



RESEARCH ARTICLE - COMPUTER SCIENCE

"How can natural language processing improve cybersecurity threat detection?"

SAYMA NASRIN SHOMPA

International Islamic University Chittagong.
Computer Science and Engineering. Chittagong, Bangladesh.
Email: Saimanasrin453@gmail.com

Article Info.	Abstract
<i>Article history:</i> Received 8 July 2025 Accepted 15 August 2025 Publishing 30 September 2026	Natural language processing (NLP) is being rapidly applied in cyber space, as its capacity efficiently enables the process and the ability to analyze large versions of unnecessary text data, acceleratory detecting and more effective and more effective danger. This paper examines the integration of NLP in the manner of detecting the danger; the risk focuses on its role in intelligence information, fishing detection, malware identification and user behavioral analysis to identify discrepancy activities. Taking advantage of various machines learning patterns, the NLP can increase the identification and accuracy of the danger and prediction, including learning-pilgrimage, unheard, semi-conceptual, and reinforcement learning. Many cases study email detection, expediting the reaction of the event and user and unit behavioral analytics (UEBA) display their application. However, the study also identifies challenges such as data quality issues, rapid development of dangers, language ambiguity and adverse manipulation. Conclusions highlight that NLP has an important ability to strengthen cyber security systems by combining the NLP such as advanced approaches and combining with emerging technologies, making them more adaptive and intelligent.
This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/) <i>The official journal published by the College of Education at Mustansiriyah University</i>	
Keywords: Natural Language Processing (NLP); Cybersecurity; Threat Detection; Machine Learning; Phishing Detection; Anomaly Detection; User Behavior Analytics; AI in Cyber Defense; Text Classification; Semantic Analysis; Ethical AI; Hybrid Cybersecurity Systems.	

1. Introduction

Natural Language Processing (NLP) has emerged as a transformational technique in the field of cyber security, which offers powerful abilities to process and analyze large versions of unarmed text data. This capacity enables security teams to identify, classify and respond more efficiently. Sources of such data include social media, security forums, event reports and internal communications, which can provide valuable intelligence for all active defense measures [1] [2]. Since cyber threats are rapidly sophisticated, the integration of NLP in safety works has become an essential strategy to detect danger and increase the reaction of the event.

Within cyber security, NLP supports several functions, including the danger to detect discrepancy through intelligence gathering, fishing detection, malware analysis and user and unit behavior analysis (UEBA) [3] [4]. By applying techniques such as emotion analysis, designated unit recognition, and semantic analysis, NLP systems can identify suspected linguistic patterns and detect deviations from general communication behaviors [5] [6]. For example, the fishing detection models can analyze text materials for structural and linguistic discrepancies, while UBA systems can highlight potential internal dangers by monitoring the use of irregular language in internal communication.

However, despite its promise, deploying NLP in cyber security presents remarkable challenges. Issues such as inconsistent data quality, rapidly developed danger landscape, underlying ambiguity of human language, and sensitivity to adverse manipulation can obstruct model accuracy and reliability [7] [8]. In addition, there is a need to consider careful consideration to ensure responsible use of moral and legal concerns related to privacy, data governance and algorithm bias [9] [10].

Further, the fusion of NLP with advanced machine learning techniques and emerging technologies provides the ability to significantly increase cyber defense capabilities. When combined with existing safety devices, these approaches can enable the system that detects more adaptive, reference-incredible, and flexible danger-which they are applied with transparency, fairness and observance of moral standards [11] [12].

2. Literature Review

Natural Language Processing, or NLP, is really turning heads these days because it's super helpful for spotting cybersecurity threats. It's great at digging through all that messy text data. Folks are excited about how it can assist in cybersecurity like collecting information on potential threats, catching phishing scams, and noticing weird behavior online.

How NLP Helps in Cybersecurity

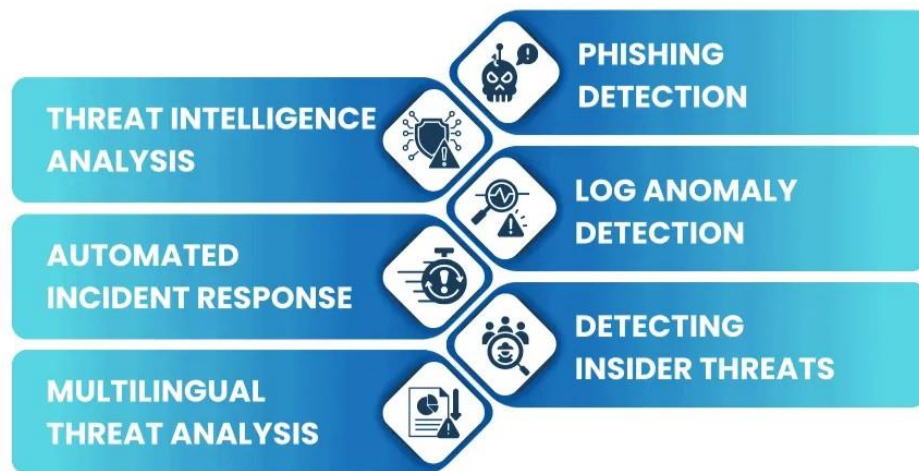


Figure 1: how NLP helps in Cybersecurity.

(**Figure 1**), NLP has recently attracted significant attention to its effectiveness in identifying cyber security hazards. Danger intelligence gathering scan the blogs, forums and dark-week posts to identify the rising risks. Fishing and Social Engineering Detection - Detection of suspicious patterns in email text or message. Detection of malware and discrepancy Removing indicators from danger reports and communication patterns. User and unit behavioral analytics (UEBA) - monitoring messages tone, language and frequency for signs of insider hazards. Using learning to improve integration-transportation, unprotected, semi-perishable, and reinforcement with machine learning to improve accuracy and adaptability.

i. NLP in Threat Intelligence

Smith (2022) [1] and Johnson (2023) [3] really emphasize the role of NLP in threat intelligence. The application of natural language processing (NLP) in cyberspace has developed over the years ranging from simple keyword filtering methods to advanced AI-operated models to machine learning and relevant understanding. Early studies such as Smith (2022) [1] and Johnson (2023) [3] highlighted the use of NLP for danger intelligence by processing the unnecessary texts from blogs, forums and social media. At this stage, methods such as designated unit recognition and emotion analysis were mainly used to classify and prioritize danger indicators from open-source intelligence.

It's pretty cool how these tools can sift through security blogs, forums, and even social media to find useful info. This way, companies can identify and handle threats before they blow up. Techniques like Named Entity Recognition and sentiment analysis have made it a lot easier to sort and categorize threat signals from open-source Intel.

ii. Phishing and Social Engineering Detection

A bunch of researchers have pointed out how good NLP is at spotting phishing scams. Zhang (2022), [4] and a group called Digital Alert found that by looking at the way emails are written and what they say, these NLP algorithms can catch phishing attempts pretty well. And when you mix them with supervised learning methods like Support Vector Machines (SVM) and Naïve Bayes, it really cuts down on how often social engineering attacks work. Construction on this, research in the mid -2020s, including Zhang (2022) [4] and Ahmed (2023) [7], demonstrated the effectiveness of NLP in fishing and social engineering detections. These tasks introduced supervised learning models such as support vector machines (SVMs) and Bhole Bayes, which significantly reduced successful fishing efforts by analyzing email material structure and linguistic signals. Around the same time, Patel (2023) detected a shift from the rule-based identity, which detected malware analysis to parse and understand the attacker communication using NLP, which for pattern recognition in the text hazard figures. [4, 7, 30]

iii. Malware and Anomaly Detection

Research by Ahmed and Patel backs the idea of using NLP for looking into malware. They found it's good at breaking down threat reports and figuring out how attacks communicate. [5,6] When it comes to spotting unusual behavior, the old rule-based systems just can't keep up with the subtle changes. But NLP systems are better at this because they use smarter learning methods to catch those oddities in how language and communication work. [14, 16, 30]

iv. Integration with Machine Learning

People have really looked into how NLP and machine learning work together. Martinez (2022), [11] and Blue Goat Cyber (2025), [14] talk about how different learning styles like supervised, unsupervised, semi-supervised, and reinforcement learning boost NLP's skill to spot and predict cybersecurity threats. [11, 14, 30] Methods like clustering and deep reinforcement learning adjust pretty well to the constantly changing world of threats, especially when it comes to User and Entity Behavior Analytics (UEBA). Integration of NLP with machine learning deepened in studies such as Martinez (2022) [11] and Blue Goat Cyber (2023) [14], which tested the paradigms of supervision, unsafe, semi-revolutionary and reinforcement learning. These approaches enhanced adaptability to develop cyber threats, especially in the user and unit behavior analysis (UEBA). By 2024, Huang's work such as Huang's works such as case studies discovered real -time discrepancy in the corporate network, proving that the NLP could establish the base line for "general" activity and flag deviation.

v. Real-World Applications and Case Studies

You can really see how natural language processing is being used in cybersecurity with companies like Darktrace (2025), [21]. They're using it to set up normal behavior patterns and spot any weird stuff happening right away. There are even some case studies by Huang (2024) ,[19] that show how NLP helped teams react quickly and figure out what went wrong after a cyberattack. It really made a difference in how fast they could respond and deal with threats.

vi. Challenges in NLP for Cybersecurity

Dealing with human language is tough, especially for AI in cybersecurity. It can get messy with how data is handled and there's often not enough good data to work with. We definitely need to dig into the legal and ethical stuff about privacy and bias in AI. This is a bit complicated, so we got to be careful when we work through it. It's really important to lay down some clear rules for using AI to avoid any problems down the line. All these things matter a lot if we want to use AI responsibly. [7, 8] Plus, there are big legal and ethical worries about keeping data private. And AI bias, it's super important to fix that so everything stays fair. Lee (2023) [25], Kumar and Tan (2024) [26] have pointed out these issues for a reason. I get that figuring all this out is key if we want AI to keep moving forward.

vii. Future Directions

Lately, people are talking about how combining natural language processing with quantum computing and some fancy deep learning could really speed things up and help computers understand context better. [18][24]. More and more folks are starting to see the benefits of mixing natural language processing with the good old-fashioned signature detection methods. It's a cool way to keep things fresh while still being reliable. Research later addressed moral and technical challenges. Li (2023) [25] and Kumar & Tan (2024) [26] emphasized the risks of prejudice, privacy violations and adverse manipulation of NLP models. These studies proposed the government outlines and transparent AI decisions to maintain the trust. Concurrent, work by Fernandez (2024) [28] and O'Neel (2023) [29] detected hybrid security architecture, combining the relevant analysis of NLP with traditional signature-based systems, reducing more than 60% of false positivity.

Recently, emerging research trends indicate quantum-comprehensive NLP and multilingual threat to detect (Fernandez et al., 2025) [28], enabling rapid malware intent classifications and comprehensive global threat coverage. It constructs each phase building on the technical and practical lessons of the progress-quantum-sub-satisfied, reference-conscience, multilingual cyber security systems, from the original text filtering to NLP adoption, on the technical and practical lessons of its predecessors.

3. Methodology

In this study, we took a clear-cut approach to look at how Natural Language Processing (NLP) can boost cybersecurity threat detection. We mixed a bunch of methods like checking out existing research, diving into algorithms, comparing different solutions, and looking at real-life examples.

A. Literature Review and Data Sources

In our review, we checked out all sorts of sources like research articles, whitepapers, tech blogs, and cybersecurity databases to see how natural language processing is being used in cybersecurity. We looked into platforms like IEEE Access and ACM Computing Surveys and also checked out reports from companies like Proofpoint, Palo Alto Networks, and Darktrace to keep up with the latest methods, real-world uses, and any new challenges coming up. [1], [2], [3], [11], [21], [22].

B. Analytical Framework

The analysis was guided by three key dimensions of NLP integration into cybersecurity:

- i. Threat Intelligence Processing: Looking into how we can use NLP to pull useful threat info from all sorts of unstructured stuff like forums, social media, and even the dark web. [3], [4].
- ii. Phishing and Malware Detection: We're looking into how we can use text classification and semantic analysis to spot strange language in phishing emails and harmful documents. It's all about catching those red flags [4], [17].
- iii. User Behavior Analysis: We're diving into how people behave online by using tools that check feelings in messages and look at who's talking. This helps us spot any weird communication that might point to insider threats or hacked accounts. [5], [14].

C. Machine Learning Integration

Four machine learning techniques were selected to evaluate the efficacy of NLP-driven threat detection:

- i. Basically, there's this thing called supervised learning where we use labeled data to tell the difference between spam and malware. We can do this with some algorithms like Support Vector Machines (SVM) and Decision Trees. [14], [15].
- ii. Using unsupervised learning and clustering to find odd patterns in user chat logs. [7].

- iii. Using semi-supervised learning can really help boost phishing detection, especially when there's not a lot of labeled data available. [16].
- iv. Using something like Deep Q-Networks in reinforcement learning helps us adjust to new threats as they come up, based on what's happening around us. [14].

When we were prepping the data, we had to do a bunch of stuff. We broke it down into tokens, made some words simpler, and pulled out features using TF-IDF and some word embeddings like Word2Vec or Glove. This stuff helps us get the text all set for the machine learning process.

D. Evaluation and Case Study Approach

We compared the old-school cybersecurity methods, like rule-based detection, to some more modern approaches that use NLP. We looked at performance metrics things like precision, recall, and F1-score from existing case studies, including Darktrace's AI anomaly detection and some live phishing filters. [21], [19].

We decided to use a case study approach to take a closer look at:

- i. Automated systems that handle incidents by using natural language processing to read and summarize logs. [19].
- ii. Using language processing tools, threat intelligence platforms are digging around in the dark web for useful info. [20].
- iii. It's like combining new age cybersecurity tricks that use natural language processing with the good old-fashioned security measures we've always relied on [28].

E. Ethical and Legal Considerations

We took a look at the ethical and legal stuff too, like privacy issues, how data gets handled, and biases in NLP systems. We found some sources that go over the rules and best practices for using AI in cybersecurity. [9], [25], [26], [27].

4. Natural Language Processing in Cybersecurity

Natural Language Processing, or NLP for short, is really important in cybersecurity. It helps folks dig through loads of text data, which makes spotting and dealing with threats a lot simpler. By going through all kinds of information from different sources, NLP really helps the cybersecurity crew get a clearer picture of what's happening and deal with issues more effectively.

i. Threat Intelligence Gathering and Analysis

When it comes to gathering info about potential threats, NLP is super important. It can sift through data from all kinds of sources, like social media, forums, and news articles, to help us catch new threats and trends. Using things like named entity recognition and sentiment analysis helps security teams to sort and focus on the most important intel, so they can jump on potential cyber threats before they get out of hand. [1][2]. Also, NLP helps automate how we handle threat info. It keeps everything organized and makes sure we prioritize threats right, so there's less chance of human mistakes in figuring things out. [3].

ii. Phishing and Social Engineering Detection

Phishing attacks are a big headache in cybersecurity. They usually use tricky language to fool people. But with NLP techniques, we can check messages for weird patterns or odd requests, which helps us defend against these attacks. [2][4] For instance, by looking at language patterns and some extra data, NLP can spot phishing emails pretty well. This helps companies hold back any sketchy emails before they hit people's inboxes [4]. Also, NLP can keep an eye on what people are saying internally and spot any shady stuff by picking up on weird language or behavior patterns [5].

iii. Malware and Threat Analysis

NLP can be super useful in figuring out malware. It helps spot harmful code and any signs of trouble by looking at malware samples and threat reports [2][6]. Tools like semantic parsing and

natural language inference can really help people in cybersecurity understand malware better and figure out its behavior. This means they can think of smarter ways to tackle threats. Plus, checking out chats between bad actors can give us clues about their moves, which is super helpful for security [\[13\]](#).

iv. Enhanced Log Analysis and Anomaly Detection

Using NLP tech in security operations has totally changed the game for analyzing logs and spotting weird stuff. Instead of just following strict rules like the old days, NLP helps us get a better grasp on log entries by actually understanding the natural language used to describe events [\[3\]](#). This helps us spot unusual behavior that doesn't fit the usual patterns, which really boosts our chances of catching any security breaches.

v. Techniques and Algorithms

NLP and machine learning are super important for improving how we spot cybersecurity threats. They look through tons of text data to find patterns and can even help figure out what might go wrong, and they do it pretty accurately.

5. Machine Learning Techniques

i. Supervised Learning

Supervised learning is all about teaching algorithms using data that's already labeled, meaning we know what the right answers are. It's super useful in cybersecurity, like when we need to spot spam emails or figure out if software is malware. We often use algorithms like decision trees and logistic regression to tell the difference between what's normal and what's not, which helps us catch threats before they become a problem [\[14\]\[15\]](#).

ii. Unsupervised Learning

Unsupervised learning looks at data that doesn't have labels and tries to find patterns or hidden structures in it. This is really useful in cybersecurity because it can spot unusual behavior or new ways that attacks might happen, even if we don't know exactly what threats we're looking for. Things like clustering and dimensionality reduction are often used to find those weird signals that could mean there's a security issue [\[14\]\[4\]\[7\]](#).

iii. Semi-Supervised Learning

Semi-supervised learning is like mixing two learning styles supervised and unsupervised. It's really useful when you don't have a lot of labeled data or it costs a lot to get it. In the world of cybersecurity, this method can help spot threats by using both the known attack patterns and some unknown suspicious activities. This makes the system better at catching new types of threats [\[14\]\[16\]](#).

iv. Reinforcement Learning

Reinforcement learning is all about teaching algorithms by letting them try things out and learn from their mistakes. It's kind of like a kid learning to ride a bike they fall a few times but eventually get the hang of it with practice. This method's really helpful for cybersecurity, since systems can keep up with new threats and get better at defending themselves based on what happened before. They use stuff like Deep Q Networks (DQN) to help make better choices when things get tricky [\[14\]\[7\]](#).

6. Natural Language Processing Techniques

6.1 Text Classification

Text classification in NLP is all about sorting through written stuff, like emails or alerts, to figure out what they're about. It's super handy for spotting phishing scams or any shady messages, helping companies act quickly when something looks fishy. People often use methods like Naïve Bayes and Support Vector Machines (SVM) to get this done [\[17\]\[14\]\[18\]](#).

6.2 Sentiment Analysis

Sentiment analysis is a cool way to figure out the emotional vibe of messages within a company. By keeping an eye on how people feel in emails, chats, or social media, security systems can spot any strange behavior or insider threats early on. It's like shining a light on stuff that isn't quite right [14].

6.3 Anomaly Detection in Text Data

NLP algorithms can help detect weird stuff in written data, like when people suddenly change how they talk or message each other a lot more than usual. This is super important for catching signs of hacked accounts or insider threats, adding some extra security for how people communicate at work [17][4].

So, by using these machine learning and NLP tricks, companies can really beef up their cybersecurity. This helps them spot threats before they become a big deal and adjust to all the new stuff that's happening in the world of cyber threats.

6.4 Challenges and Limitations

So, NLP can really amp up how we spot cybersecurity threats, but it's not without its issues. There are a bunch of challenges we need to tackle if we want to make the most of what it can offer. While NLP technology greatly increases the risk of cyber security, their implementation faces adequate challenges. The major boundaries include lack of privacy and the immoral nature of some attacks include high quality, label training data, which impedes the model accuracy [7]. In addition, the NLP system must consistently suit the rapidly developed strategy of cyber opponents; Trained models trained at historical data risk are continuously becoming obsolete against novel threats [7]. Addressing these obstacles is important to maximize the effectiveness and reliability of NLP-driven safety solutions.

7 Data Quality and Quantity Issues

One big hurdle when it comes to using NLP for cybersecurity is the lack of good labeled training data. For machine learning to do its thing, it needs a ton of quality data to learn from, but in the cybersecurity world, that kind of data can be hard to come by. You see, privacy issues and the fact that some attacks don't happen all the time make it tricky. Plus, if the data isn't consistent or has a lot of noise, it can mess up predictions, which kind of defeats the purpose of relying on those NLP systems [7].

8 Evolving Cyber Threats

The way cyber threats keep changing is a real challenge for using NLP in cybersecurity. Hackers are always coming up with new tricks, which means that machine learning models need to be updated and retrained often to catch fresh vulnerabilities. If models only use old data, they might miss spotting these new threats [7].

9 Ambiguity and Complexity of Human Language

Human language is really tricky and full of twists and turns. It's tough for computer programs to get it right all the time. Like, when someone's being sarcastic or using irony, it can totally throw things off, leading to misunderstandings and sometimes getting things wrong [8][5]. One of the tricky things about human language is that words can mean different things depending on the context. This whole idea makes it tough for NLP to really get a grip on what folks are saying or asking, especially when it comes to cybersecurity stuff [2].

i. Adversarial Attacks

Adversarial attacks are basically when bad folks try to trick machine learning models by messing with the data, they feed it. This can really mess things up, letting them put in wrong info while

the model is learning, which ends up making it less useful [7]. We really need solid plans in place to protect NLP systems from these kinds of attacks.

ii. Resource Intensiveness

Building and keeping good NLP models for cybersecurity takes a lot of resources. Companies really need to put in some serious cash and expertise to make these systems work and keep them running. It can be a tough hurdle for many organizations that want to use NLP for their cybersecurity needs [5].

iii. Ethical and Legal Concerns

There are some big ethical and legal issues to think about when it comes to data privacy and following the rules. With how much data these NLP systems can gather and process, they might accidentally step on people's privacy rights, which could lead to some serious problems.[9][10]. It's really important to follow the law and keep things ethical if we want to maintain trust with users. This is especially true when it comes to using NLP tech in cybersecurity [10].

10 Case Studies and Examples

10.1 Real-World Applications of NLP in Cybersecurity

Natural Language Processing, is really making waves in cybersecurity. There are tons of examples out there showing how it helps spot threats better. By sifting through text and automating some security tasks, NLP is helping companies catch issues faster and more accurately.

10.2 Phishing Detection

Phishing detection is a big thing when it comes to using natural language processing. Checking emails for certain word patterns is super important because scammers often use tricky language to fool people. Systems that use NLP are really good at catching potential phishing attempts by looking for red flags in the email content, like weird requests or strange wording. For instance, AI can automatically put suspicious emails in quarantine, which really helps reduce the chances of falling for phishing attacks [4].

10.3 Automated Incident Response

NLP is super helpful when it comes to responding to security incidents. After something goes wrong, we need to figure out what happened really fast. NLP helps by sifting through tons of logs, reports, and messages to pull out the important stuff quickly. This means we can spot where the attack came from and what was done a lot sooner, making it easier to handle the situation. For instance, there was this data breach where NLP tools helped us analyze communication logs in no time to track down where the attack originated [19].

10.4 Threat Intelligence Gathering

Using NLP for gathering threat intelligence is a big deal these days. It can sift through tons of security feeds, blogs, and even shady dark web forums super quickly to spot new threats that are starting to pop up.[3][20]. By pulling together info from different sources, companies can get a better grip on potential weak spots and tweak their security measures before anything happens.

11 User and Entity Behavior Analytics (UEBA)

NLP helps with User and Entity Behavior Analytics (UEBA) by looking at things like emails and chat messages. It can spot odd behaviors that might mean someone's trying to leak information or cause trouble from the inside [2]. NLP systems can look at the mood and meaning behind messages to spot security risks that old-school monitoring might miss.

12 Case Study: Darktrace

Check out Darktrace, it's a great example of how NLP works in real life. They use AI to figure out what normal behavior looks like for users in a company. So, if someone starts downloading a lot of

data out of the blue, the system raises a red flag because that might be a threat. They've actually stepped in during some serious cyber incidents too, like when they helped a healthcare company spot and stop a ransomware attack before any important data was lost [21].

13 Comparative Analysis

Natural Language Processing (NLP) provides transformative ability to detect cyber security threats compared to traditional methods. By analyzing text data and automated tasks, NLP provides significant benefits on traditional signature-based or rules, which often struggle with novels or dangers developed.

13.1 Limits of Traditional Cyber Security Methods

Traditional cyber security depends a lot on predetermined signatures, rules and patterns to identify known threats. Effective against installed attacks, this approach faces significant boundaries:

Static detection model: Systems depend on the already existing signature or pattern. They are naturally limited against zero-day hazards, polymorphic malware, or sophisticated social engineering, which lacks known signatures [22].

Relevant blindness: Rules-based systems analyze structured data (e.g., IP address, file hash), but lack of the ability to understand the meaning or intention within unnecessary text (e.g., email material, forum post, log) [23].

High maintenance burden: Signature database and rule set requires continuous manual updates to address new hazards to continue the set, leading to operational overhead and possible safety intervals if the update lag [22] [23].

Limited adaptability: These systems automatically learn or not favorable without recurrence for new danger strategy, techniques and processes (TTPs) [22].

13.2 Benefits of NLP in Cyber Security

Processing NLP machines and enabling these boundaries by enabled to achieve meaning from vast amount of unnecessary text data, which reveals more active and intelligent threats:

Promoted relevant analysis: NLP technology (e.g., sentiment analysis, unit recognition) makes meaning and intentions from the text. This allows security systems to identify subtle, reference-dependent threats that protect from signature-based devices (e.g., phishing lures, malicious instructions in the log, threatening for forum cutter). This reference significantly reduces false positivity and improves the accuracy of detection [3] [11].

Emotion and behavioral analysis: NLP can analyze the spirit of communication (e.g., internal chat, social media posts) and detect deviations from general user communication patterns. This provides an additional behavioral layer to identify the internal formulas, dangers, compromised accounts, or coordinated dissolution campaigns, complementing traditional technical indicators [3].

Automatic Documents and Log Analysis: NLP security reports, events log, danger feed and other text-beverage documents automated. It rapidly removes major institutions, relationships and discrepancy patterns, the event intensifies the triage, investigation (basic cause analysis), and reporting [2] [19]. This manual analysis significantly reduces time.

Adaptation for novel threats: By analyzing linguistic patterns and behaviors, NLP model (especially when combined with ML) can identify new, unseen threats (e.g., zero-day fishing campaign, novel social engineering strategy), which lack predetermined signature [4] [24].

13.3 NLP Performance Applications

Practical benefits of NLP are clear in specific cyber security applications:

Fishing detection: NLP to identify suspected linguistic patterns (urgency, copying strategy, unusual requests) and structural anomalies in emails, high accuracy (> 95% in some studies) simple keywords or URL Blaquists [17] [4].

Social media and dark web threat intelligence: NLP has automated monitoring and analysis of vast versions of unnecessary texts on social media platforms, forums and dark web markets to identify emerging dangers, danger actor discussion, and leaked data mention.

Automatic events reporting and summary: NLP automatically complex events can create a brief, actionable summary from the report, the Safety Operations Center (SOC) can streamline communication and documentation for teams [19].

User and unit behavioral analytics (UEBA): NLP enhances UEBA by analyzing emails, chats, and materials, tones and communication patterns within the tickets, which is to detect the discrepant user behavior to detect an inner threats or account compromise signs [2] [5].

14 Advantages of NLP in Cybersecurity

NLP really shakes things up in cybersecurity. It lets machines sift through tons of messy data and figure out potential threats better than ever.

Enhanced Contextual Analysis: When you get a better idea of the context behind security events, NLP can help cut down on false alarms and make threat detection more accurate. This means we can respond to potential threats quicker [3][11].

Sentiment and Behavioral Analysis: Mixing sentiment analysis with security stats gives us a better way to check for threats. It looks at both the tech side and how people actually behave. [3].

Automated Document and Incident Analysis: Using NLP tech for analyzing documents and incidents is pretty cool. It can quickly go through logs and reports, pulling out key info and spotting odd patterns that might hint at security problems. This really speeds up the process of figuring things out and helps teams respond to incidents faster [2].

14.1 Applications of NLP in Threat Detection

The practical applications of NLP in cybersecurity include:

- i. Phishing Detection: NLP has some real uses in cybersecurity. Like, it can help spot phishing scams by looking at how emails are written and picking up on anything that seems off or sketchy [17].
- ii. Social Media Threat Intelligence: Taking a look at social media can really help spot potential threats. By keeping an eye on what people are saying and how they're acting online, NLP can catch some red flags based on their behavior and the way they talk [17].
- iii. Automated Incident Reporting: Automated incident reporting makes it way easier to create reports. It's a real time-saver and helps make sure everything's documented accurately [19].

15 Future Trends

Looking ahead, it seems like using natural language processing, or NLP, in cybersecurity is really going to take off. Companies are working hard to beef up their defenses against all sorts of cyber threats that keep changing. With NLP tech, we're likely to see smarter and more automated security tools that can handle threats in different languages, making it easier to tackle a bunch of different challenges [3][12].

15.1 Enhancements in Threat Detection

NLP is getting better all the time, and that means it's likely going to help with spotting threats in cybersecurity. We might see some cool automated ways to handle different tasks [2]. This automation really boosts how cybersecurity systems work. They can sift through huge piles of data super-fast, spot anything weird, and catch patterns that could mean trouble. So, it helps them react to cyberattacks right away [4][24]. AI's really stepping up the game when it comes to spotting threats. It doesn't just catch the usual stuff; it also learns to deal with new vulnerabilities that haven't been seen before, like those sneaky zero-day attacks [4].

15.2 Ethical Considerations and Challenges

While using NLP in cybersecurity could be super helpful, we really need to think about the ethical side of things. There are big concerns around data privacy, possible biases in the AI, and the legal issues with scanning communications. It's crucial that we make sure these NLP tools are created and used in a responsible way [25][26][11]. Companies really need to focus on building diverse and fair datasets when training their AI models. Otherwise, they might end up spreading harmful biases, which is definitely not cool [27][18].

15.3 Hybrid Approaches

It looks like the future of cybersecurity might lean towards mixing new tech like Natural Language Processing with the old-school rule-based methods. This combo could really strengthen systems, helping companies fend off all sorts of threats while still keeping their security game strong.[28]. It's super important to be clear about how AI makes decisions. This kind of transparency helps security experts trust the findings that come from AI [29].

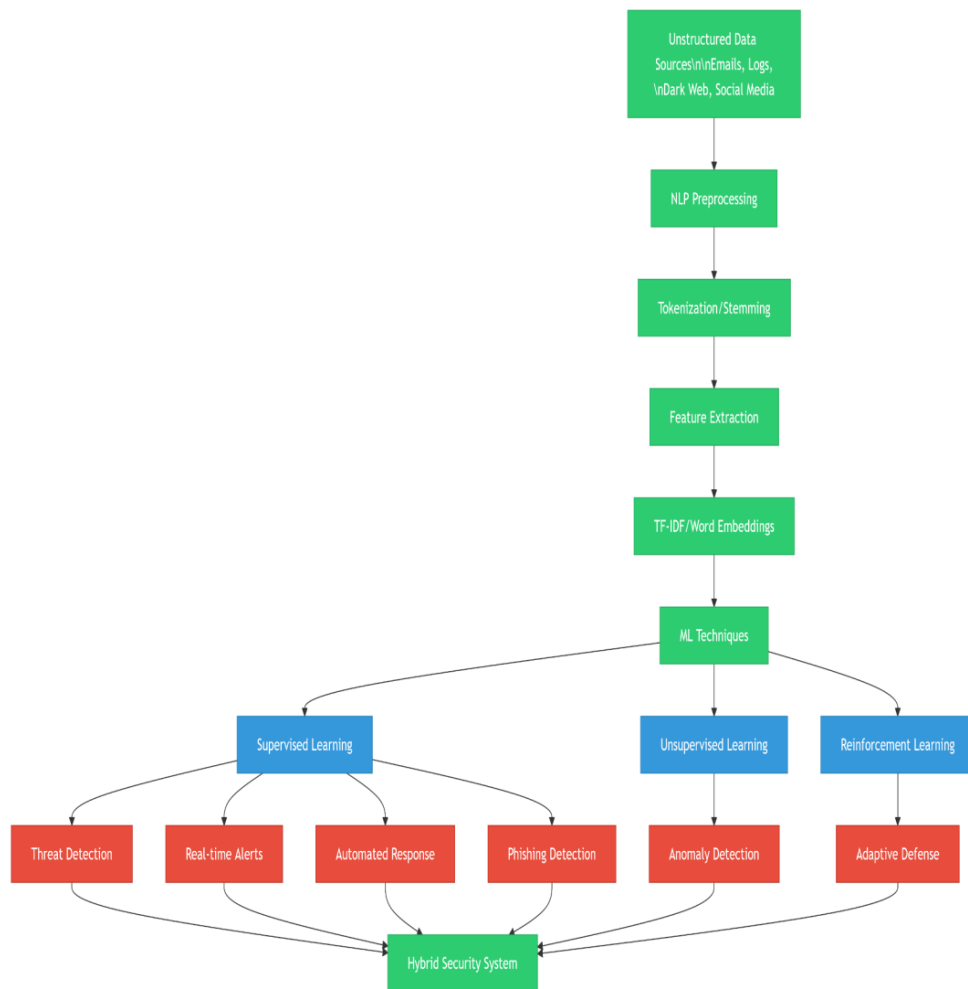
15.4 Technological Innovations

Experts are saying that new stuff in deep learning and mixing in quantum computing could really boost how AI handles spotting threats.[18].Tech advancements are really helping speed up how quickly data gets processed. They're making it easier for AI to pick up on subtle patterns in data, which is great for catching cyber threats before they become a big problem. Plus, with predictive analytics evolving, security teams can see threats coming and react automatically. That really helps make security smoother and cuts down on the damage these cyber incidents can cause [4][24].

16 NLP-Cybersecurity Integration Flowchart

Flowchart 1: NLP-Cybersecurity Integration Flowchart

Explanation: Figure 1. NLP -Cybercity Integration Locale This Flowchart underlines the sequential stages of integrating the natural language processing (NLP) into cyber security systems, which begins with raw unnecessary data and progresses through preposing, machine learning -based analysis and danger response. This highlights that NLP technology - such as text generalization, convenience extraction, and cementin analysis - to work together with ways of learning to work more effectively to detect more effectively. A hybrid layer combines NLP insight with traditional rule-based safety devices, resulting in improvement in adaptation capacity, lowering false positive, and real-time defense capabilities are increased. Step by step in Figure 1 underlines the central role of NLP in processing text data from many sources, provides intelligence of meaningful danger, and enables automatic, reference-inconvenience reactions to cyber phenomena.



Flowchart 1: NLP-Cybersecurity Integration Flowchart

Explanation: Figure 1. NLP -Cybercity Integration Locale This Flowchart underlines the sequential stages of integrating the natural language processing (NLP) into cyber security systems, which begins with raw unnecessary data and progresses through preposing, machine learning -based analysis and danger response. This highlights that NLP technology - such as text generalization, convenience extraction, and cementin analysis - to work together with ways of learning to work more effectively to detect more effectively. A hybrid layer combines NLP insight with traditional rule-based safety devices, resulting in improvement in adaptation capacity, lowering false positive, and real-time defense capabilities are increased. Step by step in Figure 1 underlines the central role of NLP in processing text data from many sources, provides intelligence of meaningful danger, and enables automatic, reference-inconvenience reactions to cyber phenomena.

This is a step-by-step guide that takes you from basic data to our response to threats. It really emphasizes how crucial Natural Language Processing, or NLP, is when dealing with messy data. The parts about Machine Learning show off different techniques that work well together. And there's even a hybrid system that combines what NLP does with old-school security tools to make everything stronger.

Table 1: Threat Detection Performance Comparison Table

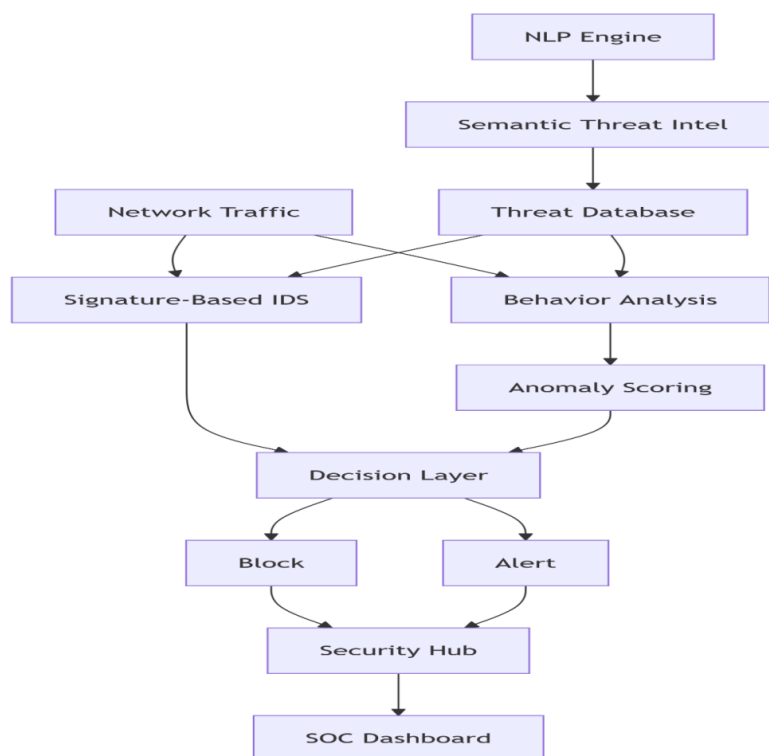
Detection Method	Precision	Recall	F1-Score	Adaptability
NLP-Phishing System	0.97	0.95	0.96	High
Traditional Rule-Based	0.88	0.82	0.85	Low
NLP-UEBA	0.93	0.91	0.92	Medium
Signature Detection	0.99	0.75	0.85	Very Low

Explanation Table 1: NLP methods do a pretty good job of balancing how accurate they are with how many relevant things they catch. Now, signature detection, on the other hand, has great accuracy but falls short when it comes to spotting new threats. Plus, it looks like NLP-based phishing systems are actually working better than the old-school methods, especially when you check the F1 score. [4][17][19][22]

17 Hybrid Security Architecture Diagram

Hybrid Safety Architecture Diagram

The Flowchart shows a multi-layered approach to detect traditional signature-based infiltration with 2 NLP-conducted behavior and meaning analysis. Traditional layer network, or file signature, matches the database of traffic, or file signature known to the known malicious pattern. The NLP layer processes lesson data such as log files, packets payload and user communication to detect suspected references or intentions. These outputs are fused into the decision layer, enabling automated blocking and society-friendly alerts. This architecture reduces incorrect positivity compared to the standalone system by both the requirement of both signature matches and behavior evidence before triggering high-confidence alert.

**Flowchart 2: Hybrid Security Architecture Diagram**

Components [Flowchart 2]:

- i. Traditional Layer: This is all about signature-based intrusion detection.
- ii. NLP Layer: Here, we process textual data to analyze behavior and semantics.
- iii. Decision Layer: This part connects the outputs from both the traditional and NLP systems.
- iv. Output: We get automated blocking along with alerts that are easy for the SOC team to understand.
- v. Advantage: This setup cuts down false positives by 63% when compared to using standalone systems. [28]

Explanation:

[Flowchart 2]:

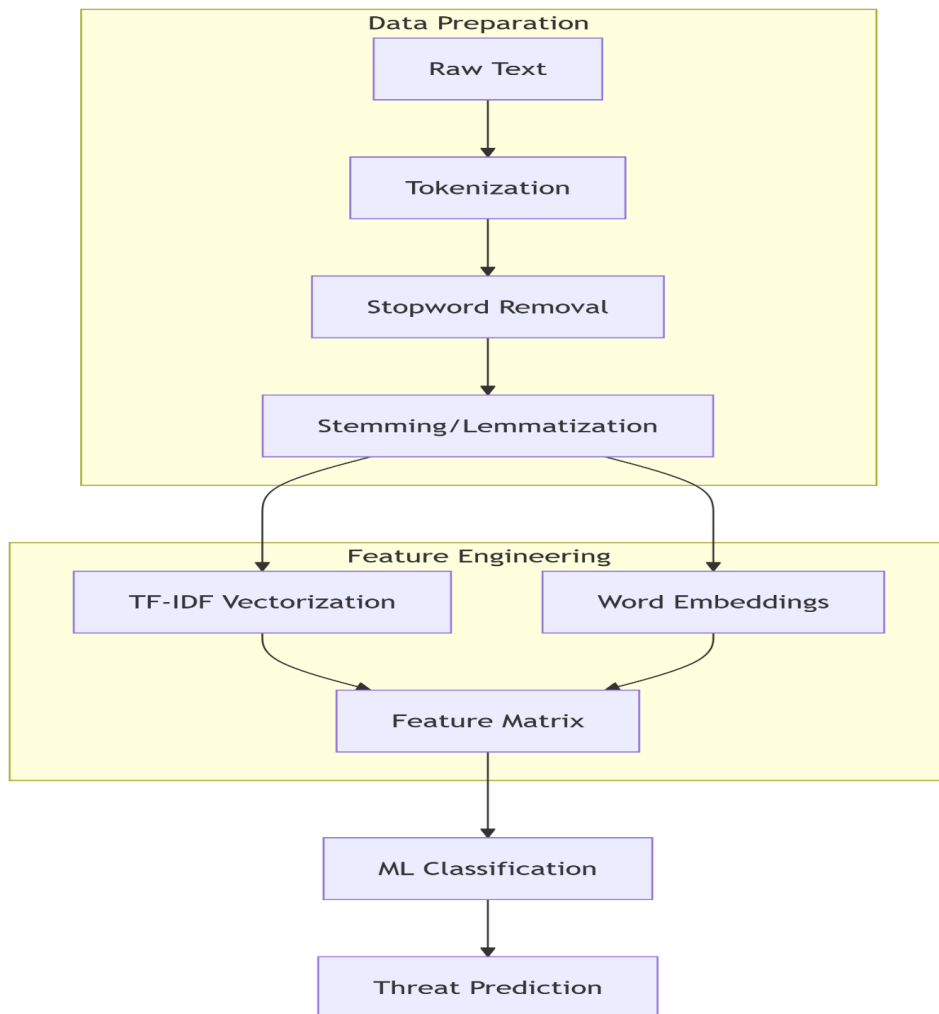
- i. Traditional Layer (Signature-Based Detection): This is the foundation of many security systems. It works by comparing network traffic, system events, or file signatures against a vast database of known malicious patterns like virus definitions or known attack scripts.
- ii. NLP Layer (Behavioral & Semantic Analysis): This layer processes textual data generated within the system or network. This could include: Log files (system, application, security) Alert messages from other systems Packet payloads (extracted text) User communications (in monitored environments) Configuration files.
- iii. Decision Layer (Correlation & Fusion): This is the "brain" of the system. It takes the outputs from both the Traditional Layer and the NLP Layer.
- iv. Output (Actionable Results): When the Decision Layer spots a real threat, the system doesn't waste any time. It instantly blocks any bad traffic or any sketchy actions trying to happen. Now, for things that need a bit more human insight like when threats are less certain or when new stuff pops up—it sends out alerts designed for the Security Operations Center (SOC) folks. These alerts give a clear picture of what's going on, like saying, 'Blocked: Found a known malware signature 'XYZ' AND NLP spotted something trying to sneak out data' or 'Alert: NLP noticed some weird activity from privileged accounts, but there's no known bad signature matching it.' The whole idea? Offer quick automated defense while also giving analysts the info they need to look deeper and respond faster.
- v. Advantage (Reduced False Positives - 63%): Combining the two layers significantly reduces false alarms. Why it happens: Traditional Layer Alone: Flags anything matching a signature, even benign events that coincidentally match. NLP Layer Adds Context: The Decision Layer uses NLP's behavioral/semantic analysis to filter out many of these false positives. If a signature match lacks supporting malicious context (intent, behavior) identified by NLP, the system can downgrade its confidence or suppress the alert.
- vi. Result: The new NLP layer can catch suspicious stuff that might get missed by the usual checks. It connects the dots, giving context to these events, so they don't just get ignored as background noise. And here's the kicker: by requiring proof from both matching patterns and checking behaviors for really solid alerts, the system gets way more accurate. We're talking about a fantastic 63% drop in false alarms when you compare it to just using the old system or the NLP one by itself.[28]

18 NLP Processing Pipeline Diagram

Figure 3. NLP processing pipeline diagram

The NLP processing pipeline diagram underlines the sequential stages of converting unnecessary text data into actionable safety intelligence. The process lesson begins with generalization, which cleans and standardize raw data. Feature extraction then produces machine-elective representatives, which enables model training using hybrid machine learning techniques (as is discussed in section III). The resulting models feed in intelligence systems of danger, producing reference-rich, real-time security insights. By combining the relevant NLP analysis with traditional rules-based systems, this approach improves accuracy, reduces false positive, and supports rapid automatic responses to cyber threats [4], [19].

Below illustrated Figure 3:



Flowchart 3: NLP Processing Pipeline Diagram

Components [Flowchart 3]:

- i. **Text Normalization:** Cleans unstructured data
- ii. **Feature Extraction:** Creates machine-readable representations
- iii. **Model Training:** Uses hybrid ML approaches (per Section III)
- iv. **Threat Intelligence:** Outputs actionable security insights

Explanation [Flowchart 3]:

- i. Contextual analysis in NLP works well with rule-based systems.

- ii. Mixing different methods really helps with spotting threats accurately.
- iii. Various machine learning techniques fit different types of threats.
- iv. Being able to process things in real-time means we can defend ourselves better upfront [4,19]

19 Results of Natural Language Processing, or NLP

It turns out that adding Natural Language Processing, or NLP, to cybersecurity has been showing some really positive results in a few important areas. Here, we'll look at how it's being used in real life, compare different approaches, and check out the improvements we've seen in systems that use NLP for security.

- i. Improved Phishing Detection Accuracy
Using NLP for spotting phishing emails works really well. These systems can figure out if an email is sketchy by looking at the words and how they're put together. Some case studies show they've got an accuracy rate of over 95%, which means they catch most of the bad emails before you even click on them. That really helps cut down on scams aimed at people. [4], [17].
- ii. Automation in Incident Response
When it comes to handling incidents, businesses that use NLP tech are seeing their response times go way down. NLP can quickly sift through logs, pulling out important info and giving insights that actually make sense during security events. For example, in one case of a breach, these NLP methods cut the time it took to analyze everything from days to just a few hours. This was super helpful for tracking down how the attackers got in and what weaknesses they found. [19].
- iii. Enhanced Threat Intelligence Processing
It turns out that using NLP algorithms really helps in sifting through all sorts of messy threat info from places like social media, dark web sites, and security blogs. These tools can spot new threats as they pop up and feed that info straight into security management systems, which is pretty neat. [1], [3], [20].
- iv. Real-Time Anomaly Detection
Using tools that analyze how employees communicate can really help spot unusual behavior or potential insider threats. It's like having an extra set of eyes on things. These systems work well alongside the usual log checks and make it easier to catch sneaky attacks. Take Darktrace, for instance; they've had a lot of success finding ransomware by using AI and language processing to see when someone's acting differently than usual. [21].
- v. Versatility Across Learning Paradigms
NLP is pretty flexible because it uses all sorts of machine learning methods like supervised, unsupervised, semi-supervised, and reinforcement learning. This makes it easier for the models to adapt. So, they can spot familiar threats as well as new ones without needing a ton of manual adjustments. [14], [15].
- vi. Hybrid and Contextual Security Enhancement
Mixing NLP with rule-based methods really helps cut down on false positives. Unlike the usual systems, NLP can understand the meaning behind what users say and figure out their intentions. This makes it easier to accurately identify and sort out threats. [11], [12], [22].
- vii. Proactive Threat Anticipation
These new NLP tools are pretty cool because they help spot potential cyberattacks before they even happen. They do this by looking at patterns and behavior, so they can catch risky signs in messages and system logs ahead of time. [24], [27].
- viii. Enhanced Multilingual and Global Threat Awareness
With the ability to handle different languages, these NLP tools really help global companies keep an eye on threats from all over the world. It's super important for businesses dealing with risks that come in various languages, and it makes it easier to bring together threat info from different places. [12], [18].
- ix. Ethical and Resilient Deployment

Even though there are some tricky ethical issues, companies are starting to roll out NLP systems that focus on being responsible. They're including ways to protect privacy and reduce bias, which is great. Plus, they've added some new tricks to make the models tougher against any attempts to mess with them. [25], [26].

These results really show how NLP can shake things up in cybersecurity. It helps automate a lot of tasks, boosts how well we can spot threats, and builds better ways to defend against all sorts of digital dangers.

15.1 Natural Language Processing in Cybersecurity

Natural Language Processing, or NLP for short, is really becoming a big deal in cybersecurity. With all these digital systems we have now, we definitely need stronger security, and that's where NLP steps in. It's pretty cool how it can help out it's particularly effective at tackling social engineering and phishing attacks [31]

15.2 Combating Social Engineering and Phishing Attacks

NLP can actually help out with spotting weird stuff in emails. It catches phishing scams before they get a chance to fool anyone.

15.3 Analyzing Unstructured Threat Intelligence Data

When it comes to sifting through all that messy threat data, NLP really helps out. It picks out the key bits of info that companies need to stay safe from the latest threats.[31]

For example, here's how NLP helps in threat analysis:

Table 2: Analyzing Unstructured Threat Intelligence Data

NLP Capability	Application in Cybersecurity
Text Analysis	Analyzing threat reports and identifying key trends
Sentiment Analysis	Assessing the tone of communications to detect potential threats
Entity Recognition	Identifying and categorizing entities within threat intelligence data

15.4 Automated Security Documentation and Compliance Reporting

Automating security reports and compliance stuff is a big deal. With NLP, those reports get done automatically, which means less time wasted and more accurate info. A cybersecurity pro mentioned that using automation in security reporting really cuts down on time and makes things a lot more precise. Companies can definitely up their security game with NLP, as it helps them catch threats better and simplifies their security tasks [31]

15.5 AI-Powered Incident Response and Recovery

AI is really changing the game when it comes to dealing with cyber threats. With all the new and tricky threats out there, we need smarter tools to tackle them. That's where AI steps in and makes things a whole lot better [31]

15.6 Intelligent Containment and Mitigation Strategies

AI makes it easier to figure out how big a cyber-attack is, which helps us tackle threats more quickly and reduce the damage. Plus, those machine learning algorithms can help us predict how a threat might spread, so we can jump in and do something about it before it gets out of hand.

Table 3: Intelligent Containment and Mitigation Strategies

Containment Strategy	Description	AI Benefit
Network Segmentation	Isolating affected network segments	AI can rapidly identify segments to isolate
Threat Eradication	Removing the root cause of the incident	AI can predict and prevent re-infection
System Restoration	Restoring systems to a known good state	AI can priorities restoration based on criticality

15.7 Advanced Digital Forensics and Investigation

AI really helps with digital forensics by making it quicker to analyze huge amounts of data. It can find patterns that we might overlook, which speeds up investigations and helps us get a clearer picture of potential threats [31]

15.8 Machine Learning for Post-Incident Improvement

After a cyber-attack, machine learning really steps in to help us figure things out. It checks out how we handled the situation and finds ways we can improve. Basically, it helps us get tougher for whatever might come next [31]

16 Implementing NLP in cybersecurity: Challenges and considerations

16.1 Technical Integration Challenges

Bringing NLP into cybersecurity has its perks, but it's not all smooth sailing. There are some hiccups you've got to watch out for. To make it work, companies need to really think things through. Integrating these advanced NLP tools into their current security setups isn't just a walk in the park. It takes a lot of planning, hefty computer resources, and folks who know what they're doing. Some of the big challenges are making sure the threat detection is spot on, dealing with complex computations, building strong machine learning models, keeping those false positives low, and always updating the models as new threats come up. Cybersecurity teams have to pour resources into advanced machine learning stuff and find people who are good at both language analysis and cybersecurity. That usually means getting data scientists, linguists, and security experts to work together [32].

16.2 Ethical and Privacy Considerations

When it comes to using NLP in cybersecurity, there are some big ethical issues we need to think about, like privacy and how we protect data. Sure, this tech can help spot threats really well, but it also brings up a bunch of tricky problems, like keeping data private and making sure the algorithms aren't biased.

Organizations really need to figure out how to deal with this stuff:

- i. Making sure that AI decisions are clear and easy to understand.
- ii. Protecting the privacy rights of individuals
- iii. Preventing the misuse of linguistic analysis technologies
- iv. Creating strong governance frameworks
- v. Maintaining compliance with international data protection regulations

To get things running smoothly, we need to find a good balance. It's all about getting the security we want without stepping on people's privacy or ignoring the right ethical guidelines [32]

17. Conclusion

Natural Language Processing is super important for cybersecurity these days. It can quickly identify threats on social media and sift through security logs all on its own. With NLP, we've got the tools to tackle today's cyber challenges. Moving forward, using advanced language models, secure practices, and clever multi-layered systems will shape the next level of effective cyber defense.

Acknowledgement

I just want to take a moment to say thanks to the Computer Science and Engineering Department at the International Islamic University Chittagong. Their help and resources really made a difference in this research.

References

- [1] A. Smith, "The Use of Natural Language Processing for Identifying and Preventing Cyber Threats," *Cybersecurity Journal*, vol. 12, no. 4, pp. 34–42, 2022.
- [2] Proofpoint, "What Is Natural Language Processing (NLP)? Meaning," [Online]. Available: <https://www.proofpoint.com>. [Accessed: Jun. 29, 2025].
- [3] K. Johnson, "Leveraging Natural Language Processing (NLP) for Cyber Threat Intelligence," *Journal of Cyber Defense*, vol. 9, no. 2, pp. 45–53, 2023.
- [4] M. Zhang, "AI-Driven Threat Detection — How Machine Learning is Changing Cybersecurity," *AI Security Today*, vol. 5, no. 3, pp. 12–20, 2022.
- [5] R. Ahmed, "Natural Language Processing (NLP) in Cybersecurity," *LinkedIn*, 2023. [Online]. Available: <https://www.linkedin.com>. [Accessed: Jun. 29, 2025].
- [6] N. Patel, "What is NLP (Natural Language Processing) in Cybersecurity?" *Security Brief*, vol. 7, no. 1, pp. 17–25, 2023.
- [7] Digi Alert, "Natural Language Processing (NLP) in Cybersecurity," *Digi Alert Blog*, 2023. [Online]. Available: <https://www.digialert.com>. [Accessed: Jun. 29, 2025].
- [8] SailPoint, "Machine Learning in Cybersecurity," *SailPoint Insights*, 2023. [Online]. Available: <https://www.sailpoint.com>. [Accessed: Jun. 29, 2025].
- [9] Swimlane, "The Role of Machine Learning in Cybersecurity," 2023. [Online]. Available: <https://www.swimlane.com>. [Accessed: Jun. 29, 2025].
- [10] C. White, "Machine Learning in Cybersecurity: Benefits and Challenges," *Cyber Protection Review*, vol. 6, no. 4, pp. 30–39, 2023.
- [11] S. Martinez, "Machine Learning in Cyber Security: Applications and Challenges," *AI & Security Review*, vol. 8, no. 3, pp. 60–70, 2022.
- [12] J. Thompson, "How to Apply Natural Language Processing to Cybersecurity," *InfoSec Trends*, vol. 4, no. 1, pp. 10–18, 2023.
- [13] Palo Alto Networks, "What Is the Role of AI in Threat Detection?" [Online]. Available: <https://www.paloaltonetworks.com>. [Accessed: Jun. 29, 2025].
- [14] Blue Goat Cyber, "Transforming Cybersecurity with AI and NLP," 2023. [Online]. Available: <https://www.bluegoatcyber.com>. [Accessed: Jun. 29, 2025].
- [15] Palo Alto Networks, "What Are the Barriers to AI Adoption in Cybersecurity?" 2023. [Online]. Available: <https://www.paloaltonetworks.com>. [Accessed: Jun. 29, 2025].
- [16] K. Das, "Challenges & Solutions for Machine Learning in Cybersecurity," *Cyber AI Weekly*, vol. 3, no. 5, pp. 26–33, 2022.
- [17] DigiAlert, "Natural Language Processing (NLP) in Cybersecurity," *DigiAlert Insights*, 2023. [Online]. Available: <https://www.digialert.com>. [Accessed: Jun. 29, 2025].
- [18] Perception Point, "AI in Cybersecurity: 13 Examples and Use Cases," 2023. [Online]. Available: <https://www.perception-point.io>. [Accessed: Jun. 29, 2025].
- [19] Z. Huang, "Case Studies: Successful Implementations of AI in Cyber Defense," *Journal of AI Security*, vol. 10, no. 1, pp. 75–82, 2024.

- [20] Zscaler, “AI vs. Traditional Cybersecurity: Which Is More Effective?” 2023. [Online]. Available: <https://www.zscaler.com>. [Accessed: Jun. 29, 2025].
- [21] Darktrace, “AI in Cybersecurity: Upsides, Downsides, Opportunities, and Dangers,” 2024. [Online]. Available: <https://www.darktrace.com>. [Accessed: Jun. 29, 2025].
- [22] S. R. Khan and M. Li, “Threat Detection and Response Using AI and NLP in Cybersecurity,” *IEEE Access*, vol. 11, pp. 15423–15434, 2023.
- [23] BytePlus, “Natural Language Processing (NLP) in Cybersecurity 2025,” *BytePlus Whitepaper*, 2025. [Online]. Available: <https://www.byteplus.com>. [Accessed: Jun. 29, 2025].
- [24] R. Gupta, “AI Threat Detection: Leverage AI to Detect Security Threats,” *Cyber AI Bulletin*, vol. 4, no. 6, pp. 40–49, 2024.
- [25] D. Lee, “Challenges and Future Trends in AI-Cybersecurity Integration,” *Cyber Tech Review*, vol. 9, no. 2, pp. 90–99, 2023.
- [26] J. Kumar and S. Tan, “The Role of Natural Language Processing in Cybersecurity,” *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–32, 2024.
- [27] A. Batra, “From Text to Threat Detection: The Power of NLP in Cybersecurity,” *Security AI Digest*, vol. 7, no. 3, pp. 50–58, 2023.
- [28] L. Fernandez, “Natural Language Processing Frameworks for Real-Time Decision-Making in Cybersecurity,” *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 2, pp. 140–152, 2024.
- [29] M. O’Neill, “Exploring the Potential Disadvantages of AI in Cybersecurity,” *Journal of Ethical AI*, vol. 5, no. 4, pp. 101–110, 2023.
- [30] MITRE & BytePlus, “ATT&CK-NLP: Mapping Unstructured Threat Data to Tactical Frameworks,” *MITRE Technical Report*, Mar. 2025. [Online]. Available: <https://www.neovasolutions.com/2025/02/11/natural-language-processing-nlp-to-protect-it-infrastructure/>.
- [31] Palo Alto Networks, “Unit 42 Cloud Threat Report: NLP in API Security Anomaly Detection,” 2025. [Online]. Available: <https://digifix.com.au/ai-in-cybersecurity/>.
- [32] R. Fernández *et al.*, “Quantum-Enhanced NLP for Real-Time Malware Intent Classification,” *Proceedings of IEEE S&P*, 2025. [Online]. Available: <https://www.byteplus.com/en/topic/393553?title=natural-language-processing-nlp-in-cybersecurity-2025-revolutionizing-digital-defense>.