] A. Brehmer and M. Teräs, "SQL injection vulnerabilities in open-source projects", Final Project, Mid Sweden University, Östersund, Sweden, Spring 2024.

[14] N. Moradpoor, "A Pattern Recognition Neural Network Model for Detection and Classification of SQL Injection Attacks", The 13th International Conference on Information and Communication Engineering (ICICE15), Jun 2015.

[15] Halfond, W. G. & Orso, A. (2005). AMNESIA: analysis and monitoring for neutralizing SQL-injection attacks. In Proceedings of the 20th IEEE/ACM International Conference on Automated Software Engineering, 174-183. https://doi.org/10.1145/1101908.1101935

[16] Shar, L. K. & Tan, H. B. K. (2013). Defeating SQL injection. Computer, 46, 69-77. https://doi.org/10.1109/MC.2012.283

[17] Tajpour, A. & Shooshtar, M. J. Z. (2010). Evaluation of SQL injection detection and prevention techniques. In Second IEEE International Conference on Computational Intelligence, Communication Systems and Networks, Liverpool, UK, 216- 221. https://doi.org/10.1109/CICSyN.2010.55

[18] Dharam, R. & Shiva, S. G. (2013). Runtime monitors to detect.

[19] Kar, D., Agarwal, K., Sahoo, A., & Panigrahi, S. (2016). Detection of SQL injection attacks using Hidden Markov Model. 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, India. https://doi.org/10.1109/ICETECH.2016.7569180

[20] N. Lambert, K.S. Lin; "Use of Query tokenization to detect and prevent SQLinjection attacks", Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, China:IEEE (2010). pp: 438-440, 2010.

[21] D. Lu, J. Fei, and L. Liu, "A semantic learning-based SQL injection attack detection technology", MDPI, 2023.

[22] A. Kumar, S. Bhatt, "Use of Query Tokenization to Detect and Prevent SQL Injection Attacks", International Journal of Science Technology & Engineering, vol. 2, issue. 01, pp. 97-103, July 2015

[23] I. Balasundaram, E. Ramaraj, "An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching", International Conference on Communication Technology and System Design, Prodedia Engineering, pp. 183-190, 2012.

[24] I.H. Witten, E. Frank, L.E. Trigg, M.A. Hall, G. Holmes, and S.J. Cunningham, "Weka: practical machine learning tools and techniques with Java implementations", 1999.

[25] J. Han, J. Pei, and M. Kamber, "Data Mining: Concepts and Techniques", Elsevier, Amsterdam, 2011.

[26] G.H. John and P. Langley, "Estimating continuous distributions in Bayesian classifiers", in Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence, pp. 338–345, Morgan Kaufmann Publishers Inc., 1995.

[27] J.R. Quinlan, "Induction of decision trees", Mach. Learn., vol. 1, no. 1, pp. 81–106, 1986.

[28] I.H. Sarker, A. Kayes, and P. Watters, "Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage", Journal of Big Data, 2019.

[29] J.R. Quinlan, "Induction of decision trees", Mach. Learn., vol. 1, no. 1, pp. 81–106, 1986.

[30] J.R. Quinlan, "C4.5: programs for machine learning", Machine Learning, 1993.

[31] I.H. Sarker, A. Colman, J. Han, A.I. Khan, Y.B. Abushark, and K. Salah, "Behavdt: a behavioral decision tree learning to build user-centric context-aware predictive model", Mobile Netw. Appl., vol. 1, pp. 1–11, 2019.

[32] I.H. Sarker, Y.B. Abushark, F. Alsolami, and A.I. Khan, "Intrudtree: a machine learning-based cyber security intrusion detection model", Symmetry, vol. 12, p. 754, 2020.

[33] L. Breiman, "Random forests", Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.

[34] M. Alghawazi, D. Alghazzawi, and S. Alarifi, "Deep learning architecture for detecting SQL injection attacks based on RNN autoencoder model", MDIP, 2024.

[35] S. Venkatramulu, M. S. Waseem, A. Taneem, S. Y. Thoutam, S. Apuri, and Nachiketh, "Research on SQL injection attacks using word embedding techniques and machine learning", Journal of Sensors, IoT & Health Sciences, vol. 2, no. 1, pp. 55-66, Mar. 2023.

[36] F. K. Alarfaj and N. A. Khan, "Enhancing the performance of SQL injection attack detection through probabilistic neural networks", MDIP, 2023.

Advancing Intelligence-Led Cybersecurity: An Architecture for Cyber Security Intelligence Center

Mehran Mahboubian[1], Amir Hossein Pourshams[1], Mohammad Mahdi Abdian[1]

[1]*R&D Center, Mobile Communication Company of Iran, Tehran, Iran*
{m.mahbubian,ah.pourshams,m.abdian}@mci.ir

Abstract

The swift progression of cyber threats presents significant challenges for organizations striving to safeguard their digital assets through traditional security methods alone. Research shows that relying only on security controls and incident response is insufficient. On the other hand Cyber Threat Intelligence (CTI) has become an essential component of effective cybersecurity strategies, facilitating the proactive identification and coordinated response to threats. This paper proposes a novel architecture for establishing a Cyber Security Intelligence Center (CSIC) within an organization. As the CSIC is a pure novel concept, the first version is implemented in the MCI R&D Office of Security to evaluate its effectiveness and performance. The CSIC would conduct cyber intelligence operations and intelligently integrate with existing security operations and business functions. The proposed CSIC architecture includes CTI lifecycle processes to perform its core functions. In the proposed CSIC intelligence operations would interact closely with security teams, such as those dedicated to prevention, detection and response, aiming to enhance organizational capabilities for preempting and identifying novel cyber threats. Preliminary findings demonstrate establishing a centralized intelligence operation through a CSIC may significantly improve an organization's time to predict, time to detect and time to respond to cybersecurity threats.

Keywords: *Intelligence-Led Security, Cyber Security Intelligence, Cyber Threat Intelligence, Cyber Security Intelligence Center.*

1 Introduction

The digital landscape has revolutionized business operations, opening avenues for growth and innovation. However, this transformation has also introduced new risks, notably in the form of cyber threats. Cybercriminals, nation-state actors, and other malicious entities continually devise new strategies to breach organizational defenses, compromising sensitive data and disrupting critical operations [1]. The traditional approach to cybersecurity, which focuses on deploying security controls and reacting to

incidents as they occur—known as reactive security—is no longer sufficient to address the evolving threat landscape. Organizations must follow Cyber Threat Intelligence (CTI) to adopt a proactive approach to cybersecurity, which involves identifying and responding to threats before they materialize [2].

CTI refers to the collection, processing, and analysis of information aimed at understanding a threat actor's motives, targets, and attack behaviors [3]. It empowers organizations to make informed decisions about their security by anticipating and mitigating potential threats before they can impact business operations. The aim of CTI is not merely reactive; it strives to provide a predictive capability to anticipate potential security incidents based on the tactics, techniques, and procedures of potential threat actors [4]. CTI encompasses a range of intelligence, including strategic, operational, tactical, and technical intelligence [5]:

- Strategic Intelligence: Provides a broad context regarding the cyber threats facing an organization or sector, useful for high-level policy and decision-making.
- Operational Intelligence: Offers insights into specific upcoming or ongoing attacks, suitable for informing operational decisions during incident response.
- Tactical Intelligence: Details the tactics, techniques, and procedures used by threat actors, aiding the development of defensive measures.
- Technical Intelligence: Includes technical indicators of compromise (IOCs) such as hashes, IP addresses, and URLs, which assist in identifying and mitigating attacks.

Despite the recognized importance of CTI and the availability of its essential components, many organizations struggle to establish and integrate it effectively. One of the main challenges is the lack of a comprehensive architecture for performing CTI actions. Hence, the need arises to establish a centralized system such as CSIC that can perform these capabilities. This study aims to address this gap by proposing an architecture for CSIC that can help organizations optimize their CTI capabilities and reduce cybersecurity risk. The proposed CTIC architecture, along with its interactions, will integrate various components of CTI. This includes intelligence collection, processing, analysis, and dissemination, as well as aligning with the organization's security operations and business goals.

2 Related Works

While cyber threat intelligence is crucial for private businesses, numerous academic research studies are also being conducted on this topic. Further advancements in the field made by [6] who developed an enhanced eight-step CTI model, building upon a pre-existing six-step model. This model introduced two additional stages: visualization

and analysis. A tool which applies this model is designed to collect data from various sources, create analytics to expedite threat mitigation time, and improve CTI regarding collection, filtering, sharing, visualization, and analysis. The tool utilizes multiple technologies and protocols, including MySQL, Elastic Search, Log stash, and TAXII. The researchers concluded their work could enhance CTI effectiveness and improve threat mitigation, demonstrating the tool's application using a real-world example.

Gong and Lee proposed a cyber threat intelligence framework aimed at enhancing the security of the energy cloud environment to quickly apply a security model to a large-scale energy cloud infrastructure, and a method for sharing and spreading CTI between the Advanced Metering Infrastructure (AMI) layer and the cloud layer [7]. The framework is designed to include the local AMI layer, the station layer, and the cloud layer. The authors demonstrate that it can effectively respond to cyber threats and also show that the proposed framework can effectively respond to cyber threats by achieving a 0.822 macro-F1 score and a 0.843 micro-F1 score for cyberattack detection in an environment that simulates the model of an attacker and an energy cloud environment.

The study [8] found that CTI tasks are often manual and resource-intensive but can resolved through automation. However, implementing the CTI function is more prevalent in larger organizations due to budget and resources, while smaller organizations rely more on tools. Skills for the CTI function can be learned on the job, but formal education is beneficial. The research also highlights how the CTI function is vital for proactive defense capabilities, enabling organizations to detect and prevent cyber-attacks more effectively. The CTI function provides organizations with insight into the techniques, tactics, and procedures of a threat actor, allowing them to develop proactive detection and mitigation strategies.

The authors of [9] propose that the increasing asymmetry between the cyber-offensive capabilities of attackers and the cyber-defensive capabilities of commercial organizations can addressed by integrating CTI into their defense mechanisms. CTI, which involves the acquisition, processing, analysis, and dissemination of information that identifies, tracks, and predicts cyber threats, can transform organizations' cyber-security behavior from being reactive to proactive, anticipatory, and dynamic.

The paper describes a case study of a large multinational finance corporation's journey to adopt and integrate CTI, transforming its cybersecurity practices. The process involved two phases. Phase 1 considers the adoption of CTI as an innovation within the organization's IT Operations Division. In Phase 2, this innovation translated into a novel solution known as CTI-as-a-service. This service is designed to package and integrate CTI into the broader commercial context for business users. The study illustrates the process of adopting and integrating CTI and provides practical insights into transforming cybersecurity practices.

The ECOSSIAN project [10] introduces a pan-European, three-layered approach to safeguard critical infrastructures (CIs) by detecting cyber incidents and swiftly generating warnings for potentially affected infrastructures. This ecosystem consists of three types of Security Operation Centers (SOCs): Organization SOC (O-SOC), National

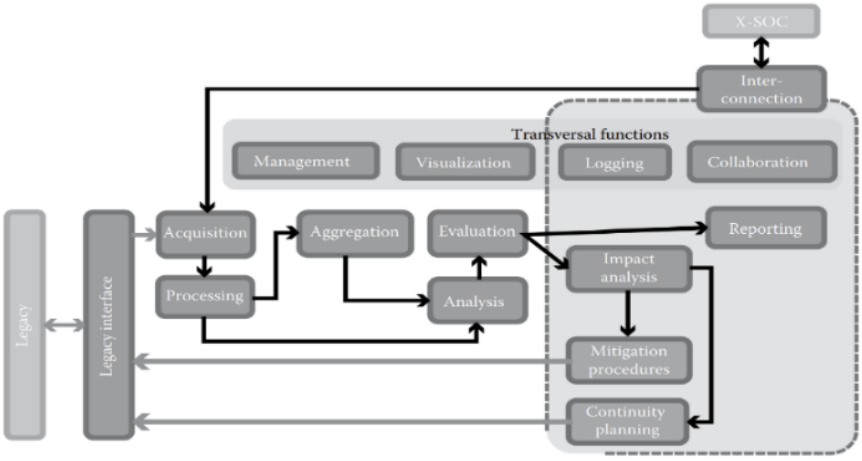

Figure 1: ECOSSIAN project architecture [11]

SOC (N-SOC), and European SOC (E-SOC).

This tri-level incident analysis network allows for flexible, scalable, and technology-independent implementations of SOCs. Functional blocks serve as modular units, facilitating detailed and context-specific functions. The functional blocks include continuity planning, visualization, interconnection, management, collaboration, reporting, impact analysis, mitigation procedure, analysis, evaluation, logging, legacy interface, processing, and aggregation.

Here we propose the CSIC comprising two main sections: the framework and architecture.

2.1 Framework

The framework of the CSIC encompasses the people, processes, and technology needed for its operation. The personnel of the CSIC include intelligence analysts, malware analysts, and forensic experts [5, 11]. The CSIC's processes follow the CTI lifecycle elements, which is necessary to perform cyber intelligence operations.

2.2 Architecture

Our proposed architecture for the CSIC incorporates various internal components and relationships with external relations to the organization's security operations and business objectives.

We classify external security operations into five classes: Asset Management, Prevention, Detection, Response and Recover [12]. These processes serve as the building components of our external stakeholders of the CSIC. The system lifecycle follows four steps: design, build, run, and defend [13]. On the other hand, the CSIC has processes of collection, processing, analysis, and dissemination that are considered to be the building

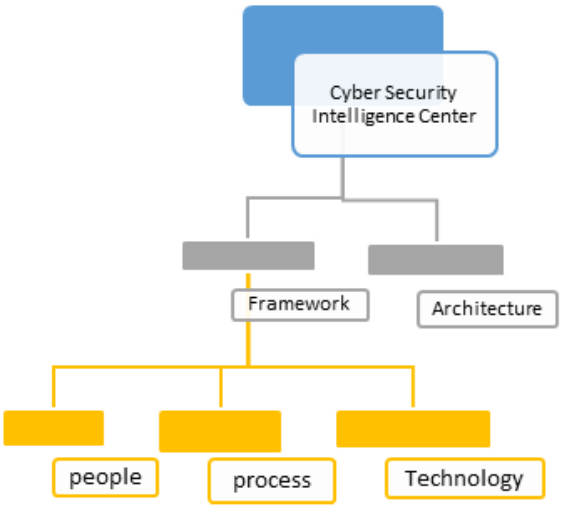

Figure 2: Proposed cyber security intelligence center frame

components of the CSIC as they execute the primary functions of a cyber intelligence operation.

2.2.1 Business and Risk components

As depicted in figure 3 the business component sets the strategic direction and overall security objectives and its interaction influences risk management and security priorities. There are five other security components in the organization:

The Risk component identifies and assesses risks to the organization. Its interaction communicates risk information to the ”Business” and “Asset Management”.

2.2.2 Design, Build, Run and DevSecOps components

DevSecOps ensures that security is considered at every stage of the software development lifecycle. It works with “Design”, “Build”, and “Run” processes.

The Design, Build, and Run components focus on developing and running secure systems and applications, considering vulnerabilities and weaknesses during the design and build phases through the DevSecOps.

2.2.3 Defend component

The Defend component is the central component of the security operations and consists of subcomponents:

- Asset Management: Identifies and inventories assets.
- Prevent: Implements preventive measures.

- Detect: Continuously monitors for threats.
- Response: Respond to detected incidents.
- Recover: Restore normal operations post-incident.

2.2.4 "Vulnerability & Weakness" component

The "Vulnerability & Weakness" component identifies vulnerabilities and weaknesses in systems. It ingests information from "DevSecOps" and "Data Processing" and outputs information into the "threat intelligence analysis" component.

2.2.5 The CSIC components

Collection. Collection within the CSIC refers to gathering information from external sources such as private/public communities, government sources, sector peers, business partners, and vendor alerts. "Collection Sources" are sources of external intelligence and threat information and serve as the input for data processing. They have subcomponents:

a. Governmental sources: Information from government agencies.

b. Sector Peers: Collaboration with other organizations in the same industry.

c. Business partners: Information from industry/business partners.

d. Vendor Alerts: Alerts from vendors about uncovered vulnerabilities and threats.

e. Threat Intelligence Services: Includes free and paid threat Intelligence.

Processing. The processing stage based on the intelligence analyst's diagnosis and intelligence requirements.

"Data Processing and Mining" normalizes, indexes, enriches, filters, and prioritizes information [14] sent from prevention and forensic and malware analysis in "defend" component because this data contains valuable information about blocked intrusion attempts and successful intrusion attempts. It has subcomponents:

a. Actors & Objectives: Understand threat actors and their goals.

b. TTPs (Tactics, Techniques, and Procedures): Identifies common tactics and techniques used by attackers.

c. Observable & Indicator: Detects specific indicators of compromise.

During the analysis phase, we consider assumptions, develop hypotheses based on them, and then evaluate these hypotheses using techniques like ACH matrix and contrarian techniques. For advanced and supplementary analysis, forensic and malware

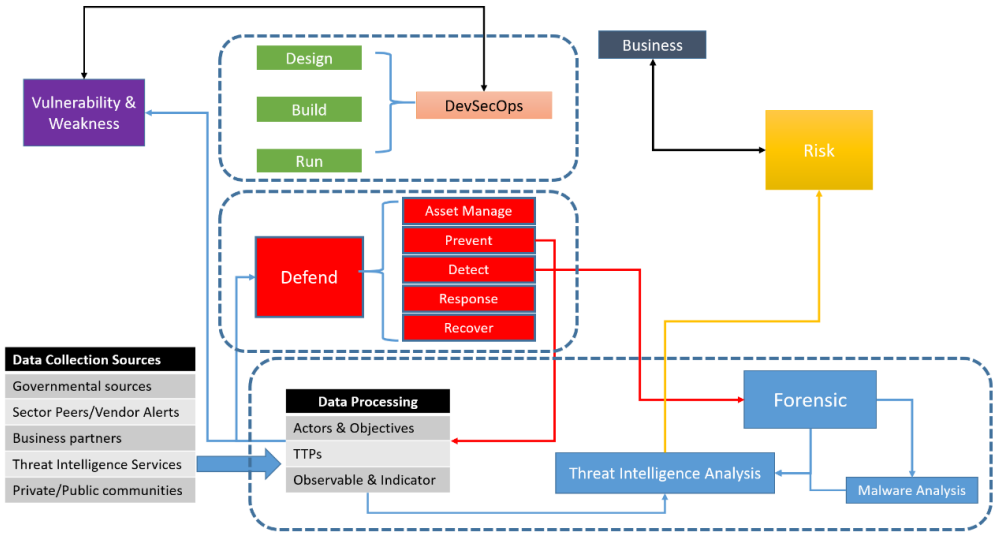

Figure 3: Proposed CSIC architecture

analysis should be done and the dissemination phase is the relations between CSIC and organization components.

The CSIC has five primary components:

Analysis. "Threat Intelligence Analysis" analyzes threat information to provide actionable insights. It ingests information from "Data Processing and Mining" and "Vulnerability & Weakness" to detect real threats and, after analysis, outputs produced intelligence about threats into the risk component.

Forensic. "Network, OS and Memory Forensic" analyzes networks, operating systems, and memory. It ingests information from monitoring and detection about detected attacks and outputs produced intelligence about technical intelligence like IoCs into the "threat intelligence analysis" component.

Malware Analysis. "Malware Analysis" analyzes malware to understand its behavior and impact. It ingests information from "Forensics" and outputs produced intelligence into "threat intelligence analysis" to help analysts know the newest malware and methods.

Relations. In CSIC there are two internal relations:

a. Continuous feedback between "Data Mining & Analytics" and "Threat Intelligence Analysis" refines detection and response strategies.

Table 1: Incident response duration reduction by MCI R&D CSIC

Case name	incident response time in MCI CERT	incident response time with MCI R&D CSIC	incident response duration reduction
RFI attack on RBT portal	two days	one day	50 %
Cerber ransomware	ten days	seven days	33%
Zeus ransomware	six days	four days	33%
Bitcoin email spam	ten days	four days	60%
WAF botnet	sixteen days	six days	62.5%
Fake spam email	three days	two days	33%
LC Trojan	thirteen days	six days	53%

b. Information from “Net-OS-Mem Forensic” and “Malware Analysis” feeds into both “Threat Intelligence Analysis” and “Defend” to improve overall security measures.

3 Results

To evaluate the effectiveness of our proposed architecture, we reassessed multiple past incidents occurred within MCI CERT in 2016. We are allowed to publish seven incidents in this paper. The summary provided in table1.

Table 1 summerizes of duration reduction in presence of MCI R&D CSIC.

The case of Cerber ransomware infection was studied in technical and tactical intelligence. This malware was first detected by virus detection engines in early March 2016, leading to immediate antivirus signature updates. However, due to the lack of a CSIC in MCI CERT and unawareness of Cerber, the malware was only recognized when it infected one of the organization’s laptops in November 2016, with no information on how to clean the malware. The containment of the infection lasted about three days, and eradication and recovery took about two days. With the minimal CSIC implemented in MCI R&D, the requirement considered monitoring security trends and malwares. In the collection phase, we identified this malware in 6-8 days. In processing phase, the indicators and signatures recognized in 1-2 days. The analysis of the malware and the TTPs lasted about 12-16 days in the analysis phase, and the report was disseminated immediately. The entire cyber intelligence operation was completed in 26 days. Thus, the detection and identification time can reduced by about nine months with updated prevention mechanisms, and the time of containment, eradication, and recovery can be reduced by about two days and one day, respectively.

In the following case, we considered operational intelligence about the Zeus Trojan, first identified in 2007. One of Zeus Trojan's variants was detected in MCI CERT in 2016. With our minimal CSIC implementation in MCI R&D, the Requirement considered monitoring security trends and malwares. In the collection phase, we identified this malware in 4-6 days. In processing phase, the indicators and signatures recognized in

1-2 days. In the analysis phase, the time of analysis of the malware and the TTPs lasted about 8-12 weeks because this malware has many variants, and the analysis was very time-consuming. (Our analysis was conducted with the help of the MITRE ATT&CK framework, introduced in 2013 and not present in 2007 at the time of the Zeus attack.) The report was disseminated immediately. The entire cyber intelligence operation was completed in three months. Thus, the detection and identification time can reduced by about two years with updated prevention mechanisms, and the time of containment, eradication, and recovery can reduced by about two days.

Now, nine years after the first case evaluated in MCI CERT, we concluded to invest in establishing CSIC. This decision resulted from the strategic intelligence we created based on our risk management and overall business strategies.

The results indicate that establishing a Cyber Threat Intelligence Center significantly enhances an organization's ability to manage cybersecurity threats more effectively. The data supports the hypothesis that a structured, intelligence-led approach to cybersecurity not only enhances threat detection and response capabilities but also builds a resilient security posture that aligns with business continuity and growth.

4 Conclusion

In this research, we proposed a novel architecture for a CSIC, a crucial and novel concept of the new cybersecurity era, detailing the sub-components necessary to develop and run the CSIC. We also demonstrated how to integrate the CSIC with other security operations within the organization and with the organization's cybersecurity requirements. After evaluating CSIC functionalities, we empirically found that establishing a centralized CSIC could significantly reduce detection and response times. The CSIC with a modular architecture demonstrates scalability, allowing for implementation within the MCI as well as across a range of other organizations, thereby enhancing its applicability and utility.

Acknowledgment We express our sincere gratitude to Mobile Communication of Iran (MCI) for their financial support of this research. Their generous funding enabled us to conduct comprehensive studies and advance our work in Cyber Security Intelligence.

References

[1] "Global Threat Report", Crowdstrike, 2023.

[2] "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation", Juniper Research, 2022.

[3] D. E. Ozkaya, Practical Cyber Threat Intelligence, 2022.

[4] Kathryn Knerler, Ingrid Parker, Carson Zimmerman, 11 Strategies of a World-Class Cybersecurity Operations Center, The MITRE Corporation, 2022.

[5] Scott J. Roberts & Rebekah Brown, Intelligence Driven Incident Response, O'Reilly Media, Inc, 2017.

[6] Lucas José Borges Amaro , Bruce William Percilio Azevedo , Fabio Lucio Lopes de Mendonca, William Ferreira Giozza, Robson de Oliveira Albuquerque and Luis Javier García Villalba, "Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data", *applied sciences,* vol. 12, no. 1205, 2022.

[7] Seonghyeon Gong, Changhoon Lee, "Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform", *Electronics,* 2021.

[8] Anzel Berndt, Jacques Ophoff, "Exploring the Value of a Cyber Threat Intelligence Function in an Organization", in *Information Security Education. Information Security in Action*, 2020.

[9] James Kotsias, Atif Ahmad, Rens Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation", *European Journal of Information Systems,* vol. 32, no. 1, pp. 35-51, 2023.

[10] Tímea Páhi, Giuseppe Settanni, "Real-World Implementation of an Information Sharing Network", in *Collaborative Cyber Threat Intelligence*, Taylor&Francis, 2018.

[11] F. Skopik, Collaborative Cyber Threat Intelligence, CRC Press, 2018.

[12] J. N. M. Dahj, Mastering Cyber Intelligence, Packt Publishing, 2022.

[13] *NIST CYBERSECURITY FRAMEWORK,* 2022.

[14] Scott C. Fitch, Michael Muckin, "Defendable Architectures", Lockheed Martin Corporation, 2019.

[15] DAVID R. MILLER, SHON HARRIS, ALLEN A. HARPER, STEPHEN VANDYKE, CHRIS BLASK, Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2011.

Migration Aware Virtual Network Embedding in Software Define Networks

Arezoo Jahani[1]

[1]*Faculty of Electrical and Computer Engineering, Sahand University of Technology, Tabriz, Iran*
a.jahani@sut.ac.ir

Abstract

The development of Software Define Networks (SDN) networks and the of Network Function Virtualization (NFV) have provided the sharing of resources for cloud service providers. Developing effective virtual network embedding (VNE) algorithms for an SDN network is crucial to improve resource utilization. However, after allocating resources to a virtual network request, most existing VNE algorithms allocate the same resources to that request until the end of execution, which causes this problem in most cases; due to the existence of disconnection in the physical network graph, even with empty resources, it is not possible to map a new request. The proposed MaVNE method in this article models the VNE as a MILP problem and while calculating the migration cost of virtual networks, it tries to address the mentioned problem. The results of evaluation and comparison of the proposed method with basic methods show the power of the proposed method in increasing the acceptance ratio of virtual networks. But the cost of migration is added to the migrated networks. Therefore, by increasing the cost, which is the cost of immigration, the acceptance ratio can be increased.

Keywords: *Network Embedding, Network virtualization, Linear problem, Migration, Software Define Network.*

1 Introduction

The rapid advancement of cloud computing services and virtualization technologies has transformed how network resources are managed and utilized. Among these technologies, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) have emerged as key enablers, allowing for more flexible and efficient network management which make it possible to easily share resources between users using cloud resources. SDN decouples the control and data planes, providing centralized control over network resources, while NFV facilitates the virtualization of network functions, enabling dynamic and scalable deployment of services. Together, these technologies

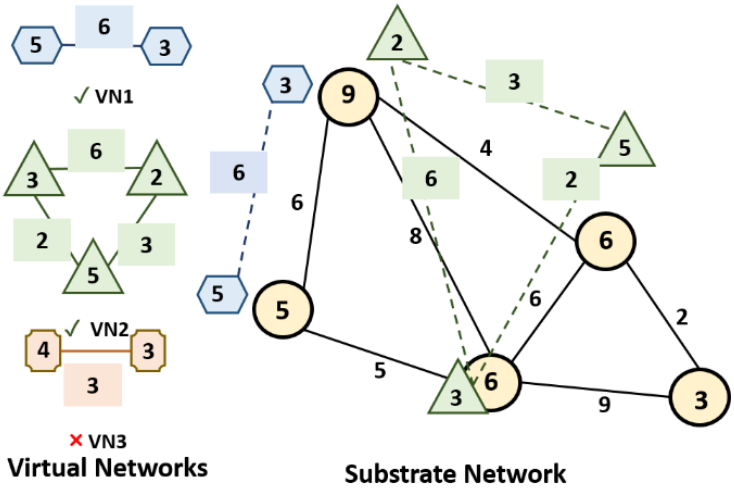

Figure 1: An example of two virtual networks embedding

have paved the way for the efficient sharing of network resources among multiple cloud service providers, giving rise to the concept of Virtual Network Embedding (VNE) [1].

VNE is a fundamental process in SDN-enabled networks that involves mapping virtual networks (VNs) onto a physical substrate network. The goal is to allocate the physical resources such as bandwidth, CPU, and memory to meet the demands of multiple VNs while optimizing resource utilization across the entire network. Effective VNE algorithms are critical for enhancing the overall efficiency and performance of SDN-based networks [2]. These algorithms must address the challenges of resource allocation in a dynamic and often unpredictable network environment, where demand can fluctuate and network topologies may change. An example of VNE is demonstrated in Fig. 1.

As shown in Fig. 1, there is a substrate network with five nodes whose resource capacity is written on nodes and seven links which their bandwidth capacity is written on links. Also, there are three different VNs with node requirements and link bandwidths. A VNE problem is looking to find a better place on the substrate network for VNs and the goal is increasing the acceptance ratio and revenue, and decreasing the cost. In Fig. 1, VN1 and VN2 are embedded successfully, but VN3 is not embedded, although there are enough resources, the resources are disconnected.

However, a significant limitation of most existing VNE algorithms is their static approach to resource allocation. Once resources are assigned to a VN request, they remain fixed for the duration of the request, regardless of changes in network conditions. This static allocation can lead to inefficiencies, particularly in scenarios where the physical network graph experiences disconnections or where available resources become fragmented [1, 3]. In such cases, even when there are sufficient resources available, the inability to reallocate or migrate resources dynamically can prevent the accommo-

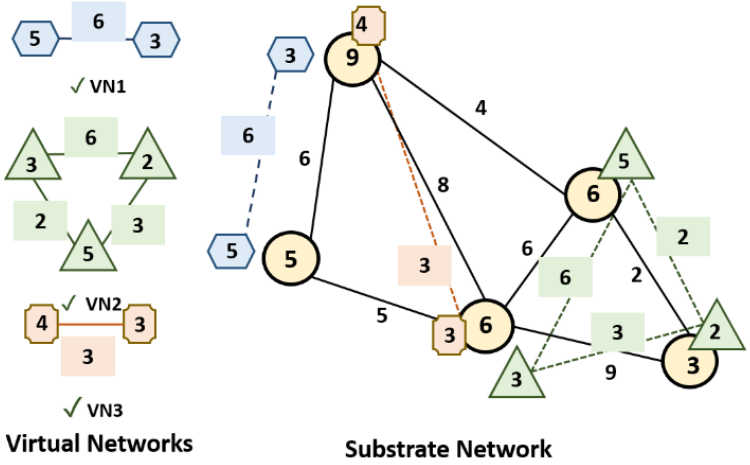

Figure 2: An example of substrate and virtual network

dation of new VN requests, thereby reducing the acceptance ratio of the network. This problem is shown in Fig. 1 which the VN3 is not mapped successfully, although there are enough resources. The problem is that the resources are disconnected and just by changing the mapping location of one of the requests, enough connected space will be created for the third request as shown in Fig. 2.

As shown in Fig. 2, imagine that VN3 is arrived after VN1 and VN2. After embedding the VN1 and VN2 like Fig. 1, there is not any enough connected resource to assign to VN3. But by changing the mapping location of one of the requests, enough connected space has been created for the third request as well.

To address these challenges, this paper proposes a Migration-Aware Virtual Network Embedding (MaVNE) approach that models the VNE problem as a Mixed Integer Linear Programming (MILP) problem. The MaVNE method introduces a dynamic resource allocation strategy by incorporating migration costs into the VNE process. By calculating the potential migration cost and considering it in the decision-making process, the MaVNE approach aims to improve the overall acceptance ratio of VN requests while managing the trade-off between resource utilization and migration overhead.

The rest of the paper is organized as follows: Section 2 provides a review of related work in the field of VNE. Section 3 details the proposed MaVNE methodology, including the formulation of the MILP problem and the migration cost model. Section 4 presents the experimental setup and results, comparing the performance of the proposed method with baseline approaches. Finally, Section 5 concludes the paper with a discussion of the findings and potential directions for future research.

2 Related Works

The VNE has attracted a lot of attention in recent years. The proposed methods for this problem can be examined from different aspects, most of which are shown in Fig. 3.

As seen in Fig. 3, VNE problems can be classified into two categories: static or dynamic. Static problems are problems in which all requests are known at the beginning of resource allocation, and resource allocation is done once, and all requests must use the same resources until the end of execution. But in dynamic mode, requests are entered into the system in order, and the number of times and the time of execution of the proposed algorithm is usually uncertain and depends on things such as the time of entering a new request [1].

The next item is the objectives of algorithms related to VNE problems, which include: cost [2], revenue, security [3], acceptance rate, and topology [4]. Most of the articles related to VNE seek to increase the revenue of the service provider, reduce the cost of the user and increase the acceptance ratio in the sense of increasing the number of received requests. Some of the latest articles also examine security and try to use physical resources that have the same security level as virtual nodes as much as possible to map virtual networks. Some articles also look for mapping based on network topology and try to use resources that lead to non-separation of the network by knowing the network topology.

Mapping of virtual networks is done in two phases: node mapping and link mapping. Node mapping is the concept of choosing suitable physical nodes for virtual nodes, which is usually done by methods such as ranking [5] or prioritizing nodes, or giving credit to nodes. Link mapping is also usually done by algorithms of finding the shortest path or commodity flow. Now, these two phases can be done in coordination [6] with each other or uncoordinated. Coordination means to think about the link mapping phase in the node mapping phase and sometimes to change the node mapping in order to achieve the goals in the next phase. This mode itself can be classified into two other cases, which are two-phase and single-phase. In the two-phase stage, the two stages of node and link mapping are performed separately and sequentially, but in the single-phase stage, the two stages are performed completely side by side.

VNE algorithms can be executed in one of two central [7] or distributed [8] modes. In centralized mode, only one node is responsible for managing the entire physical network. But in the distributed mode, the responsibility of managing the network in a distributed manner is the responsibility of several components that must communicate with each other peacefully. Also, the methods proposed in previous articles can be classified as linear programming methods, statistical methods [9], or methods based on machine learning or deep learning.

Linear programming based methods use problem modeling as a linear or non-linear programming problem and then look for a solution by searching the complete or pruned state space [10]. But statistical methods by estimating the result and machine learning

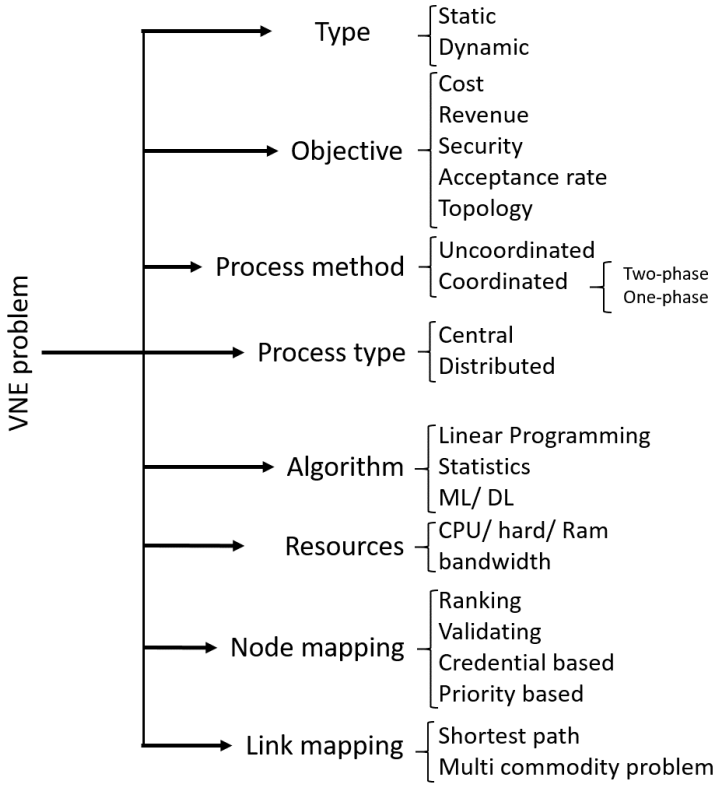

Figure 3: Classification of VNE problems

methods by learning and testing do this [11]. In node mapping, the resources that must be allocated from physical nodes to virtual nodes include processor, memory, and hard drive, and in link mapping, resources such as bandwidth are considered.

3 Proposed MaVNE method

The proposed MaVNE method is a VNE solution which model it as a Mixed-Integer Linear Programming (MILP). The main contribution of the proposed method is its migration awareness. After allocating resources to a request, the previous methods did not reclaim the resources until the end of the execution, and this problem led to the problem shown in Fig. 1 and 2, which the proposed method addressed. Therefore, the proposed method has a modeling of the VNE problem that this model is re-executed during the following three states and each time it is executed, all allocated resources are withdrawn to be re-allocated.

- A new virtual network request arrives
- Completing the arrival of an allocated virtual request

Table 1: Notation

Parameters	
$G_s = (N_s, L_s)$	Substrate network
$N_s = \{R_i \mid i \in N_s\}$	Substrate nodes with their amount of resource
$L_s = \{BW_{ij} \mid i \to j \in L_s\}$	Substrate links with their amount of bandwidth
$G_v = (N_v, L_v)$	Virtual network
$N_v = \{R_u \mid u \in N_v\}$	Virtual nodes with their amount of request
$L_v = \{BW_{uv} \mid u, v \in N_v,\ u \to v \in L_v\}$	Virtual links with their amount of required bandwidth
$R_v = (G_v, Stime_v, deadline_v)$	Virtual Request with their submitted time and deadline
i, j	Substrate nodes
u, v	Virtual nodes
$cost_{migration}$	Migration cost
M	A fix time size for extending the simulation time
Variables	
X_{uv}^{ij}	Binary variable, virtual link $u \to v$ is mapped on substrate link $i \to j$
Y_v^i	Binary variable, virtual node v is mapped on substrate node i
$delay_v^t$	Delay of virtual request v at time t
P_{uv}	The path for mapping virtual link L_{uv}

- Elapse of a predetermined fixed period of time

But we must note that with this work, a request may receive different resources during two consecutive executions, which forces migration for these types of requests.

The required notations are demonstrated in Table 1 and as demonstrated we model the substrate and virtual networks as an undirected graph with nodes and links. The nodes have resources like CPU, Ram, and hard. The links have resource like bandwidth.

The proposed MILP model for VNE is shown in Equation P1 which is a minimization problem. The objective function has fine different sections which are combined and are; (I) node mapping cost, (II) link mapping cost, (III) migration cost, if the location of nodes are changed, (IV) migration cost, if the location of links are changed, and (V) delay of virtual requests. In fact, the model minimize the embedding cost which is based on the amount of resources are used for each mapping (both of the nodes and links), the migration cost which is based on the happened migration for both of the nodes and links, and the delay for all available requests.

The constraints are shown in Equations (p1a) to (p1g). In fact, constraint (p1a) demonstrates that the amount of bandwidth of physical links allocated to virtual links should be sufficient. (p1b) demonstrates that the amount of resources required by virtual nodes should not be more than the resources available in physical nodes. Constraint (p1c) demonstrates each virtual link should be mapped on a physical path whose size is equal to the size of the path for which the virtual link is selected. Constraint (p1d) demonstrates each virtual node should mapped on only one physical node. Constraint (p1e) demonstrates that the delay of each virtual request should computed with comparing the simulation time (t) with their deadline time. Constraints (p1f)-(p1h) manage

the range of possible answers.

$$\begin{aligned}\min \sum_{i,j\in G_s}\sum_{u,v\ \in G_v} X_{uv}^{ij} * \ BW\left(L_{uv}\right) \\ + \sum_{i\in G_s}\sum_{v\in G_v} R_v * Y_v^i \\ + \sum_{i,j\in G_s}\sum_{u,v\in G_v}\sum_{t\in time} cost_{migration}\left(\left(X_{uv}^{ij}\right)_t - \left(X_{uv}^{ij}\right)_{t-1}\right) \\ + \sum_{i\in G_s}\sum_{v\in G_v} cost_{migration}\left(\left(Y_v^i\right)_t - \left(Y_v^i\right)_{t-1}\right) + \sum_{R_v}\sum_{t\in time} delay_v\end{aligned} \tag{p1}$$

$s.t$:

$$\sum_{i,j\in G_s} X_{uv}^{ij} * BW\left(L_{uv}\right) \le BW(L_{ij}) \qquad \forall u,v\in G_v \tag{p1a}$$

$$\sum_{i\in G_s} Y_v^i * R_v \le R_i \qquad \forall v\in G_v \tag{p1b}$$

$$\sum_{i,j\in G_s} X_{uv}^{ij} \le |P_{u,v}| \qquad \forall i,j\in G_s, \forall u,v\in G_v \tag{p1c}$$

$$\sum_{i\in G_s} Y_v^i \le 1 \qquad \forall i\in G_s, \forall v\in G_v \tag{p1d}$$

$$delay_v^t \ge \sum_{v\in N_s} Y_v^i * (t - delay_v) \qquad \forall t\in time, \forall v\in G_v \tag{p1e}$$

$$X_{uv}^{ij} \in \{0,1\} \tag{p1f}$$

$$Y_v^i \in \{0,1\} \tag{p1g}$$

$$delay_v^t \ge 0\ ,\ P_{uv} \ge 0 \tag{p1h}$$

As shown in problem (p1), the simulation time is the time which passed by one of these events (receiving a new request, completing one of the accepted requests, or passing a fix time size) and its initial value is zero. For better understanding focus on Fig. 4.

As shown in Fig. 4, imagine that there are four requested networks which three of them arrived at time zero. So, the first simulation time (sim_time0) is equal to zero. In order to extend the simulation time, there is three rules: (1) a request is completed. (2) a new request is arrived. (3) a fix time is elapsed.

With extending the simulation time, the MILP model is executed again. But for each execution of the proposed MILP model, all of the assigned resources should be released and all of the not completed requests should be update their remained time for using the resources. This is the point that can address the problem shown in Fig. 1, and Fig. 2.

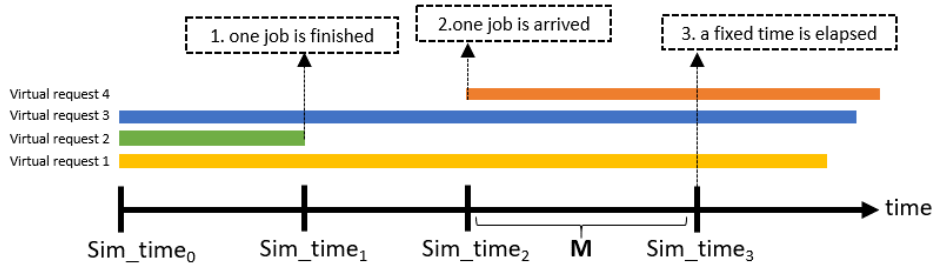

Figure 4: Three different events for expanding the simulation time

Table 2: Evaluation parameters

Substrate network	
Node numbers, link numbers	20, 54
Node capacity	[20, 70], uniform distribution
Link bandwidth	[10, 50], uniform distribution
Virtual network	
Node numbers, link numbers	[2,4], [3,7]
Node capacity	[2, 10], uniform distribution
Link bandwidth	[1, 15], uniform distribution
Arrival time	Poisson distribution
deadline	random
Fix time	20 second
Simulation	
Language, framework	Python, Pyomo
Mipgap = 0.5	A Pyomo parameter for search tree pruning

4 Evaluation of MaVNE

In order to evaluate the proposed MaVNE method, we used a random topology for substrate and virtual networks which are formed by NSG2.1 (graphical GT-ITM) [13]. The used parameters are shown in Table 2.

As shown in Table 2, we imaged that there is a substrate network with 20 nodes and 54 links. The nodes' capacity obeys a uniform distribution, between 20 and 70 and the link bandwidth also obeys the uniform distribution which is between 10 and 50. The virtual network has minimum 2 nodes and maximum 4 nodes. Also have minimum 3 and maximum 7 links. The requests arrival time obeys the Poisson distribution with random number for deadline. We implemented the proposed MaVNE and the previous paper EE-CTA in python, Pyomo and evaluated it on a Windows based system with 16G Ram, and a CPU corei7, 1.80 GHz, 11 generation.

4.1 Simulation results

We compared the proposed MaVNE with EE-CTA [1] which was a topology-aware VNE method and used a decomposition method for slicing the substrate network for better

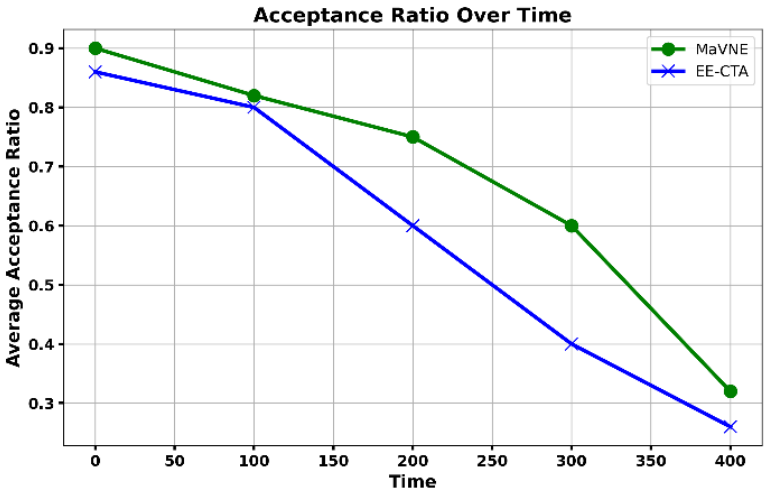

Figure 5: Average acceptance ratio over time

mapping to avoiding the problem of mentioned in Fig. 1 and Fig. 2. So, the EE-CTA was the best method for comparing with our proposed method. The acceptance ratio and the cost for different number of VNs are demonstrated respectively in Fig. 5 and Fig. 6.

As shown in Fig. 5, the average acceptance ratio decreases over time, which is due to busy resources due to an increase in the number of requests. Requests are entered into the system with Poisson distribution, and with the arrival of each new request or the completion of one of the previous requests or the passage of a fixed period of time, the allocation of resources for all requests starts again from the beginning. Also, for each reassignment, the time required for the tasks that had previously received resources but have not yet been completed is recalculated. According to Fig. 5, the proposed MaVNE method has a higher acceptance rate compared to the previous EE-CTA method, and this increase in acceptance rate is due to the ability of the proposed method to reallocate resources for all new requests and requests that have not yet been completed. We have assumed that we know the time required to execute the requests. While in the real environment, it is necessary to calculate the required time of requests usually by methods such as estimation or prediction.

As shown in Fig. 6, the cost spent on mapping requests increases with time. We have calculated this cost in two ways. One is when we have measured the migration cost of the proposed method and the other is when we have ignored the migration cost of the proposed method. The first case is shown in Fig. 6 and the second case is shown in Fig. 7.

When we included the migration cost for the requests that used different resources during different time periods, the average cost in the proposed method of MaVNE was higher than the previous EE-CTA method. However, it is necessary to bear the cost

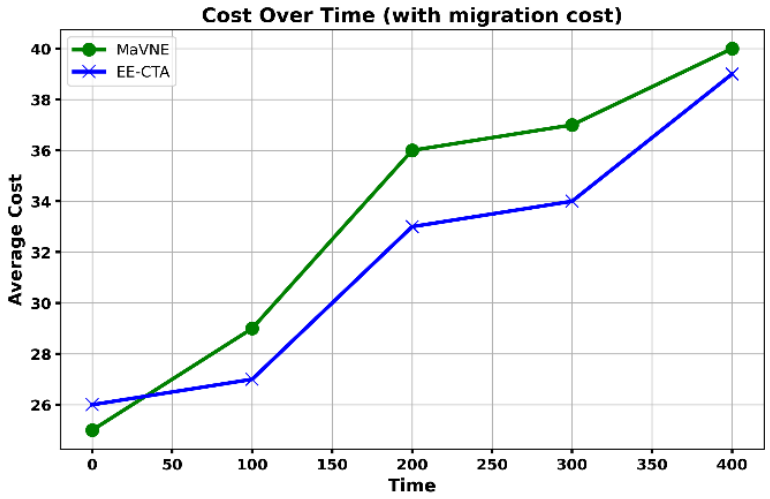

Figure 6: Average cost over time (with migration cost)

of immigration in order to increase the acceptance rate. Also, to prove the issue once again in Fig. 7, we omitted the cost of migration and the results show that in this case, the cost was significantly reduced compared to the previous method, but it is natural that in the real environment, the cost of migration cannot be omitted. And the bottom line is that in order to increase the acceptance rate, the cost of immigration must be borne. Note that the cost of migration does not cause a problem in the previous EE-CTA method. Because the previous method does not allow requests to migrate, and all requests from the first time they receive resources, must use the same resources until the end of execution and are not allowed to change resources.

As the last evaluation test, we compare the execution time of the proposed MaVNE and EE-CTA and the results are shown in Fig. 8.

As demonstrated in Fig. 8, the average execution time in the proposed MaVNE method is as close as the previous EE-CTA method. Although the EE-CTA sometimes has less execution time, it's because of not adding the executed requests to the allocation process again. However, the proposed MaVNE for each running the VNE problem, releases all the resources and assigns again all of the resources from the beginning.

5 Conclusion and future work

In order to solve the problem of not being able to allocate resources when there are sufficient and unrelated resources, MaVNE method was proposed. The proposed method can update the simulation time in the following three cases: when a running request ends. When a new request enters the system. When a fixed predetermined period of time elapses. With these explanations, the proposed MaVNE method can first retrieve all the available resources and then map all the resources from the beginning every time

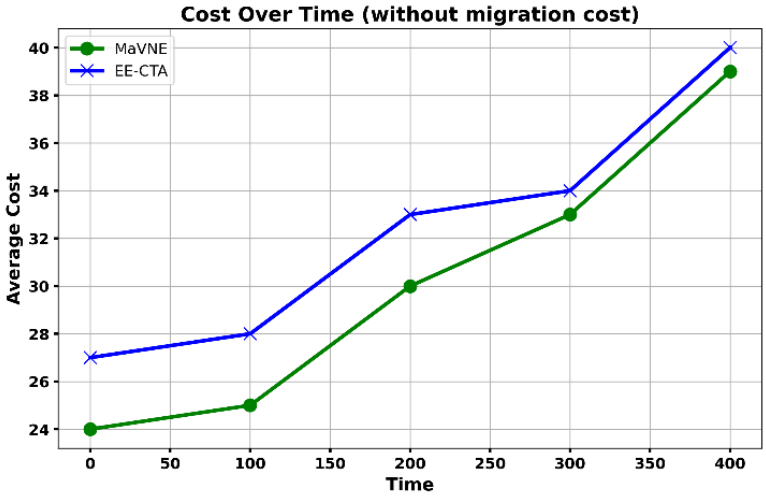

Figure 7: Average cost over time (without migration cost)

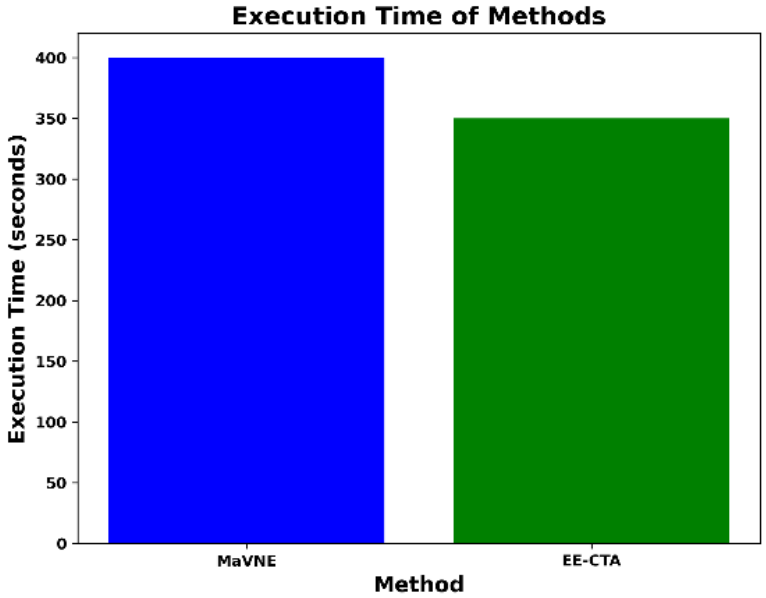

Figure 8: Average execution time

the resource allocation algorithm is re-executed. This will increase the acceptance rate. However, the cost of mapping increases due to the need to migrate requests to which the assigned resource has changed. Therefore, in order to increase the acceptance rate, it is necessary to bear the cost of immigration.

References

[1] Jahani, Arezoo, et al. "EE-CTA: Energy efficient, concurrent and topology-aware virtual network embedding as a multi-objective optimization problem". Computer Standards & Interfaces, Vol. 66, 2019, pp. 103351.

[2] Nguyen, Huu Thanh, et al. "A generalized resource allocation framework in support of multi-layer virtual network embedding based on SDN". Computer Networks 92, Vol. 2015, pp. 251-269.

[3] Wang, Yang, et al. "Minimum-cost embedding of virtual networks: An iterative decomposition approach". Computer Networks, Vol. 234, 2023, pp. 109907.

[4] Liu, Shuhao, et al. "Towards security-aware virtual network embedding". Computer Networks, Vol. 91, 2015, pp. 151-163.

[5] Cheng, Xiang, et al. "Virtual network embedding through topology awareness and optimization". Computer Networks, Vol. 56, Issue. 6, 2012, pp. 1797-1813.

[6] TG, Keerthan Kumar, et al. "NORD: NOde Ranking-based efficient virtual network embedding over single Domain substrate networks". Computer Networks, Vol. 225, 2023, pp. 109661.

[7] Duan, Zhonglei, and Ting Wang. "Towards learning-based energy-efficient online coordinated virtual network embedding framework". Computer Networks, Vol. 239, 2024, pp. 110139.

[8] Zhang, Shengyu, and Kwan L. Yeung. "Location constrained virtual optical network embedding in space-division multiplexing elastic optical networks". Computer Networks, Vol. 220, 2023, pp. 109475.

[9] Beck, Michael Till, et al. "Distributed and scalable embedding of virtual networks". Journal of Network and Computer Applications Vol. 56, 2015, pp. 124-136.

[10] Dandachi, Ghina, et al. "A robust control-theory-based exploration strategy in deep reinforcement learning for virtual network embedding". Computer Networks, Vol. 218, 2022, pp. 109366.

[11] Moreira, Cristiano L., Carlos A. Kamienski, and Reinaldo AC Bianchi. "5G and edge: A reinforcement learning approach for Virtual Network Embedding with cost optimization and improved acceptance rate". Computer Networks, Vol. 247, 2024, pp. 110434.

[12] Lim, Hyun-Kyo, et al. "Reinforcement learning-based virtual network embedding: A comprehensive survey". ICT Express 9.5, 2023, pp. 983-994.

[13] E.W. Zegura , K.L. Calvert, S. Bhattacharjee , How to model an internetwork, in: Proceedings of the INFOCOM'96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE, Vol. 2, 1996, pp. 594–602.

The Future of Artificial Intelligence, From Cognitive Science to Superintelligence

Mohammad Taha Ghaempanah[1]

[1]*PhD Student in Communication Sciences, Soore University, Tehran, Iran*
mt.ghaempanah@iran.ir

Abstract

Artificial intelligence, as one of the most significant developments of the cyber age, is rapidly advancing. From voice assistants to self-driving cars, AI is transforming the way we live and work. But what does the future hold for AI? Could we one day witness the creation of superintelligence that surpasses human intelligence? To answer this question, this research investigates the evolution of AI, from its roots in cognitive science to a future vision where AI might reach a level of intelligence that surpasses humans, manifesting as a superintelligence. The aim of this paper is to examine the trajectory of AI and its potential impact on the future of humanity. It also emphasizes the importance of understanding the nature of AI and developing it based on ethical principles. The researcher has employed a qualitative research approach to examine and analyze existing data, trends, and predictions about the future of AI. The results of this research indicate that the future of AI is very promising and has the potential to change the world, but it will also be accompanied by serious challenges. To make the best use of this technology and avoid its negative consequences, while humans must prepare for a future in which AI plays a significant role, research and development in this field must continue simultaneously, along with attention to ethical issues.

Keywords: *Artificial Intelligence, Superintelligence, Cognitive Science, Neural Networks, Machine Learning.*

1 Introduction

Artificial Intelligence is one of the most passionate and rapidly growing research fields in the 21st century. Its roots can be traced back to the early decades of the 20th century, but recent significant advancements in machine learning and deep learning have transformed AI into a primary driving force in many industries. The rapid progress in the field of AI has raised important questions about the future of AI and its impact on society and humanity. without any doubt One of the most important of these questions is the possibility of achieving superintelligence and its consequences for humankind.

Considering the recent advancements in AI, especially machine learning and deep neural networks, the possibility of achieving systems that surpass human intelligence is not far-fetched.

Human intelligence and artificial intelligence have long been intertwined, evolving along parallel paths throughout history. As humans have sought to understand and replicate intelligence, artificial intelligence has emerged as a field dedicated to creating systems capable of performing tasks that traditionally require human intellect [1]. Examining the future of artificial intelligence, particularly the possibility of achieving superintelligence in the cyber age, is of paramount importance for the following reasons:

- **Impact on daily life:** AI is increasingly permeating our daily lives, and understanding its future is essential for both individual and collective planning and decision-making.
- **Ethical and social challenges:** The development of AI is accompanied by serious ethical and social challenges that require careful examination and analysis.
- **New opportunities:** AI can create new opportunities to address global challenges such as diseases, climate change, and poverty.

The primary objective of this research, considering the key points of the present study (factors influencing the development of artificial intelligence, obstacles and challenges in developing superintelligence, the consequences of human achievement of superintelligence, the ethical development of artificial intelligence, and the role of humans in artificial intelligence), is to examine the evolution of artificial intelligence, from its roots in cognitive sciences to a future vision where artificial intelligence may reach a level of intelligence that surpasses humans, manifesting as a superintelligence.

Given the existing gaps in the research literature, this research endeavors to address this topic by adopting an interdisciplinary approach and considering the technical, social, and ethical dimensions of artificial intelligence.

2 Literature review

Based on the researcher's comprehensive review of the scientific literature on artificial intelligence, it has been concluded that: Previous research in the field of artificial intelligence has primarily focused on the technical and applied aspects of this technology. While these studies have provided valuable information about the capabilities of AI, they have not adequately addressed the social, ethical, and philosophical dimensions of this technology. Additionally, many studies have focused on short-term predictions and have paid less attention to the long-term outlook of AI. In this section, we will review several studies conducted in this scientific field, followed by an identification of the existing gaps in knowledge.

Savaliya (2024) in a study on the 'Future of Artificial Intelligence,' states that artificial intelligence has made significant advancements and has impacted various industries, increasing productivity through technologies such as machine learning and natural language processing. She further concludes that the future of AI involves advancements in cognitive science and aiming for superintelligence, emphasizing responsible development, ethical considerations, and collaboration for a smarter world [2].

Singh et al (2023) in their research titled 'Artificial Intelligence, the Future' emphasize that the development of AI technologies such as machine learning, natural language processing, and computer vision has transformed processes in fields like healthcare, finance, and transportation, increasing productivity and impacting how we live and work. AI will advance from cognitive science to superintelligence, encompassing AI categories like ANI, AGI, and ASI, with predicted potential economic impacts and job shifts [3].

Verma and Nasir (2023) conducted a study titled 'Artificial Intelligence and its Future'. This paper highlights the rapid pace of AI advancement, which may be surprising given the complexity of the technology involved. Their findings suggest that the widespread penetration of AI into various industries, including those traditionally unrelated to technology, demonstrates its adaptability and unexpected versatility. The paper also indicates that the integration of AI into daily life is happening more seamlessly and quickly than anticipated, signaling a shift in societal norms regarding technology use [4].

"Artificial Intelligence, the Future is Now" is the title of a research study conducted by Baldwin (2023). This paper notes that artificial intelligence, despite its long history dating back to the 1950s, has recently seen a surge in popularity and relevance, particularly following the launch of OpenAI's ChatGPT in early 2023, which may be surprising given the previous development timeline of AI [5].

Agrawal et al (2023) in their research titled "Enhancing Perception in Artificial Intelligence through Cognitive Science Principles" delves into the cognitive functions of perception and connects cognitive science principles to artificial intelligence, which can lead to improved performance and efficiency in AI systems. It also identifies gaps in the current performance of AI compared to the capabilities of the human brain and suggests new avenues for research in perceptual systems [6].

Based on the reviews conducted in the existing research literature, the following gaps have been identified:

- **Lack of interdisciplinary research:** Most research in the field of AI is conducted within a specific discipline (such as computer science or philosophy) and has paid less attention to the interaction between different disciplines.
- **Insufficient attention to ethical dimensions:** Many studies have addressed the technical aspects of AI and have not paid sufficient attention to the ethical issues associated with this technology.
- **Absence of a comprehensive framework for assessing the future of AI:**

Despite significant progress, there is still no comprehensive and accepted framework for assessing the long-term implications of AI.

3 Significance and Necessity of the Research

3.1 Significance of the Research

Research in the field of artificial intelligence, especially regarding its future, is of paramount importance. This significance is due to several reasons, some of which are mentioned below:

3.1.1 The Widespread Impact of Artificial Intelligence on Daily Life

- **Automation of Processes:** Artificial Intelligence is transforming the way tasks are performed across numerous industries. From manufacturing to services, AI can automate processes and increase efficiency.
- **Intelligent Decision Making:** In fields such as medicine, finance, and transportation, AI can aid in making better and more accurate decisions.
- **Human Interaction and Communication:** With the advancement of AI, the ways we communicate and interact with each other and devices are changing. Voice assistants, chatbots, and virtual reality are examples of these changes.

3.1.2 Ethical and Social Challenges

- **Algorithmic Bias:** Artificial intelligence can reinforce discrimination and inequality if its training data is biased.
- **Privacy:** The collection and use of personal data to train AI algorithms raises serious privacy concerns.
- **Unemployment:** The automation of processes by AI can lead to significant job losses.
- **Accountability:** Determining liability in the event of errors or harm caused by AI systems can be very complex.

3.1.3 New Opportunities

- **Solving Global Challenges:** Artificial intelligence can help solve some of the world's most pressing challenges such as climate change, diseases, and poverty.
- **Innovation and Creativity:** AI can be used as a powerful tool for innovation and creativity in many fields.

- **Economic Development:** Investing in AI research and development can contribute to economic growth and the creation of new job opportunities.

3.1.4 From Cognitive Science to Superintelligence

- **Cognitive Science:** The study of the human mind and cognitive processes helps researchers improve artificial intelligence algorithms and equip them with more complex capabilities such as learning, reasoning, and creativity.

- **Superintelligence:** This refers to a hypothetical intelligence that is far superior to human intelligence. Research on superintelligence seeks to understand the limitations and opportunities of such AI, as well as to develop ethical principles for its development and use.

3.2 Necessity of the Research

Given the widespread and profound impact of artificial intelligence on human lives and societies, research in this field is of paramount importance. Researchers should strive to develop AI technologies that are safe, ethical, and beneficial to humanity. Moreover, they should examine the social, economic, and ethical implications of AI and provide solutions to address its challenges.

In sum, research in AI is an imperative and can help us harness the benefits of this technology while mitigating its risks.

4 Research goals

With ambitious goals, AI research is rapidly evolving. Researchers seek to emulate the human mind, solve complex problems with intelligent systems, and ultimately, achieve artificial general intelligence. The following sections delve into specific objectives of this research:

4.1 Mimicking Human Intelligence

- **Deeper Understanding of the Human Mind:** Researchers are striving to develop more accurate computational models of learning, memory, decision-making, and creativity by studying the human brain and cognitive processes.

- **Development of Deep Learning Systems:** The primary goal of this area is to create systems that can learn from data and improve independently.

- **Creation of Powerful Natural Languages:** Developing systems that can understand and generate natural language to enable more effective human-machine interaction.

4.2 Solving Complex Problems

- **Development of Advanced Algorithms:** Creating algorithms capable of solving complex problems in various fields such as medicine, engineering, finance, and social sciences.
- **Application of AI in Various Sciences:** Utilizing AI to discover new drugs, design new materials, predict natural events, and many other applications.

4.3 Achieving Artificial General Intelligence (AGI)

- **Development of a system with general intelligence**: Creating systems capable of performing any task that a human can.
- **Understanding and Solving Abstract Problems:** Ability to understand abstract concepts, reason logically, and learn from experience.
- **Creativity and Innovation:** Ability to generate new ideas and solve problems in innovative ways.

4.4 Developing Superintelligence

- **Creating Systems with Intelligence Far Beyond Humans:** Developing systems that can surpass humans in all areas.

5 Research questions and hypotheses

5.1 Key questions

5.1.1 Limitations of Artificial Intelligence

- To what extent can we approximate human intelligence with artificial intelligence?
- Can AI experience creativity, consciousness, and emotions?
- What are the fundamental obstacles to creating artificial general intelligence?

5.1.2 Social Impacts

- How will artificial intelligence impact the job market, social structures, and international relations?
- What are the ethical and legal challenges in developing and using AI?
- How can we prevent potential risks of AI such as mass unemployment, inequality, and misuse?

5.1.3 Cognitive science and artificial intelligence

- How can human cognitive models be used to improve machine learning algorithms?
- What is the relationship between brain structure and artificial neural network architecture?
- Can consciousness be computationally modeled?

5.1.4 Artificial superintelligence

- Is it technically feasible to develop artificial superintelligence, and if so, what timeline is realistic?
- What are the existential risks associated with the development of superintelligence?
- How can we ensure the safe and beneficial development of superintelligence?

5.2 Research Hypotheses

- **Convergence Hypothesis:** This hypothesis says as technology advances and our understanding of the brain deepens, the gap between artificial intelligence and human intelligence will gradually narrow.
- **Evolution Hypothesis:** Similar to living organisms, artificial intelligence will become more complex and intelligent through continuous evolution and learning.
- **Fundamental Limitations Hypothesis:** Artificial intelligence will always face inherent limitations and will never be able to fully replicate human intelligence.
- **Existential Risk Hypothesis:** The development of superintelligence could pose a serious threat to human survival unless appropriate safeguards are put in place.
- **Coexistence Hypothesis:** Humans and artificial intelligence can coexist and evolve together.

6 Research method

Given the interdisciplinary and future-oriented nature of the topic, designing a classic quantitative study with a defined population and standardized measurement tools is challenging. Instead, a combined approach of qualitative and quantitative methods may be more suitable for answering the research questions. The research design adopted in this study was conducted in four stages. In stages two through four, data was collected from 120 experts in related fields (opinion leaders, professors, and students) at universities in Tehran Province, and subsequently analyzed:

1) Systematic Literature Review: To identify, evaluate, and synthesize previous research in the fields of artificial intelligence, cognitive sciences, superintelligence, ethics in AI, and its social impacts, reputable scientific databases such as Scopus, Web of Science, and Google Scholar were used to search for relevant articles, books, and reports.

2) Semi-structured Interviews: In order to collect qualitative data from experts in the fields of artificial intelligence, communications, and sociology to gain a deeper understanding of the challenges, opportunities, and diverse perspectives on the future of AI, a guide questionnaire, including open and closed-ended questions, was used.

3) Content Analysis: To identify patterns, key concepts, and dominant viewpoints in texts and interviews, the qualitative data was coded manually and using the NVivo content analysis software.

4) Delphi Method: To achieve expert consensus on the future of AI and prioritize its challenges and opportunities, several interviews were conducted with a selected group of experts. In this stage, the initial opinions were presented to the participants, and this process was repeated until consensus was reached.

In this research, to increase validity, methods such as content validity and construct validity were used, and to increase reliability, methods such as intra-rater reliability and inter-rater reliability were employed. In order to analyze the data, qualitative analysis methods such as coding, categorization, and interpretation were used to identify patterns, concepts, and main themes in the interview data and texts. Given this design, the present study can achieve comprehensive results regarding the future of AI and assist policymakers, researchers, and the general public in making informed decisions.

7 Core concepts of the research

7.1 Cognitive Science and Artificial Intelligence

Cognitive science delves into the study of human mental processes, encompassing perception, learning, language, and decision-making. Its primary objective is to comprehend the nature of intelligence and construct computational models thereof. Inspired by cognitive science, artificial intelligence endeavors to create systems capable of performing tasks analogous to those carried out by humans.

Cognitive science uses a framework based on four key concepts: emergence, nonlinearity, self-organization, and universality. This framework incorporates ideas from systems theory, nonlinear dynamics, and synergy. By using this approach, cognitive science can study cognition in its various complex forms using a variety of methods. [7].

7.2 Machine Learning

Machine learning is a critical subfield of artificial intelligence that empowers systems to learn from data and improve over time. Machine learning algorithms are inspired by the human brain's learning processes.

The scientific study of algorithms and statistical models when used by computer systems to perform a specific task without being explicitly programmed is known as machine learning. These algorithms construct a mathematical model based on sample data [8].

7.3 Artificial Neural Networks

Artificial neural networks are inspired by the structure of the human brain. These networks consist of a large number of interconnected artificial neurons that can process information.

Artificial neural networks can successfully solve prediction problems by using a combination of flexible nonlinear functions and delayed variables [9].

7.4 Superintelligence

Superintelligence refers to a hypothetical agent that possesses intellectual ability far surpassing that of the brightest and most gifted human mind. Such a system would be capable of solving extremely complex problems, making groundbreaking discoveries, and potentially even exerting dominance over humans.

Superintelligence refers to a hypothetical intelligence that significantly exceeds the intellectual capacity of the brightest and most gifted human minds [10].

8 Research findings

Research into the future of artificial intelligence, particularly in relation to cognitive science and superintelligence, will yield highly diverse and extensive results due to the rapid pace of advancements and complexities within this field. However, based on current trends and existing research, some of the most significant outcomes can be summarized as follows:

8.1 A deeper understanding of the human brain and intelligence

- **More accurate brain models:** By combining cognitive science and artificial intelligence, we can create far more accurate models of the human brain's functions, leading to a better understanding of learning, memory, decision-making, and creativity.
- **Treatment of brain diseases:** This deep understanding can lead to new and more effective treatments for brain diseases such as Alzheimer's and Parkinson's.

8.2 Significant Advances in Artificial Intelligence

- **Artificial General Intelligence:** The possibility of achieving Artificial General Intelligence (AGI), capable of performing any intellectual task that a human being can, is a serious one.
- **Creative AI:** AI could, in the future, engage in creative endeavors such as art, music, and literature, generating novel works.
- **Conscious AI:** Some researchers believe that we may one day achieve conscious AI, although this remains a highly controversial topic.

8.3 Socioeconomic Transformations

- **Labor market:** Artificial intelligence can significantly transform the labor market, eliminating or altering many jobs.
- **Inequality:** Increasing economic inequality is a major concern regarding the development of AI.
- **Governance and politics:** AI can play a significant role in political and social decision-making, potentially leading to new forms of governance.

8.4 Ethical and Social Challenges

- **Bias and discrimination:** AI algorithms may contain human biases and lead to discrimination against certain groups.
- **Accountability:** Determining accountability for decisions made by complex AI systems is challenging.
- **Security:** Securing AI systems and preventing their misuse is a significant challenge.

8.5 New Opportunities

- **Solving global problems:** Artificial intelligence can play a significant role in solving some of the world's most pressing problems, such as climate change, disease, and poverty.
- **Increasing productivity:** AI can lead to increased productivity in many industries.
- **Improving quality of life:** AI can contribute to improving the quality of human life by providing better services in healthcare, education, and transportation.

8.6 The Role of Humans in the Future of Artificial

Over the past few decades, information technologies have encompassed all human knowledge and skills, ultimately including the pattern recognition capabilities, problem-solving skills, and emotional and moral intelligence of the human brain itself [11].

With the advancement of artificial intelligence, the human role in society will transform. Many existing jobs will be automated, and new ones will emerge. Humans must adapt to these changes and acquire new skills.

As advancements in AI allow it to live and work alongside humans as independent agents, human-AI collaboration (HAIC), where people work with autonomous AI agents, has become increasingly common [12].

In the future, rather than competing with AI, we should seek to collaborate with it. AI can be used as a powerful tool to augment human capabilities. The ethical development of AI is of paramount importance. We must ensure that AI is developed for the benefit of all humanity and is not misused.

A crucial aspect in this context is addressing the challenges that arise. Self-regulation plays a significant role in tackling these ethical dilemmas. Self-regulation involves the ability to monitor and adjust one's behavior and decisions. In AI development, self-regulation empowers developers to oversee how the technology is used and ensure its ethical application [13].

9 Discussion and Conclusion

This research aims to provide a comprehensive overview of the future of artificial intelligence by deeply examining the relationship between cognitive science and artificial intelligence. By analyzing recent advancements in AI and exploring the challenges ahead, it concludes that AI has the potential to fundamentally transform many aspects of human life. On the one hand, AI can play a significant role in solving complex global problems such as diseases, climate change, and poverty. On the other hand, the uncontrolled and unregulated development of AI can pose serious threats to humanity. As a result, the researcher emphasizes the importance of appropriate regulations, ethical development of AI, and international cooperation in this field. Furthermore, this study highlights the role of cognitive science in AI development, suggesting that a better understanding of the human brain can lead to the creation of more powerful and intelligent AI systems. Ultimately, the researcher concludes that the future of AI depends on our current decisions and actions, and we must prepare for a future where AI plays a central role.

based on current trends and the data collected in this research, we will first review some of the most significant findings. Subsequently, we will present a proposed model of the ”conceptual framework of the future of artificial intelligence and cognitive science” that has been specifically developed and formulated by the researcher;

9.1 A Giant Leap on the Horizon

Research in the field of artificial intelligence, particularly at the intersection with cognitive sciences, points to a massive and fundamental transformation in the human future. With the rapid advancement of technology, AI has moved beyond theoretical boundaries and has become a reality of our daily lives.

9.2 From Brain Understanding to Artificial Intelligence Creation

One of the significant outcomes of research in this field is a deeper understanding of the human brain's functioning. By meticulously studying cognitive processes, researchers have been able to create more complex computational models of the brain. These models not only assist us in better comprehending and treating brain diseases but also serve as templates for developing artificial intelligence.

9.3 Superintelligence

One of the most significant questions raised in this field is the possibility of achieving superintelligence.

Superintelligence refers to an artificial intelligence system that surpasses human intelligence in all domains. Although this idea is still theoretical, many researchers believe that achieving superintelligence is inevitable

9.4 Social and Ethical Implications of Artificial Intelligence Development

Especially superintelligence, will have vast social and ethical implications. Some of these implications include changes in the job market, increased inequality, security and privacy issues, and even the existential threat to humanity.

9.5 Key Points to Remember

- Artificial intelligence is rapidly advancing and has the potential to transform the world.
- Humans must prepare for a future where AI plays a significant role.
- AI can be both an opportunity and a threat.
- To harness the benefits of AI, we need careful planning and management.
- The development of AI must be done with consideration for ethical and social issues.

9.6 This research helps us to

- Gain a better understanding of the future of artificial intelligence.
- Recognize the importance of research in the field of artificial intelligence.
- Pay attention to the ethical challenges associated with artificial intelligence.

9.7 Future Research Directions

- **Explainable AI:** Developing algorithms that can justify their decisions.
- **Ethical AI:** Designing AI systems aligned with human values.
- **Interactive AI:** Creating systems that can interact naturally with humans.
- **Physical AI:** Developing robots with complex physical and cognitive abilities.
- **Collective AI:** Creating networks of intelligent agents that can collectively solve complex problems.

The future of artificial intelligence is one filled with both hope and challenges. On the one hand, AI can help solve many of the world's problems, such as diseases, poverty, and climate change. On the other hand, if not managed properly, it can pose serious threats to humanity. To reap the benefits of AI and mitigate its risks, we need international cooperation, appropriate regulations, and the ethical development of AI. Ultimately, the future of AI is one where humans and machines will coexist, and the future we create depends on the decisions and actions we take today.

References

[1] N. Sfetcu, "Intelligence, from Natural Origins to Artificial Frontiers - Human Intelligence vs. Artificial Intelligence", MultiMedia Publishing, 2024, http://dx.doi.org/10.58679/mm97993.

[2] G. Savaliya, "Future of artificial intelligence", Futuristic Trends in Information Technology Volume 3 Book 2, IIP Series, 2024, p. 32-37, http://dx.doi.org/10.58532/V3BFIT2P2CH3.

[3] N. Singh, L. Sharma, U. Dhake, "Artificial Intelligence: The Future", Indian Scientific Journal Of Research In Engineering And Management, 2023, http://dx.doi.org/10.55041/IJSREM27796.

[4] A.Verma, B.Nasir, "Artificial intelligence and its future", 2023, https://doi.org/10.58532/v2bs16ch8.

[5] P. Baldwin, "Artificial Intelligence: The Future Is Here", The Senior care pharmacist, 2023, https://doi.org/10.4140/tcp.n.2023.427.

[6] P. Agrawal, C. Tan, H. Rathore, "Advancing Perception in Artificial Intelligence through Principles of Cognitive Science", arXiv.org, 2023, https://doi.org/10.48550/arXiv.2310.08803.

Table 1: A Conceptual Model of the Future of AI and Cognitive Science

Component	Description	Relationship to AI	Relationship to Cognitive Science
AI Subfields	Machine learning, deep learning, natural language processing, computer vision, robotics	These subfields will continue to advance and interact with cognitive science to develop more sophisticated AI systems.	Cognitive science provides insights into human cognition, which can be used to inform the development of AI algorithms.
Cognitive Science Subfields	Cognitive psychology, neuroscience, linguistics, anthropology	These subfields study human cognition, perception, language, and behavior, providing valuable insights for AI development.	The study of human cognition provides a foundation for understanding and modeling intelligent behavior in AI systems.
Interdisciplinary Research	Neuroinformatics, cognitive robotics, computational neuroscience	These fields combine AI and cognitive science to develop hybrid systems that integrate AI algorithms with biological principles.	Interdisciplinary research is crucial for bridging the gap between AI and cognitive science and developing more human-like AI.
Ethical Considerations	Bias, fairness, transparency, privacy	As AI systems become more integrated into society, it is essential to address ethical concerns and ensure that they are developed and used responsibly.	Cognitive science can help to understand the potential biases and limitations of AI systems and inform the development of ethical guidelines.
Applications	Healthcare, education, finance, transportation, entertainment	AI has the potential to revolutionize various industries by automating tasks, improving efficiency, and creating new opportunities.	Cognitive science can help to ensure that AI applications are aligned with human needs and values.
Societal Impact	Job displacement, economic inequality, privacy concerns	The development and deployment of AI raise important questions about the future of work, the distribution of wealth, and individual privacy.	Cognitive science can help to understand the potential social and economic implications of AI and inform the development of policies and regulations.

Note: This model is a conceptual framework that can be adapted and expanded upon based on specific research and developments.

[7] L. Favela, "Cognitive science as complexity science", WIREs cognitive science, Advanced Review, 2020, http://dx.doi.org/10.1002/WCS.1525.

[8] C. Khanzode, R. Sarode, "Advantages and Disadvantages of Artificial Intelligence and Machine Learning: A Literature Review", International Journal of Library & Information Science,9(1),2020, pp.3036, https://www.academia.edu/download/65414221/IJLIS_09_01_004.pdf.

[9] E. Egrioglu, E. Bas, "A new deep neural network for forecasting: Deep dendritic artificial neural network", Artificial Intelligence Review 57(7),2024, http://dx.doi.org/10.1007/s10462-024-10790-7.

[10] P. S. Aithal, "Super-Intelligent Machines - Analysis of Developmental Challenges and Predicted Negative Consequences", Social Science Research Network,2024, http://dx.doi.org/10.2139/ssrn.4683700.

[11] R. Kurzweil, "Superintelligence and Singularity", Chapter 25 of Machine Learning and the City: Applications in Architecture and Urban Design, 2022, DOI:10.1002/9781119815075.

[12] J. Huang, J. li, J. liu, and T. Zheng, "Human-AI cooperation: Modes and their effects on attitudes", School of Economics and Management, BeiHang University, China, 2022, http://dx.doi.org/10.1016/j.tele.2022.101862.

[13] R. Husna, S. Ramadhani,and Q. A'yun, "The Role of Self-Control in Overcoming Ethical Challenges in the Development of Artificial Intelligence", BICC Proceedings, 2024, 2:165169, http://dx.doi.org/10.30983/bicc.v1i1.123.

An Ensemble Deep Model for Deceptive Opinion Detection Based on Opinion Text: For English and Persian Languages

Mahmoud Ali-Arab[1], Kazim Fouladi-Ghaleh[2]

[1] *M.Sc. of Information Technology Engineering, Deep Learning Research Lab, Faculty of Engineering, College of Farabi, University of Tehran, Iran*
aliarab.m@gmail.com
[2] *Assistant Professor, Department of Computer Engineering, Faculty of Engineering, College of Farabi, University of Tehran, Iran; Head of Cyberspace Research Lab, University of Tehran, Iran*
kfouladi@ut.ac.ir

Abstract

Spam reviews, written primarily to promote or demote a product or brand, mislead people for making purchases and make decisions difficult for customers. Much research has been done to detect spam reviews, and different methods have been developed, but these methods often use metadata to detect spam review, and because of the use of metadata, singleton reviews (reviews whose author has submitted only one comment) are dropped from the dataset because these types of reviews do not give much information to the model. In addition, in existing methods, comment text is considered any other text in text classification issues, while comment text contains many features that can be extracted and used to detect spam reviews. In this research, a hybrid model using 4 BiLSTM networks is presented, trained on the comment's text and the comments' polarity. Due to the lack of polarity of opinions in different datasets, a sentiment analysis model has been used that extracts the polarity of opinions from the comments text and adds it to the dataset. Since the model depends only on the comment's text and does not use metadata, there will be no problem in detecting singleton spam reviews using this model. The proposed model is evaluated for English and Persian languages. The performance of the proposed model is comparable for both Persian and English. For English, the accuracy was 89.4% on the OpSpam dataset and 87.7% on the Hotel domain (Doctor, Restaurant (HDR)) dataset. Also, 87.7% accuracy was obtained for the Persian language on the Digikala dataset.

Keywords: *Review Spam Detection, Opinion Spam, Deep Learning, Ensemble Model, Long Short-Term Memory (LSTM), Persian, English.*

1 Introduction

Customer reviews are critical because they significantly impact other customers, and the information it provides makes a user decide to buy a product. Nearly 95% of people read the reviews written about products before buying online and then decide to purchase [10]. The impact of these comments is not only on customers, but businesses use these reviews to improve the quality of their services or marketing decisions, etc. Due to the importance of these reviews and their impact on product sales, spam reviews have also spread. Spam review is an opinion that is not the result of a person's experience and is written to promote or demote a brand. Spam reviews can lead other customers to make wrong decisions. On many websites, people can post any review, and it is difficult for humans to tell if a comment is spam, which is why spam review is becoming more and more challenging to detect. Therefore, there is a need for a model that can recognize these spam reviews.

In recent years, much research has been done to identify spam reviews, and various businesses are looking for a way to deal with spam reviews. The number of researches in this field is increasing exponentially [1], and due to the increase of unrealistic information on the Internet, the research about spam detection is increasing every day.

There is a problem called singleton spam reviews in existing methods of detecting spam reviews. These comments are written by people who have written only one comment. If metadata such as username, IP, etc. are used to train the model for detecting spam reviews, singleton reviews do not give any information to the model, and therefore in many of existing methods, these reviews are dropped from the dataset, and these methods cannot detect singleton spam reviews. In addition, in existing research, the features of the comments text are usually not considered, while comment text includes different features that can extract and use to train the model.

In this research, a hybrid model is proposed that depends only on the text of the review and its label. The polarity of comments is also extracted from the comment text using a sentiment analysis model and added to the dataset. The model is implemented so that it can be trained for different languages with minor changes.

The proposed model is also trained for Persian. Existing methods for detecting spam reviews for the Persian language using traditional machine learning models have addressed this issue, so the results obtained in this study are significantly better than existing research for Persian.

2 Background and related works

The topic of review spam detection has been one of the most active topics for research in recent years. Much research has been done on this subject, and the number of these researches is increasing exponentially. In these researches, different learning methods and characteristics have been examined. Research to detect spam review can be divided into different categories by aspects such as the type of learning, type of features used,

identification techniques, etc. In terms of the type of learning, research is divided into supervised learning, Unsupervised Learning, and semi-supervised learning [4].

2.1 Types of learning

2.1.1 Supervised learning

Supervised learning is one of the most efficient methods of machine learning. This method uses labeled data. The problem with this type of learning is that there are not enough labeled data. For this reason, researchers are trying to use other methods as well. Numerous studies have used supervised learning methods to detect spam reviews. This type of learning performs better than other machine learning methods if there is a sufficiently labeled dataset. In this research, a supervised learning method and labeled dataset have been used. As mentioned, most existing methods try to use all available metadata. For example, Huang et al. [2] have used supervised learning. They collected data using crawlers from Epinions. They also gave their model information, such as how helpful the comment was and what rating it was given. Using extensive metadata does not necessarily improve model performance. Mukherjee et al. [3] showed that the low usefulness of a comment is not a reason for the comment to be spam because one of the methods used by spammers is to use group spamming in which several people write a comment and, in this situation, Spammers are more likely to rate each other's opinions higher and choose those opinions as applicable.

2.1.2 Unsupervised learning

One of the significant problems with machine learning models is the lack of labeled data. If there is enough labeled data, the best way is to use supervised learning, but real-world data is often unlabeled, so unsupervised learning does not require labeled data. Data labeling is a difficult task that is both time-consuming and costly. Lots of data related to user comments are also unlabeled. For this reason, researchers try to use the method of unsupervised learning. Although unsupervised methods have poorer performance than supervised methods, new research seeks to optimize these methods to perform better. In 2020, Saumya et al. [5] developed an unsupervised model using LSTM and Autoencoder networks that can be trained using comment text without labels. They used the Matthew correlation coefficient (MCC) metric to evaluate their model.

2.1.3 Semi-supervised learning

In recent years a method has been used called semi-supervised learning. This method uses labeled and unlabeled data. A small set of labeled data and a set of unlabeled data are given to the model. In this method, the unlabeled data is labeled using labeled data, and then the labeled data is used as training data [4]. In this way, more labeled data is given to the model for training. Research using this method has increased in

recent years. Different methods are used for semi-supervised learning, and in [6], the performance of each of these types of methods is compared.

2.2 Related works

In this research, the issue of detecting spam reviews for both Persian and English languages has been investigated, and the efficiency of the proposed model has been evaluated for both languages. So, in the related works section, related works for English and Persian languages are discussed in two separate sections.

2.2.1 Related works for English

The issue of spam detection was first formulated by Jindal et al. [7, 8, 9]. They divided spam into three categories: unrealistic, branded, and unrelated. They claimed that the second and third categories of comments do not pose a problem and are easily identifiable, but the first category are not easily recognizable, and a model must be created to identify them [10]. In research [9], measuring the similarity of opinions has been used to identify spam. The first public dataset to detect spam reviews was published by Ott et al. [11] in 2011. This dataset contains 800 truthful comments and 800 deceptive comments about 20 Chicago hotels. Deceptive reviews in this dataset are written by Amazon Mechanical Turk (AMT). A few years later, Li et al. [13], based on Ott et al. [11] dataset, introduced a dataset prepared in three domains: hotel, doctor, and restaurant. This dataset is one of the most widely used datasets in spam detection, and the amount of data in the Li et al. [13] dataset is more than the dataset of Ott et al. [11].

In the study of Wael et al. [12], the effect of different preprocessing stages on the data on the efficiency of the spam detection model was investigated. Several preprocessing methods on the text such as stop word removal, removing emphasis marks, stemming, etc. were examined in this study and the effect of each of these methods by teaching several different models of machine learning such as Naive Bayes Network, Support vector machine, random forest, etc. were measured. With the growth of deep neural networks, usage of these networks in spam review detection research has also increased. In general, deep neural networks have several advantages over traditional machine learning methods. First, neural network-based models have many nonlinear methods that can be modified and enhanced based on neural network depth. Second, neural networks can derive features from raw data. That is, the feature extraction step is done in the neural network itself, and the third thing that is most used in the field of working with text is that using deep learning if a good word embedding is used in model training, the model can easily understand the relationship between words and their proximity to each other and even sentence structure [14]. Lie et al. [15] Have used CNN networks to detect spam reviews. In their research, word vectors are given as input features to the network, and spam reviews are directly identified using CNN.

The use of hybrid methods and the integration of several deep learning models have also been considered to detect spam reviews. Zhang and Ren [16] used document-level learning to detect spam. First, a document is given to the model, and using CNN combined with a network (Gated-RNN), the sentences and their structure are learned, and the document vectors are extracted by this method, then these vectors are used directly to detect spam reviews. Zhao et al. [17] have used a new method called using word order-preserving in the convolutional layers and merging CNN network, instead of using the usual concatenation layer in the convolutional network. This maintains the order of the words in the integration layer and improves the CNN network for spam detection.

The length of review texts is very different, so a maximum length is usually considered for the input text. This maximum length should be chosen so that the model has the most performance, but if this maximum length is small, a large part of the data will be lost, and if this maximum length is considerable, it will have a high computational cost. So, Kumar et al. [18] came up with using the full text of the reviews. They divided the text of each review into several smaller parts and assigned a label equal to the original review label for each of them. These scaled-down comments were given to a combined CNN and GRU networks model, and the final label was determined by max-voting. Barushka et al. [19] developed a deep neural networks (DNN) model. They have tried to use the content of the review to train their model, using both the bag of words (BOW) and the meaning of the words to teach the model. They also used N-gram and Skip-gram word embedding methods to obtain word vectors and train their model.

2.2.2 Related works for Persian

The proposed model is also trained and evaluated with Persian data in this research. Therefore, existing methods to identify spam opinion in Persian have been reviewed in this section.

Little research has been done to identify spam reviews in Persian. Existing research has also used traditional machine learning methods for this subject, so their results are not very good. Safarian et al. [20] have used feature ranking for review spam detection. They have tried to examine the various features used to train the model in the problem of spam review detection. They have used different models such as Naive Bayes, decision tree, support vector machine, etc. Each of these models is trained with different features such as overall product rating, the sentiment of comments, POS tags, etc. In their research, training data from users' opinions of the Digikala website (the most extensive retail site in Iran) has been used. Basiri et al. [32] Also tried to use various machine learning methods such as Naive Bayes, decision tree, support vector machine, and various features extracted from the comment text and other metadata available in the dataset. Their research has been done on balanced and unbalanced data, and according to the obtained results, the support vector machine for unbalanced

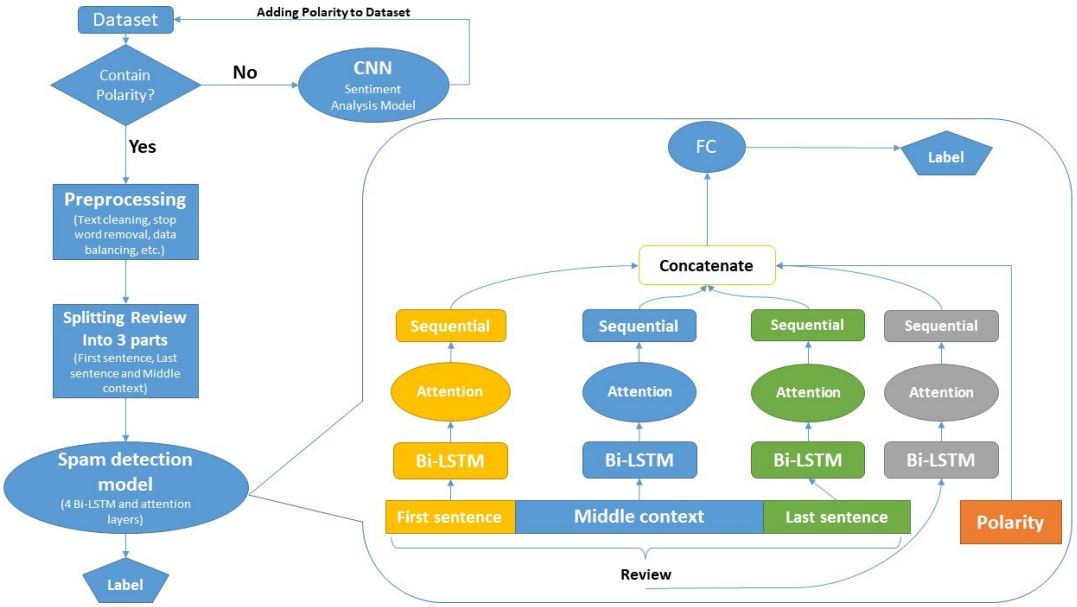

Figure 1: Proposed model architecture

data and the decision tree for balanced data have the best performance.

3 Methodology

This research aims to provide a hybrid model for detecting spam reviews. In the proposed model, only the text of the reviews and their labels is used to train the model. Due to the effect of opinion polarity on the problem of spam review detection [21], and given that the polarity of opinions may not be present in different datasets, in this study, the polarity of opinions is extracted by a sentiment analysis model and added to the dataset. In the text of a comment, the first sentence and the last sentence are more critical, and for this reason, in this research, training is done on the first and last sentence separately. As shown in Figure 1, in this research, the text of the comment is divided into three parts: first sentence, last sentence, and middle context, and each of these three parts is given to a bidirectional long short-term memory (BiLSTM), and the entire comment text is given to a BiLSTM. There is a total of 4 BiLSTMs in the proposed model. The output of each BiLSTM layer, after passing through a self-attention layer, eventually joins together to form a vector. The polarity of the review, which is calculated as binary (positive or negative), is also joined to this vector at this stage, and the resulting vector is given to a fully connected layer (classification layer) to produce the final output label.

Table 1: Statistics of HDR dataset

	Turker	*Expert*	*Customer*
Hotel (P/N)	400/400	140/140	400/400
Restaurant (P/N)	200/0	120/0	200/200
Doctor (P/N)	200/0	32/0	200/0

3.1 Dataset

In this research, two datasets OpSpam [22] and (Hotel, Doctor, Restaurant (HDR)) [13], have been used. The reason that several datasets are used in this research is to the proposed model be comparable with different models and different researches, and also the performance of the model is measured in different domains.

OpSpam [22] is a balanced database that contains 1,600 reviews of Chicago hotels. This dataset contains 800 spam comments and 800 real comments. There are 400 negative comments and 400 positive comments in each of these categories. In this dataset, real comments are collected from the Yelp website, and deceptive comments are generated by Amazon Mechanical Turk (AMT).

Data sets (Hotel, Doctor, Restaurant (HDR)) [13] have also been used in this research, which is one of the most widely used datasets in research in the field of spam review detection. This dataset is collected in three domains of comments related to hotels, restaurants, and doctors. real comments in this dataset are collected from customers of each domain and deceptive comments are written by AMT or employees of each domain (expert). The statistics of this dataset are given in Table 1.

3.2 Data preparation

As shown in Figure 2, the dataset is first examined to see if it includes the polarity of the comments. If the dataset does not have the polarity of comments, the sentiment analysis model automatically extracts the polarity of the comments in binary (positive or negative) from the comments text and adds it to the dataset. The dataset is then divided into two parts: training data and evaluation data. In this study, 20% of the data is considered evaluation data, and the rest is considered training data.

After this step, the data balance is checked, and if the dataset is unbalanced, the data are balanced using the OverSampling method. This method is one of the standard methods of data balancing.

After balancing the data, the comment text is divided into the first sentence, middle context, and final sentence. Each of these sections is tokenized. The entire text of the comment is also tokenized at this stage. In this research, the SpaCy library has been used for preprocessing in English, and also Hazm and Parsivar libraries have been used for Persian. After data tokenization, the stop words are removed, and word vectorization is performed. Finally, these vectors are given as input data to the spam review detection model.

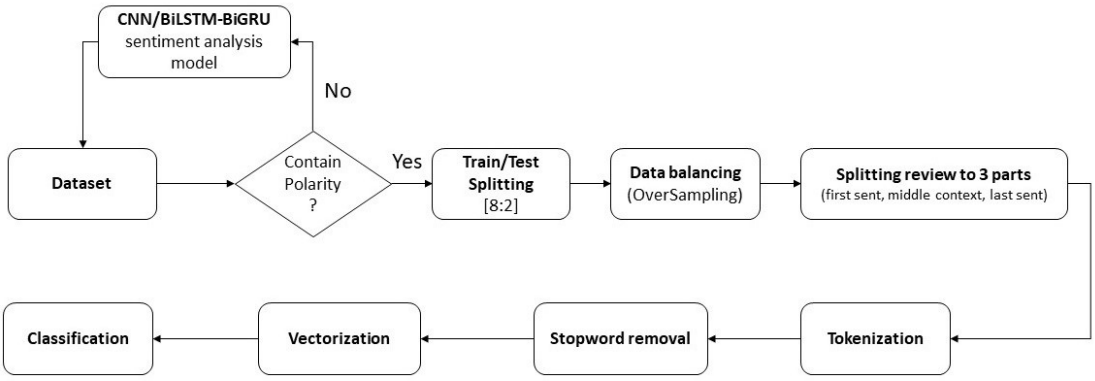

Figure 2: Data preparation flowchart

3.3 Comment polarity extraction

Due to the effect of opinion polarity in detecting spam reviews [21] in this study, the polarity of comments has been used to detect spam opinions. Because the polarity of opinions may not be present in many datasets, first, the dataset is examined. If the polarity of opinions is not available, using a sentiment analysis model, the polarity of opinions is extracted from the text of the opinion and added to the dataset. Finally, the model is trained to detect spam using this new dataset.

For English, an open-source sentiment analysis model has been used, implemented using CNN, and has an accuracy of about 85%. For Persian, an ensemble sentiment analysis model has been used, implemented using BiLSTM and BiGRU networks, and has an accuracy of about 92%. In this research, sentiment is considered binary, and one opinion can be positive or negative.

3.4 Bidirectional Long Short-Term Memory (BiLSTM) layer

Long Short-term memory networks (LSTMs) are commonly used for sequence models, and since a text is also a sequence of words and letters, LSTM networks perform well for text classification issues. These networks are a particular type of recurrent neural network (RNN) that has solved the problem of gradient vanishing by introducing memory cells and gate mechanisms. In this type of network, the information generated at the output is stored in a memory cell. This storage operation is controlled by three gates (g_i, g_f, g_o) and determines the amount of forgetting or storage of information defined in Equations 1 to 3. In these equations, x_j is the input at position j of the sequence given to the model. h_{j-1} is also the state of the previous cell.

$$g_i = \sigma(x_j W^{x_i} + h_{j-1} W^{h_i}) \tag{1}$$

$$g_f = \sigma(x_j W^{x_f} + h_{j-1} W^{h_f}) \tag{2}$$

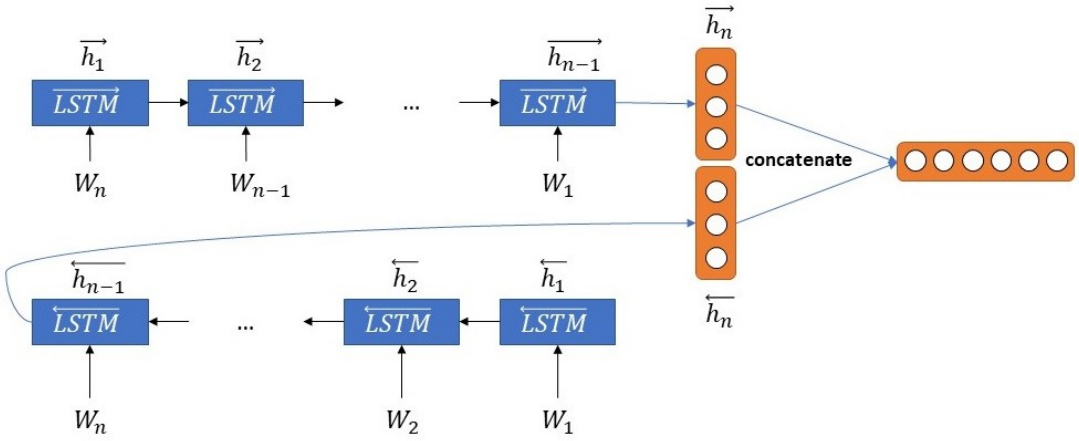

Figure 3: Bidirectional Long Short-term memory (BiLSTM) architecture

$$g_o = \sigma(x_j W^{x_o} + h_{j-1} W^{h_o}) \tag{3}$$

The new model is also a linear equation of x_j and h_{j-1} given to a tanh activation function (Equation 4).

$$z = \tanh(x_j W^{x_z} + h_{j-1} W^{h_z}) \tag{4}$$

The value of z in a linear combination with the previous amount of memory creates a new amount of memory. Equation 5 shows this linear combination in which c_j is the new value, and c_{j-1} is the previous value of the memory cell. g_f controls the amount of forgetting the previous amount of memory, and g_i specifies the new amount to be stored in the memory cell.

$$c_j = g_f c_{j-1} + g_i z \tag{5}$$

The final output, as mentioned, is controlled using the g_o gate, and the c_j value is generated using the tanh activation function, which is shown in Equation 6. In this equation, h_j represents the LSTM output at position j.

$$h_j = g_o(\tanh(c_j)) \tag{6}$$

The BiLSTM model has been used in this research. BiLSTM traverses the sequence in two directions. Two LSTMs are used in this model, one of which follows the sequence from beginning to end and the other from end to end. Moreover, the training process is done this way. The information of these two LSTMs is concatenated in each step. The architecture of the BiLSTM model is shown in Figure 3.

BiLSTM output in each position is the concatenation of the output of forwarding LSTM ($\overrightarrow{LSTM}$) and the output of backward LSTM ($\overleftarrow{LSTM}$) (Equations 7 to 9).

$$\overrightarrow{h_t} = \overrightarrow{LSTM}(e_t, \overrightarrow{h_{t-1}}) \tag{7}$$

$$\overleftarrow{h_t} = \overleftarrow{LSTM}(e_t, \overleftarrow{h_{t-1}}) \tag{8}$$

$$H_t = (\overrightarrow{h_t} : \overleftarrow{h_t}) \tag{9}$$

In this research, the text of each comment is divided into three parts: the first sentence, the middle context, and the final sentence. Each of these parts is given to a BiLSTM. The entire comment text is also given to a BiLSTM. That is, in total, the proposed model includes 4 BiLSTM models.

3.5 Self-attention mechanism

Self-attention is a particular attention mechanism that can efficiently detect dependence in different parts of a sequence such as convolutional neural networks or recurrent neural networks, with the difference that in comparison with recurrent neural networks or convolutional neural networks have fewer parameters and less complexity. The output of the self-attention layer is a weighted average of different positions of the sequence.

In this research, multilayer perceptron has been used as the primary attention function, and softmax function has been used for normalization. The output vectors of the first sentence, the middle context, and the last sentence generated by BiLSTM are represented by s_1, s_2, and s_3. The input of the attention layer itself is a combination of three vectors, s_1, s_2, and s_3, which are displayed as $S = [s_1 : s_2 : s_3]$. Equations 10 to 12 show these steps.

$$Adp = \tanh(W \cdot S^T + b) \tag{10}$$

$$Attention = \text{softmax}(Adp(S)) \tag{11}$$

$$Attention_i = \frac{\exp(Adp(S_i))}{\sum_{i=1}^{3} \exp(Adp(S_i))} \tag{12}$$

The output of the self-attention mechanism is the weighted average S, while the weight matrix is Attention. In practice, the output of the self-attention mechanism is still a sequence, and each element can be seen as a representation of the document. The final output of the self-attention mechanism is displayed with Z.

The output of the BiLSTM corresponding to the entire comment text is displayed with s_c. s_c and Z are both representations of the comment text that concatenate together. At this point, the polarity of the review represented by p is also added to this sequence. Equation 13 specifies the final output generation steps.

$$O = [Z : s_c : p] \tag{13}$$

This output (O) is given to a fully connected (FC) layer to generate the output label. The final label is generated in binary and specifies whether the comment is spam or genuine.

Table 2: Optimal hyper-parameter values for each dataset

Dataset	Embedding size	Learning rate	Hidden size	Epochs
OpSpam	100	0.0007	64	35
HDR → Hotel	100	0.0005	64	40
HDR → Doctor	100	0.0005	64	40
HDR → Restaurant	100	0.001	32	40
Digikala (Persian lang)	50	0.005	40	15

4 Results

As mentioned earlier, the proposed model for English is evaluated on the OpSpam and HDR datasets, and for Persian on the Digikala dataset. Because the proposed model for Persian and English has been evaluated, the comparison of results for each language is given in separate sections. Compared to the base model [10] and other models, the results showed that the proposed model's performance for the OpSpam dataset and the Hotel domain of the HDR dataset is better than other models. Also, for Persian, the obtained results showed that the performance of the proposed model is much better than the existing methods.

4.1 Evaluation metrics and Hyperparameters

In this research, several evaluation metrics have been used to make the results more reliable and to be able to compare these results with other research. Accuracy, $F1$, *Recall*, and *Precision* metrics are used (equation 14 to 17). The use of multiple evaluation metrics is crucial in research that uses unbalanced data sets because the use of one metric cannot show reliable results.

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \tag{14}$$

$$Recall = \frac{TP}{TP + FN} \tag{15}$$

$$Recall = \frac{TP}{TP + FN} \tag{16}$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{17}$$

The proposed model hyperparameters are adjusted to obtain the best result for each dataset. Table 2 shows metadata per dataset. This table lists essential parameters such as learning rate, embedding layer size, hidden layer size, and the number of configured epochs per dataset.

Table 3: The proposed model result for English datasets

Dataset	F1	Accuracy	Precision	Recall
OpSpam	88.6	89.4	86.6	90.6
HDR → Hotel	87.7	87.7	87.9	87.5
HDR → Doctor	88.54	89.51	96.66	81.69
HDR → Restaurant	86.42	86.25	85.36	87.5

Table 4: Results comparison for English

Dataset	Model	Year	F1	Accuracy	Precision	Recall
HDR (Hotel)	EnsDOS [25]	2019	85.7	85.7	85.5	86.1
	SOMCNN [29]	2021	85	86	85	86
	CNN_BiLSTM [30]	2021	86.1	83	86.8	85.3
	Proposed Model	-	**87.7**	**87.7**	**87.9**	**87.5**
HDR (Doctor)	EnsDOS [25]	2019	85	84.7	83.6	86.5
	SOMCNN [29]	2021	**93.0**	**94.0**	93	**93.0**
	CNN_BiLSTM [30]	2021	92.8	91	**97.0**	88.9
	Proposed Model	-	88.54	89.51	96.66	81.69
HDR (Restaurant)	EnsDOS [25]	2019	85.8	85.5	84.1	**88.5**
	SOMCNN [29]	2021	**88.0**	**88.0**	89	87
	CNN_BiLSTM [30]	2021	80.9	77.5	**90.5**	73.1
	Proposed Model	-	86.42	86.25	85.36	87.5
OpSpam	SingleCNN [23]	2017	81.1	81.2	78.2	84.3
	IMP [24]	2018	-	83.5	-	-
	MFCNN [26]	2020	86.5	83.5	84.6	88.4
	DOSDL [27]	2020	87.1	87.2	**87.3**	87.5
	DOSLSTM [28]	2020	-	83.3	78	81
	Proposed Model	-	**88.6**	**89.4**	86.6	**90.6**

4.2 Result comparison for English

Table 3 shows the results obtained for the proposed model for different English datasets. The training and evaluation of this model for English have been done on two widely used datasets, OpSpam and HDR. The HDR dataset includes three domains: Hotel, Doctor, and Restaurant. Due to the differences in the domains of this dataset, training/evaluation of each domain has been done separately. Table 3 shows the results for each dataset in separate rows.

In the following, a comparison is made between the results of the proposed model for English and the existing methods (Table 4). However, before explaining the comparison table, it should be noted that the results of research in spam review detection are highly dependent on the dataset. For this reason, in Table 4, the results of other research are presented based on their datasets, and the best results obtained for each research are shown in this table.

As shown in Table 4, the performance of the proposed model for the OpSpam and

Table 5: The proposed model results for Persian (Digikala dataset)

Dataset	F1	Accuracy	Precision	Recall
Digikala	88.6	89.4	86.6	90.6

Table 6: Results comparison for Persian

Model	Year	Digikala			
		F1	Accuracy	Precision	Recall
FRRSD [32]	2019	82.4	83.3	-	82.4
SURSD [33]	2019	78.0	-	-	-
Proposed	-	**87.4**	**87.7**	**88.6**	**86.2**

Hotel domain of HDR datasets is better than the other methods, but for the Restaurant and Doctor domains of (HDR) dataset, the proposed model performs worse than the other methods. One reason for this difference is the size of datasets. The OpSpam and Hotel (HDR) datasets are larger than the Restaurant (HDR) and Doctor (HDR) datasets. Therefore, it can be said that according to the obtained results, the performance of the proposed model is better on larger datasets and does not perform well on a small dataset. According to the results in Table 4 for the Restaurant (HDR) and Doctor (HDR) datasets, none of the models is better than the other in all metrics.

4.3 Result comparison for Persian

As mentioned in this study, the proposed model on a Persian dataset was also trained and evaluated. Since not much research has been done for Persian on this subject, there are not many datasets to detect spam reviews. The only dataset used by researchers in this field is the Digikala dataset (Digikala.com, the largest retail website in Iran). This research has used this dataset to train and evaluate the model. Table 5 shows the results obtained by the proposed model for the Digikala dataset.

The following compares the results of the proposed model and existing methods in the field of spam review detection for Persian (Table 6). Not much research has been done to detect spam reviews for Persian, and existing methods have used traditional machine learning methods. In all methods presented in this table, the Digikala dataset has been used.

There is a big difference between the performance of the proposed model and other methods of detecting spam for Persian, and the proposed model has a better performance than other methods. The main reason for this difference in performance is that other methods (FRRSD, SURSD) use traditional machine learning methods to detect spam reviews. Although metadata is also used in these methods, their performance is significantly lower than the proposed method. This indicates that the use of metadata does not increase efficiency and, in some cases, may reduce model performance due to challenges such as singleton spam reviews or group spamming.

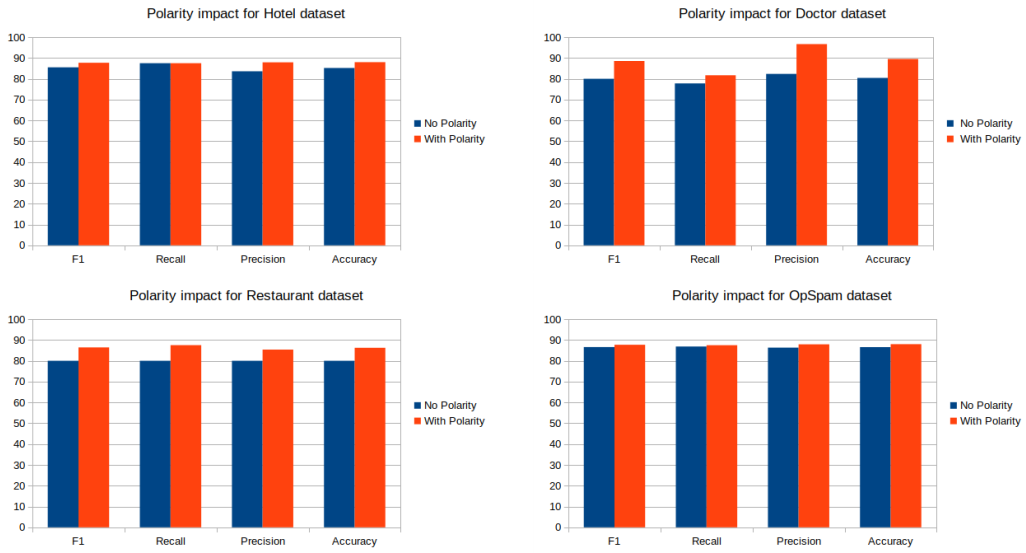

Figure 4: Impact of using opinion polarity in proposed model for different dataset

4.4 Impact of each Technique

This section examines the impact of "data balancing" and "review polarity" used in the proposed model.

4.4.1 Using review polarity

To determine the effect of using the polarity of review in the proposed model to detect spam reviews, the model is trained once without using polarity and once using polarity, and the results can be seen in Figure 4. As shown in this figure, the impact of using the polarity of reviews is considerable.

4.4.2 Data balancing

Data balancing can increase the model's efficiency because if the data set is balanced, the model will be trained equally on each class. In this section, the impact of using data balancing is examined. The OpSpam dataset is balanced, so there is no need to use balancing, but the Doctor (HDR) and Restaurant (HDR) datasets are not balanced and need to be balanced. As explained, this study used OverSampling to balance the data. This section shows the impact of using data balancing (Figure 5). As shown in Figure 5, the use of data balancing in unbalanced domains of the HDR dataset (Doctor and Restaurant domains) has significantly impacted model performance.

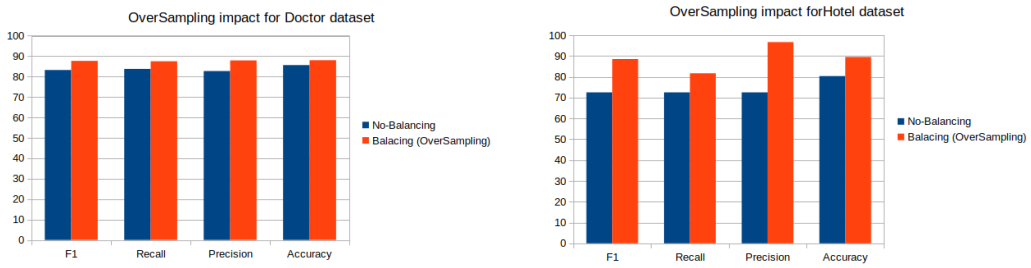

Figure 5: Impact of oversampling for imbalances datasets

5 Conclusion and future works

This research aims to provide a model using deep learning to detect spam opinions, in which only the text of the comments and their labels are used for training. Since in the comment text, the first and last sentences are more important than the middle context, in the proposed model, the comment text is divided into three parts, the first sentence, the middle context, and the last sentence, and each of these sections is given to a BiLSTM model. The entire comment text is also given to a BiLSTM. Using a sentiment analysis model, the polarity of opinions is also extracted in the absence and given to the spam review detection model. Finally, the output of the four BiLSTMs and the polarity of the review are concatenated together to form a vector. This vector is then given to a fully connected (FC) network, generating the final label. Various techniques such as balancing, using the self-attention mechanism, etc., have been used to increase the efficiency of the proposed model.

The proposed model for Persian and English languages has been trained and evaluated in this research. For English, two datasets, OpSpam and HDR, were used. Comparing the proposed model with similar methods shows that the proposed model performs better than similar works for the OpSpam dataset and Hotel domain of the HDR dataset. Although performance enhancement is minor in the proposed model, it is worth noting that only the text of the comments was used for learning in this study, and no metadata was used. For Persian, considering that the research done so far has all used traditional machine learning methods, the performance of the proposed model was much better compared to them. Although model performance is currently acceptable, some points can improve model performance and be referred to as future work. One of these tasks is to use algorithms to find the optimal value of hyper-parameters or use meta-learning. It is also possible to augment the data by translating the comment into different languages and then returning it to the original language and using it to balance the data.

References

[1] Alessandro Bondielli, Francesco Marcelloni, A survey on fake news and rumour detection techniques, Information Sciences, Volume 497, 2019, Pages 38-55, ISSN 0020-0255,

https://doi.org/10.1016/j.ins.2019.05.035.

[2] Li, Fangtao & Huang, Minlie & Yang, Yi & Zhu, Xiaoyan. (2011). Learning to Identify Review Spam. IJCAI Proceedings-International Joint Conference on Artificial Intelligence. 2488-2493. 10.5591/978-1-57735-516-8/IJCAI11-414.

[3] Arjun Mukherjee, Abhinav Kumar, Bing Liu, Junhui Wang, Meichun Hsu, Malu Castellanos, and Riddhiman Ghosh. 2013. Spotting opinion spammers using behavioral footprints. In Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '13). Association for Computing Machinery, New York, NY, USA, 632–640. DOI:https://doi.org/10.1145/2487575.2487580

[4] Raga S. H. Istanto, Wayan Firdaus Mahmudy, and Fitra A. Bachtiar. 2020. Detection of online review spam: a literature review. In Proceedings of the 5th International Conference on Sustainable Information Engineering and Technology (SIET '20). Association for Computing Machinery, New York, NY, USA, 57–63. DOI:https://doi.org/10.1145/3427423.3427434

[5] Saumya, Sunil & Singh, Jyoti. (2022). Spam review detection using LSTM autoencoder: an unsupervised approach. Electronic Commerce Research. 22. 10.1007/s10660-020-09413-4.

[6] Alexander Ligthart, Cagatay Catal, Bedir Tekinerdogan,Analyzing the effectiveness of semi-supervised learning approaches for opinion spam classification, Applied Soft Computing, Volume 101, 2021, 107023, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2020.107023.

[7] N. Jindal and B. Liu, "Analyzing and Detecting Review Spam", Seventh IEEE International Conference on Data Mining (ICDM 2007), 2007, pp. 547-552, doi: 10.1109/ICDM.2007.68.

[8] Nitin Jindal and Bing Liu. 2007. Review spam detection. In Proceedings of the 16th international conference on World Wide Web (WWW '07). Association for Computing Machinery, New York, NY, USA, 1189–1190. DOI:https://doi.org/10.1145/1242572.1242759

[9] Nitin Jindal and Bing Liu. 2008. Opinion spam and analysis. In Proceedings of the 2008 International Conference on Web Search and Data Mining (WSDM '08). Association for Computing Machinery, New York, NY, USA, 219–230. DOI:https://doi.org/10.1145/1341531.1341560

[10] Zeng, Zhi-Yuan & Lin, Jyun-Jie & Chen, Mu-Sheng & Chen, Zorro & Lan, Yan-Qi & Liu, Jun-Lin. (2019). A Review Structure Based Ensemble Model for Deceptive Review Spam. Information. 10. 243. 10.3390/info10070243.

[11] M. Ott, Y. Choi, C. Cardie, and J.T. Hancock. 2011. Finding Deceptive Opinion Spam by Any Stretch of the Imagination. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies.

[12] Wael Etaiwi, Ghazi Naymat, The Impact of applying Different Preprocessing Steps on Review Spam Detection, Procedia Computer Science, Volume 113, 2017, Pages 273-279, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.08.368. (https://www.sciencedirect.com/science/article/pii/S1877050917317787)

[13] Jiwei Li, Myle Ott, Claire Cardie, and Eduard Hovy. 2014. Towards a General Rule for Identifying Deceptive Opinion Spam. In Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), pages 1566–1576, Baltimore, Maryland. Association for Computational Linguistics.

[14] Y. Ren and D. Ji, "Learning to Detect Deceptive Opinion Spam: A Survey", in IEEE Access, vol. 7, pp. 42934-42945, 2019, doi: 10.1109/ACCESS.2019.2908495.

[15] Li, L., Ren, W., Qin, B., & Liu, T. (2015). Learning Document Representation for Deceptive Opinion Spam Detection. CCL.

[16] Yafeng Ren and Yue Zhang. 2016. Deceptive Opinion Spam Detection Using Neural Network. In Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers, pages 140–150, Osaka, Japan. The COLING 2016 Organizing Committee.

[17] Zhao, Siyuan & Xu, Zhiwei & Liu, Limin & Guo, Mengjie. (2018). Towards Accurate Deceptive Opinion Spam Detection based on Word Order-preserving CNN. Mathematical Problems in Engineering. 2018. 10.1155/2018/2410206.

[18] Jain N., Kumar A., Singh S., Singh C., Tripathi S. (2019) Deceptive Reviews Detection Using Deep Learning Techniques. In: Métais E., Meziane F., Vadera S., Sugumaran V., Saraee M. (eds) Natural Language Processing and Information Systems. NLDB 2019. Lecture Notes in Computer Science, vol 11608. Springer, Cham. https://doi.org/10.1007/978-3-030-23281-8_7

[19] Barushka A., Hajek P. (2019) Review Spam Detection Using Word Embeddings and Deep Neural Networks. In: MacIntyre J., Maglogiannis I., Iliadis L., Pimenidis E. (eds) Artificial Intelligence Applications and Innovations. AIAI 2019. IFIP Advances in Information and Communication Technology, vol 559. Springer, Cham. https://doi.org/10.1007/978-3-030-19823-7_28

[20] Safarian Neshat, Basiri Mohammad Ehsan, KHOSRAVI HADI. Feature ranking for Persian Spam Review detection. JOURNAL OF SOFT COMPUTING AND INFORMATION TECHNOLOGY (JSCIT). 2019 [cited 2022March12];8(2):1-16. Available from: https://www.sid.ir/en/journal/ViewPaper.aspx?id=745032

[21] Hernández-Castañeda, Ángel & Calvo, Hiram & Gambino, Omar. (2018). Impact of polarity in deception detection. Journal of Intelligent & Fuzzy Systems. 35. 1-10. 10.3233/JIFS-169610.

[22] Myle Ott, Yejin Choi, Claire Cardie, and Jeffrey T. Hancock. 2011. Finding Deceptive Opinion Spam by Any Stretch of the Imagination. In Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, pages 309–319, Portland, Oregon, USA. Association for Computational Linguistics.

[23] Bhargava, Rupal, Baoni, Anushka, and Sharma, Yashvardhan. Composite sequential modeling for identifying fake reviews. Journal of Intelligent Systems, 28, 04 2018.

[24] Hernández-Castañeda, Ángel, Calvo, Hiram, and Gambino, Omar. Impact of polarity in deception detection. Journal of Intelligent & Fuzzy Systems, 35:1–10, 07 2018.

[25] Zeng, Zhi-Yuan, Lin, Jyun-Jie, Chen, Mu-Sheng, Chen, Zorro, Lan, Yan-Qi, and Liu, Jun-Lin. A review structure based ensemble model for deceptive review spam. Information, 10:243, 07 2019.

[26] Ye Wang, Bixin Liu, Hongjia Wu Shan Zhao Zhiping Cai, Donghui Li Cheang Chak Fong. An opinion spam detection method ased on multi-filters convolutional neural network. Computers, Materials & Continua, 65(1):355–367, 2020.

[27] Anass, Fahfouh, Jamal, Riffi, Mahraz, Mohamed Adnane, Ali, Yahyaouy, and Tairi, Hamid. Deceptive opinion spam based on deep learning. In 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS), pages 1–5, 2020.

[28] P Mahalakshmi, Varri Sampreeth, Challa Venkataramana. Detection of opinion spam using lstm networks. 29:67 – 75, Apr. 2020.

[29] Neisari, Ashraf, Rueda, Luis, and Saad, Sherif. Spam review detection using self-organizing maps and convolutional neural networks. Computers & Security, 106:102274, 2021.

[30] Liu, Yuxin, Wang, Li, Shi, Tengfei, and Li, Jinyan. Detection of spam reviews through a hierarchical attention architecture with n-gram cnn and bi-lstm. Information Systems, page 101865, 2021.

[31] Safarian Neshat, Basiri Mohammad Ehsan, KHOSRAVI HADI. Feature ranking for Persian Spam Review detection. JOURNAL OF SOFT COMPUTING AND INFORMATION TECHNOLOGY (JSCIT). 2019 [cited 2022March12];8(2):1-16. Available from: https://www.sid.ir/en/journal/ViewPaper.aspx?id=745032

[32] M. E. Basiri, N. Safarian and H. K. Farsani, "A Supervised Framework for Review Spam Detection in the Persian Language", 2019 5th International Conference on Web Research (ICWR), 2019, pp. 203-207, doi: 10.1109/ICWR.2019.8765275.

The Importance of Modern SEO in the Success of Online Businesses

Yashar Abri[1], Faezeh Khadem[2]

[1]*M.Sc. Student, Information Technology Engineering, Faculty of Engineering, College of Farabi, University of Tehran, Iran*
yasharabri@ut.ac.ir
[2]*M.Sc. Student, Computer Engineering, Artificial Intelligence and Robotics, Faculty of Engineering, College of Farabi, University of Tehran, Iran*
faezeh.khadem@ut.ac.ir

Abstract

This study examines the dimensions of Search Engine Optimization (SEO), the enhancement of search experience, and the role of Artificial Intelligence in transforming and improving their performance. First, the main concepts of the internet, the web, search engines, and website optimization methods are introduced. Then, the relationship between AI and search engines is explored, with a focus on the role of AI in improving SEO processes. In the research methodology section, a cascade approach has been employed to develop and implement software optimization models. The findings indicate that both internal and external SEO optimization, with an emphasis on modern techniques, contribute to improving website rankings in search results. Additionally, the impact of AI in data analysis and the continuous optimization of SEO strategies is discussed. Finally, the article highlights the importance of continually adapting SEO techniques to changes in AI-integrated search engine algorithms and the necessity of producing high-quality content.

Keywords: *Website, Search Engine, Search Engine optimization (SEO), Search Experience Optimization, Online Business, Artificial Intelligence.*

1 Introduction

The advancement and increasing complexity of information technology has led to the emergence of various types of websites as providers of information, services, and products. Currently, there are numerous websites on the internet. For example, according to the latest report in 2024 by Hostinger [1], approximately 810 million websites are built using WordPress as a content management system, which is estimated to account for only about 43% of all websites globally and around 62% of websites with a known content management system (Figure 1).

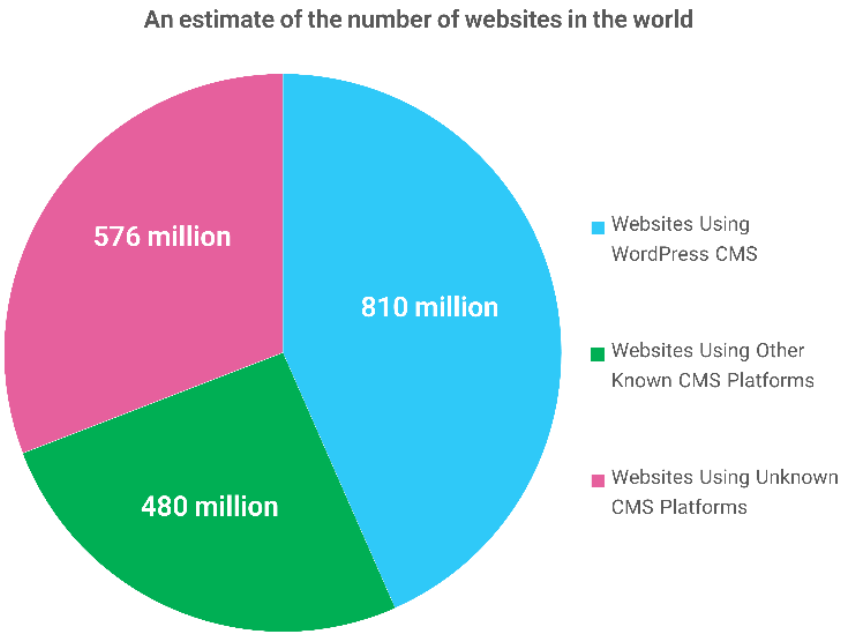

Figure 1: A representation of global websites and their respective content management systems

For website owners, site traffic is an important factor that requires attention, as the success of a website is typically determined by its traffic. Additionally, maintaining a website not only requires time but also incurs costs, and a lack of visitors can negatively impact those who have launched their websites as an online business.

Implementing Search Experience Optimization (SXO) techniques—or a somewhat similar earlier concept known as Search Engine Optimization (SEO)—offers a solution to ensure that a website is optimized both for users and visitors searching for the content provided on the site and for search engines. This allows the site to be more easily recognized and ranked higher, thus appearing on the first page of search results. Increasing sales is one of the reasons businesses need SEO. Of course, other ways can drive traffic to a website, and search engines are just one of them [2], which is the focus of this paper. Typically, searchers enter relevant keywords into search engines and visit the websites that appear on the results page. This has created competition among websites operating in similar domains [3]. Therefore, to increase the chance of attracting traffic to the website, it is essential to ensure that the website is sufficiently indexed by search engines to increase the likelihood of appearing on the first page. To make a website easily identifiable by search engines, Search Engine Optimization (SEO) techniques must be employed [4, 5].

Paying attention to these SEO tips, which will be discussed later in the paper, provides a way for your website or blog to appear higher in the search engine results

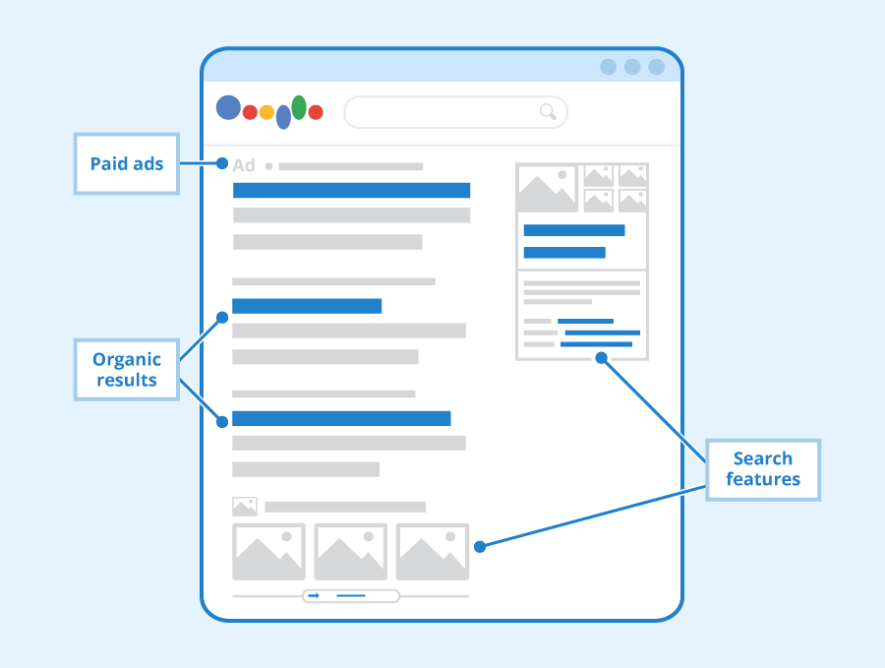

Figure 2: A view of a search engine results page (SERP) in a browser [7]

page (like Google or Bing) and attract more visitor traffic. Thus, the overall goal of implementing SEO techniques on a website or blog is to improve its ranking in search engines, specifically achieving placement on the first page of search results (SERP), indicating that SEO optimization methods are working effectively [6] and are impactful (Figure 2).

2 Literature Review

In this section, we will review concepts and previous research related to the topic of this study. First, a brief explanation of the internet and the web, as the main foundations of digital communication, will be provided to clarify their differences. Then, the functionality of search engines and their impact on website optimization strategies will be examined. Finally, the role of artificial intelligence (AI) in transforming and improving search engine performance, along with its challenges, and its influence on website optimization strategies will be discussed.

It is important to note that the findings and information in this field are sometimes based on data and documentation published by the search engine providers themselves. However, in some cases, these results are derived from leaked internal information from these companies (which at times contradicts their officially published documents regarding SEO metrics). Additionally, practical experiences and analyses from SEO specialists working in digital marketing agencies, who are directly involved in website optimiza-

tion, have been referenced. This combination of various sources leads to a deeper understanding of how search engines function and how their optimization strategies can be improved.

2.1 The Internet and the Web

The Internet, known as a network of interconnected networks, is a global system that connects all computer networks using the TCP/IP (Transmission Control Protocol/Internet Protocol) standard, allowing any user with a digital device, such as a computer or mobile phone, to access services provided by servers or other users. As a result, the widespread penetration of the internet has had a positive impact on the advancement of technology, particularly in the fields of information and communication [8]. This includes the exchange of data, images, videos, and sound [9].

The World Wide Web, or the web, commonly referred to as "www" is one of the services available on the internet and is widely used for transferring data across the internet, as it supports multimedia. In other words, information is transmitted not only through text but also via images, videos, sounds, and other files. In terminology, a website is defined as a collection of web pages typically grouped under domains or subdomains on the World Wide Web. The homepage of a website contains text, images, or information arranged in a particular format determined by the site owner, often with the help of a web designer. The homepage may also include links to other important pages or a table of contents for the site's pages. Visitors can access a website directly or indirectly. For direct access, visitors are usually directed to the homepage, but for indirect access (often through search engines), they are led to a non-homepage that contains keywords they searched for [10]. Today, SEO specialists and content creators strive to develop dedicated, optimized pages for specific keywords, which are referred to as landing pages.

2.2 Search Engines

Search engines are websites designed to search for various information resources across other websites. In addition to websites, many search engines now offer installable applications. Search results display a wide range of data from different websites as information sources, helping users find content stored on other sites. While search engines use different algorithms and methods to display results, fundamentally, every search engine scans portions of the internet for important keywords and presents the relevant words and phrases to users [11]. Some search engines increase search speed by scanning portions of the internet offline, storing them in a history-like cache, and regularly updating them.

Table 1: Examples of On-Page and Off-Page Optimization

On-Page Optimization	Off-Page Optimization
High-quality, informative content (not just promotional)	Use of anchor text links
Page title tags	Relevance of the page title
Heading tags	External page ranking
Bold, italic, and underlined keywords	The topic of the website providing a meaningful link to your site
Alt tags for images	
Meta tags (keywords, descriptions)	
Linked keywords	

2.3 Search Engine Optimization (SEO)

Search Engine Optimization (SEO) is an effort to make websites more popular without the need for paid advertisements. However, this approach involves other costs, such as lightweight, fast, and optimized coding and programming, as well as the expenses associated with content production, including hiring writers for article creation or even studio teams for producing high-quality videos. SEO typically consists of two main components: on-page optimization [12], which includes elements you can often modify directly from your website's content management system, and off-page optimization, which involves creating content and referral links to your site from other websites. These components are further detailed in Table 1.

It is evident that optimization elements evolve over time. Other important factors also influence SEO, such as having a well-designed website and ensuring user and customer satisfaction

2.4 Search Engines and Artificial Intelligence

Search engine service providers, in addition to offering standalone AI services like interactive chat, are now aiming to integrate AI-generated answers and summaries directly into search result pages. While this raises legal and intellectual property concerns regarding the ownership of website content, it also impacts SEO optimization strategies. Previously, content creators would meticulously include all possible keyword variations because search algorithms operated on an exact match basis, where even a single character change could affect results. However, with AI integration, search engines now perform semantic understanding beyond simple keyword matching.

Critics argue that such algorithms can obscure search results, making ranking methods less transparent and even causing a decline in search engine performance. Despite these concerns, search engine providers are continuously improving their algorithms and result quality to maintain their position in this highly lucrative market. The search industry, though expensive and energy-intensive, has proven to be extremely profitable for the leading providers, despite the challenges faced by many companies in achieving

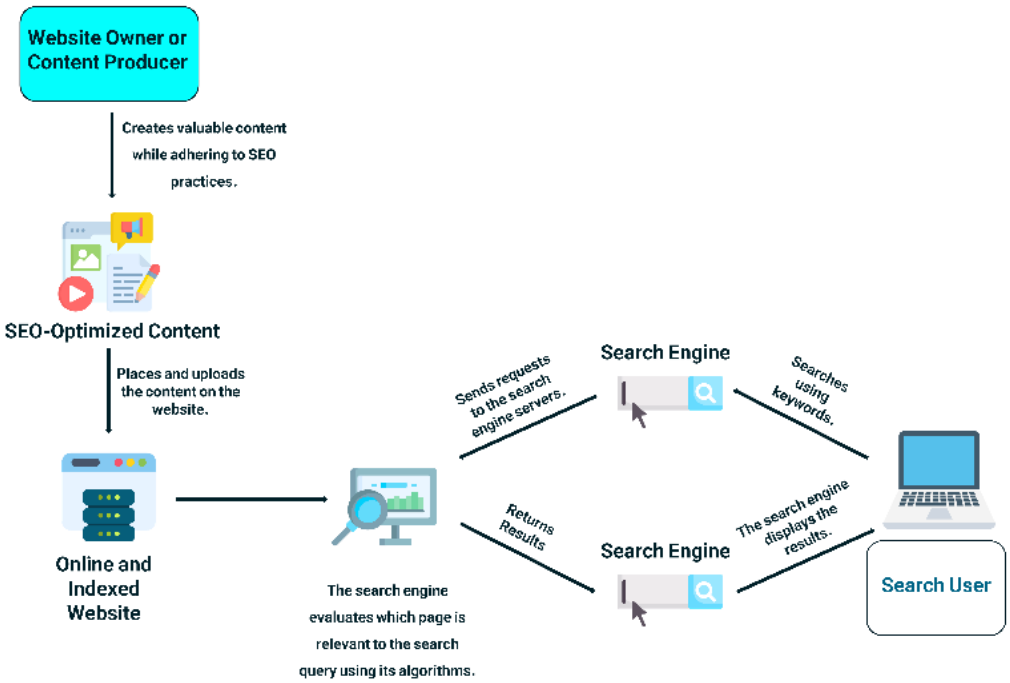

Figure 3: Diagram of the Search Process and Interaction Between Search Engine Users and Website Content Owners

success.

Artificial intelligence is shaping a new era of SEO, providing new opportunities for both search engine robots in ranking and website owners in optimization. AI can now interpret content more holistically, eliminating the need for content creators to include all variations of keywords or synonyms, thereby streamlining content production, search, and user delivery processes (Figure 3). However, this also introduces challenges, such as the need for software, content, and even structural changes on websites, as well as increased hardware processing costs for search engine service providers.

3 Research Methodologies

This research follows a five-step system development methodology, illustrated in Figure 4, which is based on the sequential or waterfall model. Initially, the necessary analyses are conducted for implementing and creating an SEO plugin for a website's content management system (CMS), such as a WordPress plugin [13]. Subsequently, the analyzed data is translated into a design that is user-friendly, and the SEO strategies for the target website are incorporated into the system design.

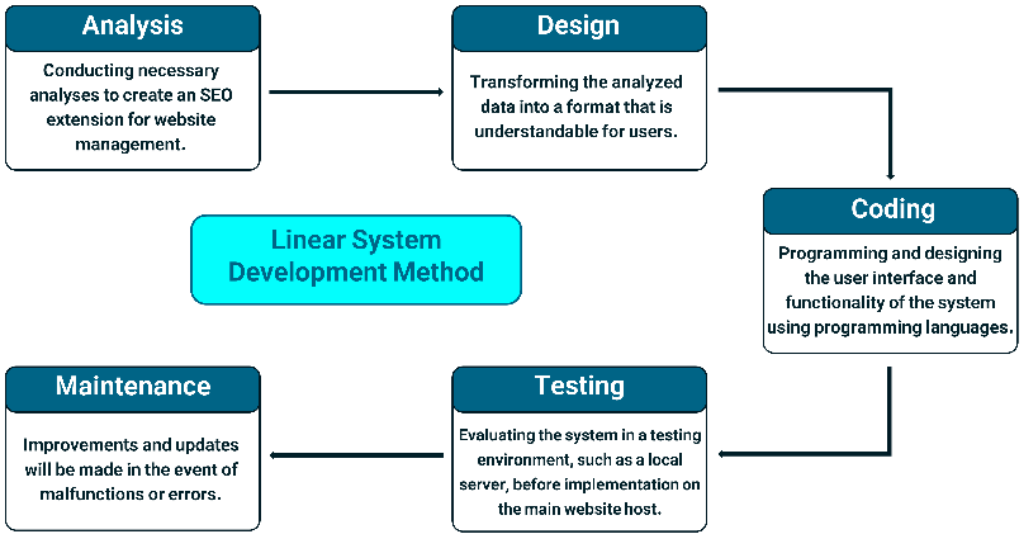

Figure 4: System Development Structure for Designing and Building an SEO Plugin

The system is then implemented as a coded application using programming languages like PHP, which is compatible with WordPress and Linux-based hosting services. During the testing phase, system evaluations are conducted in a simulated environment, such as a local server, to ensure the system functions properly before being deployed on the website's host. Finally, in the maintenance phase, updates and upgrades are applied to resolve issues such as system malfunctions or errors [14]. The developed software system must be capable of addressing both on-page and off-page SEO optimization needs, as well as providing AI tools for content generation and SEO status analysis.

4 Findings

Search Engine Optimization (SEO) is a multifaceted process that begins with problem analysis and the identification of needs [5]. Developing a system for SEO [15], where software plays a crucial role, significantly simplifies the process for website owners and makes SEO implementation more straightforward [16].

4.1 On-Page SEO Optimization

Website owners must first focus on optimizing the internal elements of their web pages. This optimization involves the proper configuration of page titles, content headings, meta descriptions, and relevant keywords. These elements are essential for structuring the website and aiding search engines in better understanding and interpreting the

content of the pages [17]. Furthermore, the visual appeal and page loading speed, which are partly the responsibility of content creators and partly the responsibility of programmers, should not be overlooked. These factors not only affect the rankings of search engines but also significantly impact user satisfaction, which is the ultimate goal. By implementing these changes, the website becomes more understandable for search engines and delivers well-organized and high-quality content to users, increasing user satisfaction and the likelihood of return visits or service and product purchases.

Search engine algorithms are continuously updated to provide a better user experience during searches. These updates are typically based on better analysis of user behavior and the delivery of more relevant content. One key factor in ranking on search results pages is user behavior, such as the time spent reading articles. This underscores the importance of content quality [18], which plays a crucial role in attracting users and encouraging them to spend more time on the website. Therefore, understanding the stages of optimization and conducting thorough keyword research are essential prerequisites for improving SEO. Keyword research is one of the most critical aspects of SEO, as it directly impacts the number of visitors attracted to the website. Choosing the right keywords is of utmost importance [19]; if chosen incorrectly, the website may not receive the appropriate traffic. Keywords can be categorized into short-tail, long-tail, and seasonal, each playing a vital role in the optimization process.

Short-tail keywords typically have high competition and were historically the most common search terms. However, over time, users have learned to input more detailed queries to achieve more precise results, leading to the prominence of long-tail keywords in search displays. Long-tail keywords generally have lower competition, though their significance has become more apparent to many business owners today. Seasonal keywords are those that are active during specific times of the year. For example, travel companies see a surge in traffic during holiday periods, stationery and office supply retailers during the back-to-school season, gift-giving businesses around festivals, and companies dealing in steel and construction materials in particular seasons of the year. This trend mirrors that of traditional physical markets, where businesses, through experience, understand which times of the year bring more customers. Today, in addition to competitor analysis, there are commercial tools available that can assist website owners in identifying the most effective keywords and applying them correctly.

4.2 Off-Page SEO Optimization

As previously mentioned, on-page SEO requires a focus on the technical and content elements of a website. This includes optimizing web pages, meta descriptions, keywords, and URLs (i.e., the addresses of the website's internal pages) [20]. However, with advancements in search engines or the introduction of new ranking criteria, additional elements may be introduced, or the current ones may lose their significance. Regardless, keeping these measures up to date ensures that search engines can correctly interpret the site's content, leading to improved search result rankings. Additionally, the use of

high-quality content, appropriate images, and videos can play a key role in increasing user engagement and boosting the website's ranking over time.

Off-page SEO is another crucial factor in improving search engine optimization. This encompasses activities conducted outside the website itself, such as building high-quality backlinks [21], along with valuable content and social media engagement [22]. Social media activity not only contributes to marketing efforts and attracting traffic and new customers [23], but also serves as a backup for your website's content. If you value your textual, visual, and video content, as well as other files such as PDFs, sharing them on social media and messaging platforms can ensure that if there is an issue with your site and content is lost, it can be recovered from these platforms. Although there are no absolute guarantees regarding the long-term availability of these social platforms, careful research can help you choose more reliable and valuable options. Search engines place significant importance on backlinks, as well as brand mentions without links, particularly those coming from reputable and relevant websites. The higher the quality of these backlinks, the more positive the impact on a website's ranking.

Therefore, to achieve optimal SEO results, website owners must pay close attention to both on-page and off-page optimization. This process not only involves technical optimization but also requires delivering high-quality content and fostering meaningful interactions with users via social media and other relevant platforms.

4.3 The Impact of Artificial Intelligence on SEO

In recent years, Search Engine Optimization (SEO) has become a vital component of digital marketing. However, traditional SEO tactics are no longer sufficient to keep up with the constantly evolving search engines and changing customer behavior. Artificial Intelligence (AI) has emerged as a game-changer in the SEO landscape, providing marketers with new methods and tools to optimize websites and content for search engines.

With the increasing integration of AI, search engines have improved their ability to understand user intent and deliver more accurate and relevant results. Consequently, businesses must optimize their websites and content more effectively to stay competitive and drive traffic.

Artificial Intelligence (AI) is a technology that enables computers or machines to perform tasks similar to those carried out by the human brain. In today's world, advancements in AI are being applied across nearly every aspect of life. In conjunction with digital marketing, AI simplifies how companies connect with customers at the right time.

The e-commerce sector has seen significant growth in recent years due to the rising popularity of online shopping and greater access to the internet and mobile devices. As a result, e-commerce websites are increasingly competing for customer attention and transactions. Companies are investing more in their digital strategies and e-commerce products, including enhancing user experience and developing more sophisticated and

personalized marketing efforts. They are also leveraging analytics and big data to gain insights into customer behavior, allowing them to deliver better-targeted marketing messages and products. With so many businesses competing for similar customers, e-commerce websites must keep their digital strategies and services up to date to remain competitive.

AI has a promising future in digital marketing. It can assist marketers in analyzing vast amounts of data and making more intelligent marketing decisions. Additionally, AI can help personalize marketing messages and deliver more targeted ads based on customers' specific preferences.

One of the most significant advantages of AI in digital marketing is its ability to automate many repetitive tasks. Data entry, content development, and social media management are examples of such tasks. This allows marketers to focus on more strategic activities like data analysis and developing new marketing initiatives.

In the future, we can expect to see more AI-powered chatbots and virtual assistants that provide personalized services and support to customers. Additionally, more AI-driven marketing automation products are likely to emerge, helping companies optimize their marketing operations and increase overall return on investment (ROI) [24].

AI technology can enhance a website's visibility in search engine results pages (SERPs). AI can analyze website content and optimize it for specific keywords and phrases relevant to a particular industry or niche. It can also identify technical SEO issues and suggest solutions to fix them. AI can help identify opportunities for link building, content marketing, and other SEO initiatives while detecting and eliminating harmful files or content. Moreover, AI can track visitor behavior and recommend ways to improve user experience.

By analyzing website content and optimizing it for relevant keywords and phrases, AI can boost a website's visibility in SERPs. By resolving these issues, websites can achieve higher visibility in SERPs [25].

5 Conclusion

Search Engine Optimization (SEO) is a crucial tool for improving a website's ranking on search engines. By effectively applying various SEO techniques, website owners can optimize their sites to achieve higher rankings on Search Engine Results Pages (SERPs). This increased visibility can drive more traffic to the site, which in turn leads to business growth. The process of website optimization encompasses strategies that target both on-page and off-page SEO. On-page SEO focuses on content optimization and the strategic use of keywords, while off-page SEO aims to enhance the website's credibility through backlinks and even unlinked brand mentions.

In addition to technical aspects of the site, such as optimized coding [26] and fast loading times [27], high-quality content is emphasized. Quality content, along with its presentation and layout, plays a significant role in attracting and retaining visitors.

Websites that offer valuable content are more likely to engage users and increase traffic, thereby improving their search engine rankings.

It is important to note that SEO is an ongoing process that requires continuous attention and effort. As search engine algorithms evolve, website owners must adapt their SEO strategies to maintain competitiveness and preserve high rankings.

Artificial Intelligence (AI) can assist in identifying user behavior patterns, which can be used to improve website performance, content quality, and user experience. Additionally, AI can automate repetitive tasks and optimize website maintenance, freeing up resources for further enhancement of website performance, content quality, and user experience [24].

References

[1] Brian, "Top 23 WordPress Statistics: Defining Trends and Insights for 2024", Hostinger Tutorials. Accessed: Sep. 25, 2024. [Online]. Available: https://www.hostinger.com/tutorials/wordpress-statistics

[2] N. Septiani, N. Lutfiani, F. Putri Oganda, R. Salam, and V. Tashya Devana, "Blockchain Technology in the Public Sector by Leveraging the Triumvirate of Security", in 2022 International Conference on Science and Technology, ICOSTECH 2022, 2022. doi: 10.1109/ICOSTECH54296.2022.9829101.

[3] S. Das, Search engine optimization and marketing: A recipe for success in digital marketing. Chapman and Hall/CRC, 2021.

[4] R. Supriati, E. Royani Dewi, Triyono, D. Supriyanti, and N. Azizah, "Implementation Framework for Merdeka Belajar Kampus Merdeka (MBKM) in Higher Education Academic Activities", IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 3, no. 2, 2022, doi: 10.34306/itsdi.v3i2.555.

[5] B. Mardisentosa, U. Rahardja, K. Zelina, F. P. Oganda, and M. Hardini, "Sustainable Learning Micro-Credential using Blockchain for Student Achievement Records", in 2021 6th International Conference on Informatics and Computing, ICIC 2021, 2021. doi: 10.1109/ICIC54025.2021.9632913.

[6] S. Schultheiß and D. Lewandowski, " 'Outside the industry, nobody knows what we do' SEO as seen by search engine optimizers and content providers", Journal of Documentation, vol. 77, no. 2, 2021, doi: 10.1108/JD-07-2020-0127.

[7] Seobility Wiki authors, "SERP - Definition and SEO Relevance", Seobility Wiki. Accessed: Sep. 29, 2024. [Online]. Available: https://www.seobility.net/en/wiki/SERP

[8] M. K. Daoud et al., "Optimizing online visibility: A comprehensive study on effective SEO strategies and their impact on website ranking", Journal of Infrastructure, Policy and Development, vol. 8, no. 7, p. 4860, 2024.

[9] D. Lewandowski, S. Sünkler, and N. Yagci, "The influence of search engine optimization on Google's results:: A multi-dimensional approach for detecting SEO", in ACM International Conference Proceeding Series, 2021. doi: 10.1145/3447535.3462479.

[10] T. Batiuk, V. Vysotska, and V. Lytvyn, "Intelligent system for socialization by personal interests on the basis of SEO technologies and methods of machine learning", in CEUR Workshop Proceedings, 2020.

[11] N. Noy, M. Burgess, and D. Brickley, "Google dataset search: Building a search engine for datasets in an open web ecosystem", in The Web Conference 2019 - Proceedings of the World Wide Web Conference, WWW 2019, 2019. doi: 10.1145/3308558.3313685.

[12] M. Poturak, D. Keco, and E. Tutnic, "Influence of search engine optimization (SEO) on business performance", International Journal of Research in Business and Social Science (2147- 4478), vol. 11, no. 4, 2022, doi: 10.20525/ijrbs.v11i4.1865.

[13] S. Julião and M. C. Malta, "A study of the WordPress SEO plugins for microformats", in ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, 2020. doi: 10.5220/0010014901540161.

[14] S. Haribabu, P. Siva Sai Kumar, S. Padhy, G. Deepak, A. Santhanavijayan, and D. Naresh Kumar, "A Novel Approach for Ontology Focused Inter- Domain Personalized Search based on Semantic Set Expansion", in 2019 15th International Conference on Information Processing: Internet of Things, ICINPRO 2019 - Proceedings, 2019. doi: 10.1109/ICInPro47689.2019.9092155.

[15] A. Panchal, A. Shah, and K. Kansara, "Digital Marketing - Search Engine Optimization (SEO) and Search Engine Marketing (SEM)", International Research Journal of Innovations in Engineering and Technology, vol. 5, no. 12, 2021.

[16] D. Giomelakis, C. Karypidou, and A. Veglis, "SEO inside newsrooms: Reports from the field", Future Internet, vol. 11, no. 12, 2019, doi: 10.3390/FI11120261.

[17] Y. Yang, K. Zhao, D. Zeng, and B. J. Jansen, "How search engine advertising affects sales over time: An empirical investigation", arXiv preprint arXiv:2008.06809, 2020.

[18] A. Mathur et al., "Dark patterns at scale: Findings from a crawl of 11K shopping websites", 2019. doi: 10.1145/3359183.

[19] C. Lopezosa, L. Codina, J. Díaz-Noci, and J. A. Ontalba-Ruipérez, "SEO and the digital news media: From the workplace to the classroom", Comunicar, vol. 28, no. 63, 2020, doi: 10.3916/C63-2020-06.

[20] Q. Yang, X. Hong, Z. Wang, and H. Zhang, "Reserve price of risk-averse search engine in keyword auctions with advertisers' endogenous investment", RAIRO - Operations Research, vol. 55, no. 1, 2021, doi: 10.1051/ro/2019103.

[21] Zaharuddin, U. Rahardja, Q. Aini, F. P. Oganda, and V. T. Devana, "Secure Framework Based on Blockchain for E-Learning during COVID-19", in 2021 9th International Conference on Cyber and IT Service Management, CITSM 2021, 2021. doi: 10.1109/CITSM52892.2021.9588854.

[22] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information", J Ambient Intell Humaniz Comput, vol. 10, no. 5, 2019, doi: 10.1007/s12652-018-0798-z.

[23] A. Van Looy, Social media management: using social media as a business instrument. Springer Nature, 2022.

[24] B. Rathore, "Usage of AI-Powered Marketing to Advance SEO Strategies for Optimal Search Engine Rankings", Eduzone : international peer reviewed/refereed academic multidisciplinary journal, vol. 05, no. 01, 2016, doi: 10.56614/eiprmj.v5i1y16.300.

[25] T. Kumar, "Integration of Intelligent AI & SEO: A Review of Various Factors", 2023.

[26] J. Hassan Noor, "The effects of architectural design decisions on framework adoption: A comparative evaluation of meta-frameworks in modern web development", 2024.

[27] K. Kowalczyk and T. Szandala, "Enhancing SEO in Single-Page Web Applications in Contrast With Multi-Page Applications", IEEE Access, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3355740.

Cyberattack Defense in Smart Cities: Leveraging Quantum Neural Networks for Secure Route Planning in ADAS

Mahdi Seyfipoor[1], Mohammad Javad Samii Zafarqandi[2], Siamak Mohammadi[3]

[1] *PhD Student at School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Iran*
mahdiseyfipoor@ut.ac.ir
[2] *Undergraduate Student in Computer Engineering at Faculty of Engineering, College of Farabi, University of Tehran, Iran*
mjavadsamii@ut.ac.ir
[3] *Associate Professor at School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Iran*
smohamadi@ut.ac.ir

Abstract

In the context of smart cities, real-time route planning systems are essential for both autonomous and conventional vehicles. However, the reliance on Advanced Driver Assistance Systems (ADAS) introduces cybersecurity vulnerabilities. This paper proposes a framework using Quantum Neural Networks (QNNs) to address these issues by combining quantum computing's data processing capabilities with neural networks' decision-making strengths. The framework incorporates real-time threat detection using quantum parallelism and neural network pattern recognition to identify and mitigate cyberattacks at an early stage. Quantum algorithms, such as Grover's and Shor's, are utilized to optimize search processes and secure communications. QNNs enable dynamic feedback, refining decision-making to adapt to evolving threats while maintaining computational efficiency. The integration of QNNs enhances route planning and protects transportation systems against emerging cyber threats, contributing to improved operational efficiency and cybersecurity resilience in smart cities.

Keywords: *Cyberattack, Smart City, QNN, Route Planning, ADAS.*

1 Introduction

1.1 Smart Cities and Urban Mobility

Smart cities are urban environments that leverage advanced technologies to improve the quality of life for citizens by optimizing infrastructure, services, and communication

systems. Central to the smart city concept is the integration of digital technologies, data analytics, and automation to manage resources more efficiently and sustainably. In this context, the transportation sector plays a pivotal role, with technologies such as Advanced Driver Assistance Systems (ADAS) and autonomous vehicles facilitating efficient, safe, and eco-friendly mobility solutions. These systems rely on real-time data processing and intelligent decision-making to enable smooth operation within densely populated urban areas.

1.2 Cybersecurity Challenges in Smart Cities

Despite their potential, smart cities are vulnerable to a range of security threats stemming from the heightened interconnectivity of devices and systems. The extensive use of sensors, networks, and software in managing urban infrastructure presents numerous entry points for cyberattacks. Threat actors can target a wide range of city functions, including power grids, public transportation, traffic management, and communication networks. Successful cyberattacks on these systems could disrupt essential services, compromise citizen privacy, and cause severe economic damage. Thus, cybersecurity has become a critical concern for the reliable functioning and future development of smart cities.

1.3 Cyber Attacks on Vehicles and ADAS

Among the various smart city components, the transportation sector, especially vehicles equipped with ADAS, is particularly vulnerable to cyber threats. ADAS enhances vehicle safety [1] by offering features like automatic braking, lane departure warnings, and adaptive cruise control, relying heavily on data inputs from external sensors and systems for route planning, traffic updates, and vehicle-to-vehicle communication. Cyberattacks on ADAS can target these critical functions, disrupting route planning algorithms, misinforming vehicle navigation systems, or even overriding essential safety features. Such attacks could lead to traffic accidents, endanger passengers, and disrupt urban mobility on a large scale.

1.4 Preventing Cyberattacks with Quantum Neural Networks

To counter these cybersecurity threats, several solutions have been proposed, ranging from enhanced encryption techniques to advanced intrusion detection systems. Among these, Quantum Neural Networks (QNN) have emerged as a promising approach. QNN [2] combines the computational power of quantum computing with the adaptability of neural networks, offering potential breakthroughs in real-time threat detection and response. By leveraging quantum algorithms, QNN can process vast amounts of data at unprecedented speeds, significantly accelerating decision-making processes, which is essential for time-sensitive applications like route planning in ADAS. Furthermore, QNN

enhances security by making it more difficult for attackers to predict or manipulate system behavior, providing an additional layer of defense against increasingly sophisticated cyberattacks.

2 Related Works

Cyberattacks present significant threats across various sectors, exploiting vulnerabilities in critical industries such as healthcare, finance, and infrastructure. In healthcare, ransomware attacks compromise patient data, disrupt essential services, and lead to substantial financial losses, underscoring the need for enhanced cybersecurity measures [3]. In the financial sector, Distributed Denial of Service (DDoS) attacks exploit the expanding digital presence of banks, with advanced models such as Support Vector Machines (SVM) proving effective in detecting these attacks [4]. Critical infrastructure, including energy and manufacturing, is increasingly vulnerable due to digital transformation, with many risks stemming from outdated legacy systems and inadequate cybersecurity investments [5].

To mitigate the risks posed by cyberattacks, various approaches have been developed across industries. Traditional methods such as encryption and Intrusion Detection Systems (IDS) are commonly employed, while newer technologies like blockchain and machine learning (ML) are gaining traction. Data encryption, including the use of AES algorithms, ensures secure data transmission, particularly in high-stakes applications like those in the mining sector [6]. IDS remain vital in detecting network intrusions, with innovations like the Neighborhood Outlier Factor significantly improving anomaly detection in distributed systems [7]. Blockchain provides decentralized solutions but still faces challenges related to scalability and security [8]. Meanwhile, machine learning plays a critical role in cybersecurity by analyzing large datasets, improving threat detection capabilities, and adapting to the ever-evolving threat landscape [9].

In this paper, we employ QNN to counter cyberattacks on ADAS and route planning, harnessing its speed and adaptability to significantly improve threat detection and response in these critical, time-sensitive systems.

3 Optimizing Route Planning and Security in Dynamic Urban Environments

3.1 Dynamic Urban Environments

One significant advancement in dynamic urban environments is the rise of autonomous vehicles. These self-driving cars use advanced technologies, such as real-time object detection, parallel processing, and route planning, to navigate city streets efficiently and safely. Their capability to process extensive data in real-time allows for rapid decision-making, obstacle avoidance, and the selection of optimal routes [10]. This significantly reduces traffic jams and enhances overall transportation efficiency.

Despite these advancements, there are still significant challenges in optimizing route planning in such complex and ever-changing environments. Quantum computing, particularly QNNs, offers a promising solution. Quantum computing leverages the principles of quantum mechanics to perform computations much faster and more efficiently than classical computers. QNNs can process and analyze large and complex datasets more effectively, enabling more accurate and efficient route optimization in dynamic urban settings.

In this paper, we first define route planning in urban environments and explain the fundamentals of QNNs. We then introduce strategies for enhancing QNNs' performance and compare these strategies based on specific criteria.

3.2 Advanced Driver Assistance Systems (ADAS)

ADAS refers to a collection of technologies designed to enhance vehicle safety and facilitate more efficient driving by assisting the driver in various scenarios. This system uses sensors, cameras, and other technologies to monitor the vehicle's surroundings and provide real-time feedback or assistance. ADAS offers support in decision-making during driving, especially in complex, dynamic environments, such as urban areas with heavy traffic, unpredictable pedestrian movements, and frequent changes in road conditions.

ADAS plays a significant role in enhancing driver awareness by issuing warnings and taking partial control of the vehicle when necessary [11]. In Fig. 1, ADAS Sensors are shown. The data from these sensors is fused to enable real-time processing and decision-making. This system can detect potential hazards, issue alerts, and intervene to prevent or mitigate accidents. They are designed to assist, not replace, human drivers, but in certain situations, such as route planning or avoiding obstacles, ADAS may temporarily assume control over specific vehicle functions. One crucial aspect of ADAS is its contribution to route planning. By continuously analyzing traffic patterns, road conditions, and other variables, ADAS helps drivers select optimal routes. This feature is especially valuable in dynamic urban environments, where traffic congestion, roadwork, and other obstacles frequently arise. By making real-time adjustments to routes, ADAS can improve efficiency and safety, reducing the cognitive load on drivers.

With the growing reliance on ADAS for tasks such as route planning, the system becomes increasingly susceptible to cyber-attacks, particularly in scenarios where control is delegated to ADAS. Cybercriminals target these systems to exploit vulnerabilities, leading to potential disruptions. These attacks can manipulate or disable ADAS-controlled features like route planning, creating hazardous conditions for drivers. For instance, an attack could alter the vehicle's routing algorithms or deactivate critical safety functions when ADAS is in control, severely undermining the system's reliability. Protecting ADAS from such threats is vital, as a compromised system in urban environments, where split-second decisions are essential, could result in catastrophic consequences.

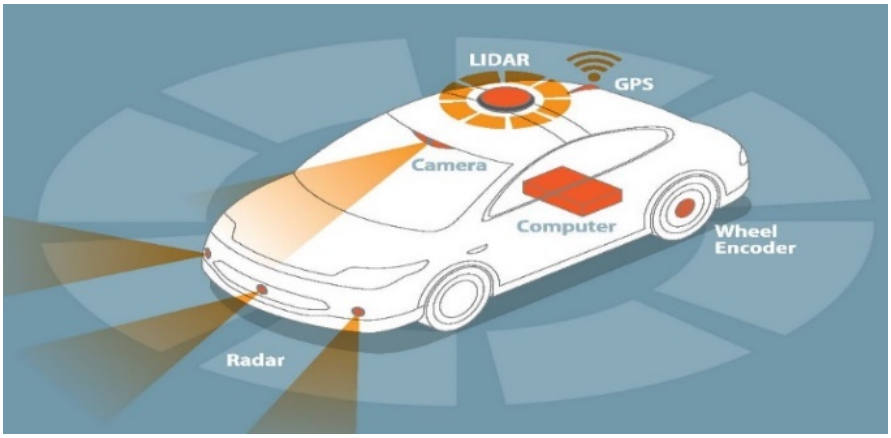

Figure 1: Overview of ADAS Sensors, Including Radar, LIDAR, Camera, and GPS

3.3 Route Planning

Route planning is a process used to determine the most optimal path from a starting point to a destination, considering various factors such as distance, time, traffic conditions, and user preferences. As illustrated in Fig. 2, the process involves collecting and analyzing large volumes of data, including map data, traffic information, speed limits, and real-time data such as traffic congestion [12]. This information is critical for determining the best possible route.

To achieve optimal pathfinding, route planning systems rely on sophisticated algorithms. Common examples include Dijkstra's algorithm and the A* algorithm, which evaluate nodes and edges in a graph to calculate the shortest or fastest route based on predefined metrics. These algorithms efficiently process potential routes and identify the most suitable path for navigation. As these systems advance, they increasingly integrate real-time data and user preferences to provide more effective navigation solutions [13]. However, the increasing complexity and connectivity of route planning systems in smart cities also introduce significant security risks. These systems, which manage both machine and human transportation, are vulnerable to cyberattacks. Malicious actors could attempt to take control of the system, manipulating route suggestions and creating a controlled environment that favors their objectives. By controlling critical transportation routes, attackers could generate widespread disruptions, traffic jams, or even chaos across a city.

4 Cybersecurity Risks

The concept of control is fundamental to understanding the threats posed by cyberattacks on route planning systems. Attackers aim not just to disrupt navigation but to take control of the system itself. By manipulating data inputs, altering suggested

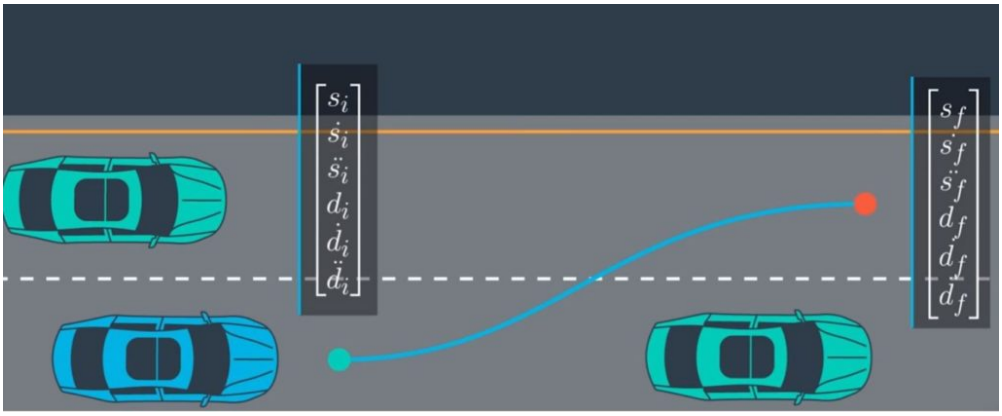

Figure 2: Route Planning Utilizing Map Data, Traffic Information, Speed Limits, and Real-Time Data

routes, or intercepting communications between the user and the navigation system, cybercriminals [14] can direct vehicles along paths that serve their interests, potentially leading to hazardous or destructive outcomes in urban environments. Given the high stakes in smart city ecosystems—where both machines and humans rely on seamless transportation—robust, real-time cybersecurity measures are essential. These systems must be capable of detecting and responding to threats in real time, preventing attackers from gaining control over critical urban infrastructure.

4.1 Types of Cyberattacks on ADAS

Cyberattacks on ADAS, particularly in relation to route planning, take several forms:

Data Manipulation: By tampering with sensor inputs or traffic data, attackers can mislead the system into making incorrect routing decisions.

Man-in-the-Middle (MitM) Attacks: Intercepting communications between the ADAS and external data sources allows attackers to inject false information or reroute vehicles.

Denial-of-Service (DoS) Attacks: Overwhelming the system with illegitimate requests can render the ADAS unresponsive, disrupting real-time route updates.

Algorithm Exploitation: Exploiting weaknesses in the route-planning algorithms can lead to unsafe or inefficient decisions.

4.2 Cybersecurity Framework for Route Planning in ADAS

To address these vulnerabilities, a comprehensive cybersecurity framework for ADAS is proposed, focusing on three main components: detection, prevention, and post-attack correction.

Figure 3: Post-Attack Route Correction

Detection of Cyberattacks: The system's first responsibility is identifying when a cyberattack is taking place. Continuous, real-time monitoring of ADAS inputs and outputs enables the detection of anomalies. Neural networks (NNs), known for their strength in pattern recognition, are utilized to detect deviations from normal behavior, such as sudden route changes or inconsistencies between sensor data and external communications. These networks can learn and adapt to new threats over time, improving their accuracy in identifying attacks.

Prevention of Cyberattacks: Once an attack is detected, the system must act immediately to prevent further damage. This includes blocking unauthorized data inputs, stopping suspicious communications, and verifying the accuracy of incoming data. Predictive analytics help anticipate potential attack methods by analyzing past data, allowing the system to take preemptive measures. If needed, the system can assume temporary control, rerouting the vehicle or implementing safety protocols to avoid high-risk areas or dangerous situations.

Post-Attack Correction: In situations where the attack is not detected or prevented in real time, the system must be able to diagnose and correct the effects of the attack. As Shown in Fig. 3, Post-attack correction is initiated when the system identifies deviations from pre-set constraints programmed into the ADAS. Neural networks trained under specific guidelines—such as avoiding highly congested areas, quiet backroads, or one-way streets—play a key role in identifying compromised routes. If the vehicle enters restricted or dangerous zones, the system will recognize this as an attack and respond by either rerouting the vehicle to a safer path or correcting the route to ensure passenger safety.

4.3 Leveraging Neural Networks for Advanced Cybersecurity Solutions

Neural networks are a key component of this cybersecurity framework due to their ability to identify patterns, handle complex data, and continuously learn from new information. These characteristics are essential for detecting anomalies that may signal a cyberattack [15], as well as for real-time decision-making. NNs excel at analyzing large, multifaceted datasets—such as traffic conditions, sensor inputs, and communication streams—and making quick, accurate decisions that prevent or mitigate attacks. Moreover, neural networks' learning capabilities allow them to adapt to evolving threats, improving the system's ability to detect new types of cyberattacks over time.

In the event that an attack has caused the vehicle to be directed onto an incorrect or unsafe route, neural networks also play a critical role in post-attack correction. By quickly assessing the situation and comparing it against known safe parameters, the system can autonomously reroute the vehicle or make necessary adjustments to ensure a safe journey.

4.4 Real-Time Processing and Quantum Computing

Given the rapidly changing and unpredictable nature of urban environments, real-time processing is critical to the success of this cybersecurity framework. The system must handle large volumes of sensor data, vehicle communications, and traffic information simultaneously and without delay. To meet these demands, parallelism is required, allowing multiple processes to run concurrently to ensure that threat detection, prevention, and route correction occur in real time. Quantum computing offers a powerful solution to this challenge. Quantum computers can process large datasets in parallel, significantly reducing the time needed for complex calculations. When integrated with neural networks, quantum computing enhances the system's ability to detect cyber threats, optimize routes, and secure communications. This combination provides the computational power required to process vast amounts of data in real time, while also improving the system's accuracy and speed in responding to threats.

The integration of quantum computing with neural networks, resulting in QNNs, presents a promising direction for enhancing the cybersecurity of ADAS-controlled systems. In the subsequent sections, the potential of quantum computing to enhance neural network performance will be examined, particularly in the context of real-time threat detection, decision-making, and route optimization. By leveraging the strengths of both technologies, the system can offer robust protection for critical transportation infrastructure, ensuring both safety and operational efficiency amid evolving cyber threats.

5 Quantum Computing

Quantum computing is a new approach to calculation that uses principles of fundamental physics to solve extremely complex problems very quickly. Quantum computing

uses subatomic particles, such as electrons or photons. Quantum bits, or qubits, allow these particles to exist in more than one state (i.e., 1 and 0) at the same time. Quantum neural networks are computational neural network models which are based on the principles of quantum mechanics.

5.1 The Fundamentals of Quantum Computing

In quantum computing, superposition refers to the ability of a qubit to exist in multiple states simultaneously. Unlike classical bits, which can be either 0 or 1, qubits can be in a state that is a combination of both 0 and 1 [16]. This is a fundamental concept of quantum mechanics and is crucial for the power of quantum computing.

Quantum computers operate with the so-called qubits, which are quantum states that are allowed to be in a superposition of the two orthonormal vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

The symbol $|\rangle$ is called a ket. It is used to denote a column vector. These two vectors form the canonical basis of C^2 and are referred to as the computational basis. Now, qubits in a pure state can be expressed as:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2}$$

A general qubit state $|\Psi\rangle$ can be expressed as a linear combination of these basis states

where $\alpha, \beta \in C$ and fulfill [17]:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

5.2 Quantum Gates

Quantum gates and qubits are the fundamental elements of gate-based quantum computations. These gates are unitary operators that act on qubits, represented by unitary matrices of size $2^n \times 2^n$, where n is the number of qubits the gate operates on.

The Pauli X, Y, and Z gates are fundamental examples of single-qubit gates. These gates can be represented in the standard basis $\{|0\rangle, |1\rangle\}$ as follows:

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4}$$

which represent a π radians rotation around the x, y, or z axis respectively. Note that this gate functions similarly to the logical NOT gate, which converts 0 bits to 1 bits and vice versa. Also, Hadamard gate could be introduced as below:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{5}$$

which creates a superposition of $|0\rangle$ and $|1\rangle$. The Hadamard gate can also be interpreted as a $\frac{\pi}{2}$ radians rotation in y, followed by a π radians rotation in x. There also exist gates that act on multiple qubits. An essential type of these multiple qubit gates is the controlled gate. Given a unitary matrix U of dimension n. The $(d+n)$-dimensional controlled-U gate, C-U, is the matrix of the form:

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \tag{6}$$

where I is the d-dimensional identity matrix. An important example of controlled gates is the controlled-NOT (CNOT) gate. When expressed in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, it is:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{7}$$

5.3 Quantum Algorithms

Quantum computing enables parallel processing on an unprecedented scale, allowing the system to monitor and process multiple data streams simultaneously. In the context of route planning, quantum computers can be employed to ensure real-time analysis and decision-making without compromising the speed or accuracy of the route suggestions.

For example, Grover's algorithm, a quantum algorithm designed for search optimization, can be used to rapidly scan through vast datasets to detect anomalies or malicious activities within the system [18]. It achieves this in significantly fewer steps than classical algorithms, making it highly effective in identifying and mitigating security threats in real time.

Additionally, Shor's algorithm can be applied to enhance the cryptographic security of communication channels used by route planning systems. While traditionally used to break classical encryption methods, Shor's algorithm can also be utilized to develop quantum-resistant encryption protocols. This helps secure the transmission of data between different components of the system, ensuring that hackers cannot intercept or manipulate the information flowing through the route planning infrastructure.

6 Hybrid Approach: Quantum Neural Networks (QNNs)

QNNs combine the computational power of quantum mechanics with the learning capabilities of neural networks. By harnessing quantum computing's ability to process complex data and neural networks' capacity for pattern recognition and decision-making, QNNs offer an advanced framework for optimizing systems like ADAS (Advanced Driver Assistance Systems), particularly in the context of cybersecurity and real-time route planning.

6.1 Structure of QNNs

QNNs integrate the computational capabilities of quantum circuits with the learning power of neural networks to enhance performance, particularly in tasks involving high-dimensional data and complex decision-making. The structure of QNNs is built to capitalize on quantum parallelism, where quantum gates and circuits perform operations like superposition and entanglement, allowing the system to explore multiple possibilities simultaneously. This quantum parallelism accelerates the processing of complex input data, such as sensor readings or environmental information, by transforming it into quantum states that can be analyzed more efficiently.

Once the input data is encoded into quantum states, the quantum circuits process it, handling tasks like feature extraction, optimization, or pattern recognition [19]. This processing in the quantum layer enables the system to rapidly explore multiple scenarios, ensuring that computationally intensive tasks are managed effectively. The refined quantum data is then converted back into classical information and passed to the neural network layers for further interpretation. The neural networks, leveraging the optimized quantum data, make predictions and decisions based on the refined information, such as identifying cyberattacks or determining optimal routes.

In certain QNN configurations, the interaction between quantum and neural components extends to a feedback loop, where the output from the neural network is reintroduced into the quantum layer for further optimization or refinement. This iterative process creates a dynamic flow of information between the two systems, allowing for continuous learning and real-time adaptation to evolving scenarios. The quantum feedback loop ensures that QNNs remain flexible and responsive to new data or threats, improving the overall decision-making process.

A key advantage of QNNs lies in the quantum speedup they provide. Quantum algorithms enable the system to perform complex tasks such as optimization and pattern recognition more rapidly than classical methods, particularly when dealing with large datasets or intricate decision-making scenarios. This hybrid architecture ensures that QNNs can efficiently process and analyze high-dimensional data, making them ideal for real-time applications like cybersecurity in dynamic environments.

By combining the strengths of quantum computing and neural networks, QNNs create a powerful system that not only handles vast amounts of data but also improves decision-making and optimization processes. This integration enhances the system's ability to learn from new information and adapt to changes, making it a crucial tool in advanced applications requiring real-time processing and high accuracy.

6.2 Application of QNNs in Cybersecurity for ADAS

QNNs offer significant improvements to the cybersecurity of ADAS, particularly in the areas of detection, prevention, and post-attack correction.

In cyberattack detection, QNNs can process vast amounts of sensor data and communications in parallel, identifying anomalies faster and more accurately. Quantum

circuits preprocess complex data, such as sensor inputs and external communication patterns [20], identifying early signs of an attack before they become critical. The neural network interprets this quantum-processed data to detect deviations from expected behavior, such as sudden route changes or inconsistencies in data inputs.

In the prevention phase, QNNs use quantum algorithms to predict and prevent vulnerabilities by analyzing real-time data, optimizing the input for neural network layers to make immediate decisions. If a potential threat is identified, the system can block unauthorized inputs, reroute the vehicle, or trigger safety protocols. The combination of quantum speed and neural adaptability allows for proactive prevention, minimizing the potential for damage before an attack escalates.

And in post-attack correction, QNNs handle the complex task of diagnosing and correcting the effects of undetected or unresolved attacks. The quantum layer rapidly performs optimization tasks, such as finding alternative routes or restoring compromised systems, while neural networks apply the corrected information in real time. If the vehicle has been directed into dangerous or restricted zones, the QNN will promptly identify the issue and reroute the vehicle to safety, ensuring the attack's impact is neutralized.

6.3 Advantages of QNNs in System Security and Performance

QNNs provide several critical benefits in the context of ADAS cybersecurity. The combination of quantum data processing and neural network learning enables enhanced detection and decision-making capabilities, allowing the system to rapidly identify cyber threats and formulate accurate responses. QNNs' ability to process large volumes of data in real time is essential for dynamic urban environments, where fast and reliable decisions are crucial to maintaining safety.

Additionally, QNNs continuously learn and adapt, improving their effectiveness in detecting emerging threats. This learning ability, combined with quantum optimization, enhances the system's capacity to reroute vehicles during cyberattacks, ensuring passenger safety and minimizing disruption. The integration of quantum computing for complex tasks like real-time optimization and error correction ensures that ADAS can quickly recover from attacks and maintain operational efficiency.

The subsequent sections will delve deeper into the specific quantum algorithms and neural network structures employed in the QNN framework, illustrating their practical application in safeguarding ADAS-controlled systems from evolving cyber threats.

7 Experimental Results

This section presents a comparative analysis of classical and QNN-based route planning systems under various cyberattack scenarios. The results highlight the superior performance of QNN-based systems in terms of security and efficiency.

Table 1: Security robustness and recovery time comparison under cyberattacks

METRIC	CLASSICAL ROUTE PLANNING	QNN-BASED ROUTE PLANNING
DATA MANIPULATION ATTACK	Fails to detect subtle changes in sensor/traffic data, leading to incorrect routing decisions.	quickly identifies tampered data, ensuring minimal route deviations.
MITM ATTACK	Communication interceptions often lead to rerouting or incorrect decisions.	Detects and mitigates false information early, ensuring secure and accurate routing.
DOS ATTACK	System becomes unresponsive, causing significant delays in route updates.	Detects and isolates attack traffic, maintaining real-time updates with minimal delay.
ALGORITHM EXPLOITATION	Susceptible to algorithmic weaknesses, causing inefficient or unsafe decisions.	Strong resilience to exploitation, detecting anomalies and recalculating efficiently.
RECOVERY TIME	Takes longer to recover and recalibrate after attacks.	Recovers faster by quickly isolating and responding to attacks.
DETECTION ACCURACY	May miss sophisticated attacks or react too late.	Detects attacks more accurately due to quantum-enhanced pattern recognition.
SYSTEM DOWNTIME	High downtime due to delayed detection and mitigation.	Minimal downtime; recovers swiftly from attacks and resumes normal operations.

Table 1 shows that QNN-based systems respond to cyberattacks like Data Manipulation, MitM, and DoS more effectively, offering quicker detection and recovery compared to classical systems. Similarly, Table 2 demonstrates that QNN-based systems provide higher route accuracy, faster processing times, and better resilience to attacks, especially under heavy loads or attack conditions, while also being more power-efficient.

8 Conclusion

In dynamic urban environments, particularly with the rise of autonomous vehicles, efficient route planning is a critical challenge. Traditional algorithms like Dijkstra's and A* have served as foundational methods for navigating complex cityscapes, but they are now increasingly supplemented by quantum computing innovations. The combination of real-time data processing, advanced algorithms, and the growing integration of machine-to-human interactions has made route planning systems indispensable in smart cities. However, these systems are vulnerable to cybersecurity threats, where attackers seek to gain control and manipulate routes to create disruptions.

Quantum computing, with its unique properties such as superposition and entanglement, offers transformative potential for addressing these vulnerabilities. Quantum

Table 2: Performance metrics comparison in normal and attack conditions

Scenario	Route Accuracy	Processing Time	Attack Resilience	Power Efficiency
Classical (Normal Operation)	Good accuracy but vulnerable to incorrect decisions in complex environments.	Relatively slower, especially under high data loads.	Low resilience to attacks, leading to significant route deviations.	Moderate but increases significantly under attack conditions.
Classical (Under Attack)	Low accuracy during attacks; hard to maintain optimal routes.	Slows down further, exacerbating response time.	Vulnerable to repeated attacks with delayed recovery.	Increased power consumption due to repeated recalculations.
QNN (Normal Operation)	High accuracy, even in complex and dynamic conditions.	Faster computations due to quantum enhancements.	Naturally more resilient to attacks, ensuring accurate routing.	Efficient with minimal energy overhead.
QNN (Under Attack)	Maintains high accuracy even during sustained attacks.	Processes data efficiently with minimal delays, even under attack.	Strong resilience to attacks, detecting and responding early.	Slightly increased power, but more efficient under attack than classical systems.

Neural Networks (QNNs), Grover's algorithm, and Shor's algorithm provide tools for enhancing both the efficiency of route planning and the security of the system. QNNs enable more efficient data processing and better route optimization, while quantum algorithms can strengthen anomaly detection and cryptographic security, protecting the integrity of the system against malicious control. Furthermore, the integration of quantum machine learning ensures that route planning systems can adapt in real time, identifying and neutralizing potential threats before they escalate.

By leveraging the capabilities of quantum computing, urban route planning systems can not only optimize navigation but also defend against emerging cyber threats, ensuring secure, efficient, and resilient transportation networks in smart cities. As technology continues to evolve, the role of quantum computing will become increasingly essential in maintaining the balance between efficiency and security in these interconnected urban ecosystems.

References

[1] F. Jiménez, J. E. Naranjo, J. J. Anaya, F. García, A. Ponz, and J. M. Armingol, "Advanced Driver Assistance System for Road Environments to Improve Safety and Efficiency", Transportation Research Procedia, vol. 14, pp. 2245–2254, Jan. 2016.

[2] A. Kukliansky, M. Orescanin, C. Bollmann and T. Huffmire, "Network Anomaly Detection Using Quantum Neural Networks on Noisy Quantum Computers", in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-11, 2024.

[3] E. A. Al-Qarni, "Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies", International Journal of Advanced Computer Science and Applications, vol. 14, no. 5, 2023.

[4] U. Islam et al., "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models", Sustainability, vol. 14, no. 14, p. 8374, Jan. 2022, doi: https://doi.org/10.3390/su14148374.

[5] D. A. S. George, D. T. Baskar, and D. P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors", Partners Universal International Innovation Journal, vol. 2, no. 1, pp. 51–75, Feb. 2024.

[6] Y. Yu, "Encryption Technology for Computer Network Data Security Protection", Security and Communication Networks, vol. 2022, p. e1789222, Aug. 2022.

[7] J. Jabez and B. Muthukumar, "Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach", Procedia Computer Science, vol. 48, pp. 338–346, 2015, doi: https://doi.org/10.1016/j.procs.2015.04.191.

[8] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017.

[9] U. I. Okoli et al., "Machine learning in cybersecurity: A review of threat detection and defense mechanisms", World Journal of Advanced Research and Reviews, vol. 21, no. 1, pp. 2286–2295, 2024.

[10] M. M. Diaz and F. Soriguera, "Autonomous vehicles: theoretical and practical challenges", Transportation Research Procedia, vol. 33, pp. 275–282, 2018.

[11] S. L. Page, J. Millar, K. Bronson, S. Rismani, and Aj. Moon, "Driver perceptions of advanced driver assistance systems and safety", arXiv:1911.10920 [cs], Sep. 2021.

[12] D. Delling, P. Sanders, D. Schultes, and D. Wagner, "Engineering Route Planning Algorithms", Algorithmics of Large and Complex Networks, pp. 117–139, 2009.

[13] D. Luxen and C. Vetter, "Real-time routing with OpenStreetMap data", Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems - GIS '11, 2011.

[14] A. Giannaros et al., "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions", Journal of Cybersecurity and Privacy, vol. 3, no. 3, pp. 493–543, Sep. 2023.

[15] R. K. Vigneswaran, R. Vinayakumar, K. P. Soman and P. Poornachandran, "Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security", 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018.

[16] R. D. Schafer, "An Introduction to Nonassociative Algebras", 1996.

[17] G. Ortega Ballesteros and D. Cirici, "GRAU DE MATEMÀTIQUES Treball final de grau Quantum algorithms for function optimization", 2021.

[18] A. M. Dalzell et al., "Quantum algorithms: A survey of applications and end-to-end complexities", arXiv.org, 2023. https://arxiv.org/abs/2310.03011.

[19] K. Beer, D. Bondarenko, T. Farrelly, T. J. Osborne, R. Salzmann, D. Scheiermann, R. Wolf, "Training deep quantum neural networks", Nature Communications, vol. 11, no. 1, p. 808, Feb. 2020.

[20] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities", arXiv:2207.03534 [cs], Jul. 2022.

Vision-based Efficient Traffic Control and Scheduling System for Smart City Intersections with Emphasis on Emergency Vehicles

Mahdi Seyfipoor[1], Sayyed Muhammad Jaffry[2], Siamak Mohamadi[3]

[1] *PhD Student at School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Iran*
mahdiseyfipoor@ut.ac.ir
[2] *Undergraduate Student in Computer Engineering at Faculty of Engineering, College of Farabi, University of Tehran, Iran*
smjaffry@ut.ac.ir
[3] *Associate Professor at School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Iran*
smohamadi@ut.ac.ir

Abstract

Smart cities move towards automating tasks to make people's life easier. Signalized intersections are one of the most common issues people face on a daily basis. Using sensors to improve the time allotment for different roads at the intersection can reduce waiting time for the vehicles, which can in turn reduce pollution and simply help people reach their destinations faster. Leveraging computer vision can aid in this process. We can use object detection to analyze the busyness of different roads, emergency vehicles and accidents, to allocate suitable times to each road. It can also help reduce collisions due to premature green lights, resulting in cars entering the intersection crashing with those leaving it.

Keywords: *Smart City, Computer Vision, Edge Computing, Traffic Lights.*

1 Introduction

Smart cities are cities that use various sensors to provide its main operating systems with real-time data. This may include water, sewerage, traffic, law enforcement, security and surveillance systems [1]. The data that are collected can be used by city officials to aid in decision-making, efficient resource allocation, troubleshooting, or automate certain tasks. Automating the city's traffic control system can have many benefits: improve traffic flow, reduce CO_2 emissions, and lower the travel-time of passengers. One of the most valuable parts of a smart traffic control system, in controlling the intersections,

is using smart traffic lights. During different times of the day, traffic is distributed differently. Therefore, using a static time allotment scheme, that does not change based on the different circumstances, is inefficient. A dynamic time allotment policy takes into account various parameters such as, the busyness of a road, emergency vehicles that are arriving, and the cars in the intersection. Many countries have adopted some form of smart traffic lights. The goal of such systems is to use data available at intersections and roads to act like a traffic police officer, and hopefully better, since the officer may not have as much data as a system does. The control that the system has over the road needs to be backed by an accurate knowledge base, and these data can be obtained using sensors, such as, cameras. The use of computer vision can help us design such a system. It can conduct the necessary operations we require for a smart traffic light. Using object detection, we can detect the busyness of a road, identify any emergency vehicle (EV) and the path it is taking, and also find out if there are any cars in the intersection.

2 Related Works

Azad and Ramazani [9] propose an algorithm based on Q-Learning combined with deep neural networks, which resulted in a 34% decrease in queue waiting time. Wiering [10] proposed reinforcement learning algorithms, which reduced average waiting times by 25% in experiments where the cars were identical and travelled at similar speeds. Ferreira [11] introduced a infrastructure-less, vehicle-to-vehicle-communication based approach, and was able to show a reduction of CO_2 emissions up to nearly 20%. Younes and Boukerche [12] propose an arterial traffic light (ATL) controller, intelligent traffic lights communicate with each other to generate an efficient traffic light algorithm for the entire network. They also proposed intelligent traffic light controlling (ITLC) algorithm which schedules each isolated traffic light efficiently, resulting in a 30% increase in traffic flow fluency compared to the online OAF [13]. Gradinescu et al. [14] have also used a similar approach, resulting in significant reductions in waiting time, fuel consumption and pollutant emissions. Huang et al. [15] use syncronized timed Petri nets (STPN) to design an urban traffic network control system. They use a modular technique so that the network can be extended easily.

3 Methods

Our proposed smart traffic light control system consists of 4 units: Physical unit, object detection unit, processing unit and scheduling unit. The physical unit controls the flow of data from the sensors towards the object detection unit. It is the lowest level in the system. The object detection unit is tasked with identifying different objects and their count in the data provided by the physical unit. There are many models used for object detection, most famously Single-Shot-Detectors (SSD) [2], Residual Networks (ResNet)

[3] and You-Only-Look-Once (YOLO) [4]. YOLO is well-known for its fast and efficient performance, and lightweight versions of it such as YOLO-LITE [5] are used in embedded and real-time systems. The processing unit will gather the information of the vehicles, pedestrians, and active emergency vehicles, and process the information for the scheduling unit, which will allot green light-times to each road in the intersection. The units can be implemented in two major ways: edge computing (embedded), and server processing. The former uses a processor embedded inside the device that is controlling the intersection to store, process and analyze without using a dedicated external server, and in the latter the data are sent to an external server which will send an output back to the device [6]. Each method has its own advantages and disadvantages. In edge computing, we do not rely on network or cellular connections to send and receive information from the server, rather the device will compute the output on-site, making it favorable for real-time applications [6]. Using edge computing is also better for security, is more cost-effective, and lower in power consumption compared to traditional computing [6].

There is a lot of information that is available at an intersection. The data and conditions that our scheduler requires are as follows: active emergency vehicles and the roads they are approaching from, accidents that have occurred at the intersection or on any roads connected to the intersection, the existence of cars in the intersection, the number of cars on the roads connected to the intersection, and the pedestrians in or at the intersection. The scheduler treats each of the roads and pedestrian crossings as a set of *tasks* that need to be scheduled. Each of the roads and crossings (tasks) contain conditions, which are basically the vehicles or pedestrians occupying it. It will prioritize the roads based on the conditions as mentioned in table 1. The nature of the scheduler is similar to that of a Round Robin scheduling policy [7] because we use a circular queue. The difference is that each road will receive a time-slice that is decided by the conditions mentioned above, i.e. busyness, EVs and accidents. The effect of accidents on traffic and the proper methods of dealing with them need to be studied further, therefore in this paper, we have focused on emergency vehicles. Ghazal et al. [8] propose using a handheld controller to trigger the emergency vehicle protocol. This controller will be used by the emergency vehicles approaching the intersection. We propose using object detection to identify the emergency vehicles, but handheld devices can also be used to assist decision making.

As we can see, the vehicles that are already inside the intersection hold the highest priority, and will not be preempted by any other vehicles. A similar statement is also true for pedestrians inside the intersection. If any task is scheduled to activate next, it will have to wait until the higher priority tasks have been completed. A flowchart for the general functionality of the system is provided in fig. 1.

In fig. 1, we see that if the system spots an EV (Emergency Vehicle), it will attempt to open the signal for the road containing the EV, and keep that road open until the EV crosses the intersection. We understand that this shift cannot always happen instantaneously, as there may still be cars inside the intersection. Instead, the system

Table 1: Priorities of tasks in the scheduler, a greater priority shows higher importance

Conditions	Priority
Vehicles/pedestrians inside the intersection	3
Emergency Vehicles	2
Vehicles/pedestrians at the intersection	1

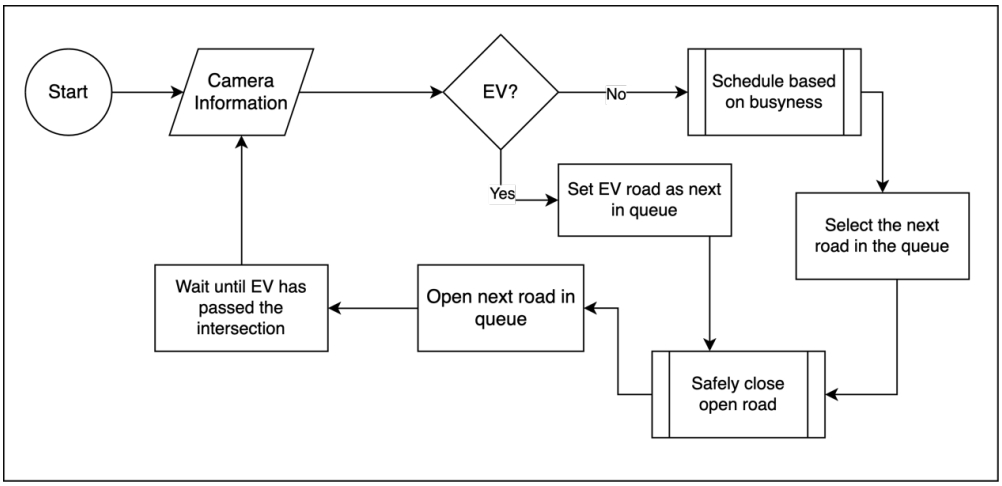

Figure 1: Flowchart of the traffic control system

will initiate a closing process for the currently open road, which is explained in fig. 2. It is important to note that the next road will open only once the safe closing process is completed, meaning that the intersection is clear of vehicles and pedestrians. In the scheduling process, the total period is divided among the roads, with busyness being the main factor. Newly arriving vehicles may or may not extend the time of a signal, but the signal will definitely stay open for a newly arriving EV.

Fig. 2 shows the safe road closing process. The light turns yellow for 3 seconds before turning red, after which it checks whether the intersection is clear of vehicles and pedestrians or not. The system will keep monitoring the intersection until it is empty.

We can define a syntax for possible scenarios: a road leading to an intersection I_i is denoted by L_i. The time remaining until the signal for L_i turns to green is $R_i(t)$. The time remaining until the signal for L_i turns yellow is $G_i(t)$. Busyness can be measured by a $busy\_factor$, where the sum of the $busy\_factor$ of all the roads equals 1.

There are 3 main approaches we can take in order to schedule times for each road. These approaches differ based on the total interval that is divided between the roads. One approach is to have a constant interval or period, denoted by P. After P seconds, the scheduler will reevaluate the intersection, and allot the times based on the new conditions. In this approach the sum of green light-times of all the roads are equal to P, such as shown in (1). Extending this approach can help us arrive at a superior method, which is a preemptive version of the one we just mentioned, meaning that the

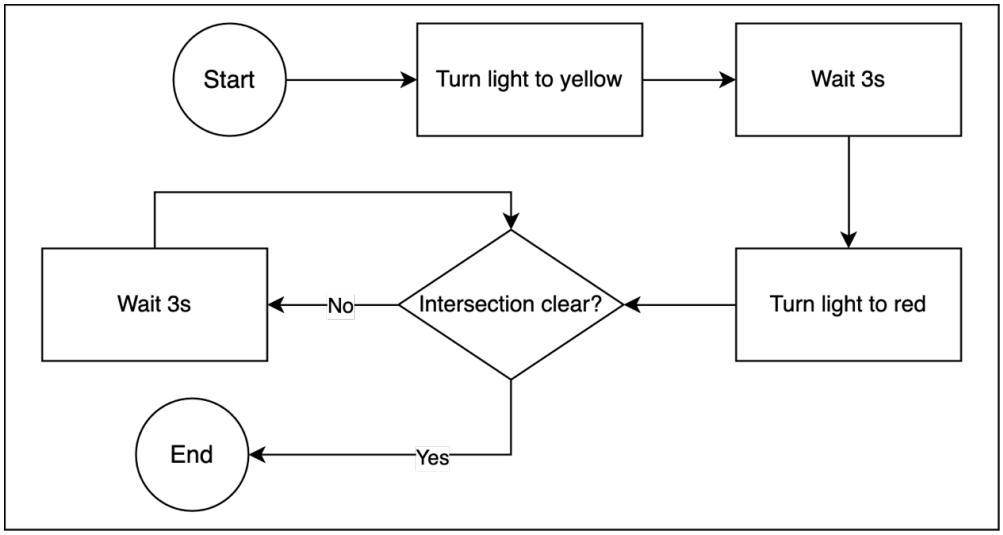

Figure 2: Safe road-closing process

scheduler will preempt the remaining allotted time to a task if it finishes prematurely. This can also be implied by using accurate data and car speeds in the simpler method.

$$\sum_{i=1}^{4} \max\{G_i(t)\} = \sum_{i=1}^{4} window\,(L_i) = P \tag{1}$$

$$Allocated\_Time = busy\_factor \times P \tag{2}$$

Another approach is to use memory for the scheduler. This way, the scheduler will remember the time allocation that was used during previous periods. If one road had stayed open for much longer than usual due to reasons such as an EV or a crash, the other roads will be compensated as they did not get a fair amount of time. The drawback to this approach is that even though the scheduler tries to be fairer than the first approach, this level of fairness may not be necessary most of the time, since the other roads might not be as crowded as the road with the longest time-slice in the previous period. Using memory can even cause a higher waiting time compared to not using memory, because the conditions can completely change during an interval.

A third approach is to have a dynamic period, in which the sum of the time-slices of the roads can vary depending on the conditions. For example, if all the roads leading to an intersection are more vacant than usual, then using a constant period will have a higher average waiting time for the vehicles at the intersection when compared to using a shorter period. Using a dynamic period can help by reducing the waiting time for the vehicles at an intersection. A question that naturally follows is how the period should be calculated at each interval, for which we propose using a set of predefined periods that can be used by the scheduler based on the current conditions. For example, an intersection can use the following periods based on the conditions {60s, 100s, 120s, 180s,

300s, etc.}. If the intersection is relatively empty, the scheduler can choose a smaller period so the utilization rate of the intersection stays high. From an OS perspective, this is similar to assigning the CPU to a new task when a task finishes before the time allotted to it ends, and in contrast to waiting for the allotted time to end, even if the task finishes sooner than expected. Using predefined periods simplifies the scheduling process, while providing a "good enough" scheduling scheme. Extending this idea, the scheduling process itself can also use a smaller quantum of time, and each road receives a multiple of the quantum. For Example, time-slices can be multiples of a 10 second quantum.

One point to keep in mind is that an accident or the arrival of an EV can occur at any time. If the system only updates the condition values after an interval, the effectiveness of the scheduling scheme will be reduced, and may even prove to be counter-productive to its objective. This leads us to constantly check for a change in high-priority conditions, so the system can only take action if a condition, such as an EV or cars inside an intersection, changes.

4 Simulation

We modeled the intersection as a task set, with each road leading to the intersection as a task. The vehicles are subtasks, with the EV subtasks having the ability to preempt other tasks in the intersection. While an EV subtask may not be the first subtask of a task, the task will keep running until the EV subtask is completed. Table 2 contains the information of the simulation setup. The simulation was done using Python. The preemptive versions of the algorithms were simulated.

The set of periods available for dynamic period selection was {60, 90,120,180,240}, and the choice was uniformly spread over the $busy\_factor$ axis.

The results of the simulation suggested that there was not a huge difference among the methods when it came to scenarios where the intersection was regarded as crowded. The waiting time and total number of cars passed was also similar. The main reason for this was that all 3 methods were preemptive in nature, meaning, that if there were no more cars on a road, the scheduler would stop the execution of that task. On the contrary, for simple traffic signals, the traffic light would keep on executing the same task until the allotted time for it was over, which resulted in a waste of valuable time.

5 Conclusion

We introduced 3 approaches to schedule the allocation of the intersection to the roads leading to it. The main points of difference in the methods were the use of memory and the selection of the scheduling period. Using memory will incur a cost, and is not needed anyways. Constantly gathering information causes all 3 methods to perform similarly, and therefore the different periods will not affect the system greatly.

Table 2: Simulation Setup Parameters

Parameter	Value
Period (not applicable to dynamic period)	240s
Time added per car	2s
Time it takes a car to cross the intersection	2s
Probability of new car arriving	10-40%
Probability of EV arriving	10%

References

[1] Moura, Filipe & de Abreu e Silva, Joao. (2021). Smart Cities: Definitions, Evolution of the Concept, and Examples of Initiatives.

[2] Wei Liu et al, "SSD: Single Shot MultiBox Detector", arXiv:1512.02325, 2015

[3] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun, "Deep Residual Learning for Image Recognition", arXiv:1512.03385, 2015.

[4] Joseph Redmon, Santosh Divvala, Ross Girshick, Ali Farhadi, "You Only Look Once: Unified, Real-Time Object Detection", arXiv:1506.02640, 2015.

[5] Jonathan Pedoeem, Rachel Huang, "YOLO-LITE: A Real-Time Object Detection Algorithm Optimized for Non-GPU Computers", arXiv:1811.05588, 2018

[6] K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research", in *IEEE Access*, vol. 8, pp. 85714-85728, 2020.

[7] Abraham Silberschatz, Peter B. Galvin, and Greg Gagne. 2012. Operating System Concepts (9th ed.). Wiley Publishing.

[8] B. Ghazal, K. ElKhatib, K. Chahine and M. Kherfan, "Smart traffic light control system", 2016 Third International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA), Beirut, Lebanon, 2016, pp. 140-145.

[9] Azad, Seyedeh & Ramazani, Abbas. (2023). Smart control of traffic lights based on traffic density in the multi-intersection network by using Q learning. Discover Artificial Intelligence.

[10] Wiering, M.; Vreeken, J.; Van Veenen, J.; Koopman, A. Simulation and optimization of traffic in a city. In Proceedings of the IEEE Intelligent Vehicles Symposium, Parma, Italy, 14–17 June 2004;

[11] M. Ferreira and P. M. d'Orey, "On the Impact of Virtual Traffic Lights on Carbon Emissions Mitigation", in *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 284-295, March 2012.

[12] M. Bani Younes and A. Boukerche, "Intelligent Traffic Light Controlling Algorithms Using Vehicular Networks", in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 5887-5899, Aug. 2016.

[13] K. Pandit, D. Ghosal, H. M. Zhang and C. -N. Chuah, "Adaptive Traffic Signal Control With Vehicular Ad hoc Networks", in *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1459-1471, May 2013.

[14] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea and L. Iftode, "Adaptive Traffic Lights Using Car-to-Car Communication", *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, Dublin, Ireland, 2007.

[15] Y. -S. Huang, Y. -S. Weng and M. Zhou, "Modular Design of Urban Traffic-Light Control Systems Based on Synchronized Timed Petri Nets", in *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 2, pp. 530-539, April 2014.