Assignment of Cryptography and Network Security



Course Title: Cryptography and Network Security
Course Code: CCE-421

Submitted To:

Golam Md. Muradul Bashir
Professor
Department of Computer and Communication Engineering
Faculty of Computer Science and Engineering

Submitted By:

Farzana Afrin Hafsa	Id 1902006
Serajum Munira	Id 2002001
Sumayea Rahman	Id 2002054
Nishita Bristy	Id 2002071
Sunjida Khaton	Id 2002074
Adida Khan Tui	Id 2002076

Faculty of Computer Science and Engineering

Patuakhali Science & Technology University
Dumki, Patuakhali

Question 1:

What is Quantum Key Distribution (QKD), and how does it differ from Post-Quantum Cryptography (PQC) in how it secures a connection? (4 Marks)

Answer: QKD is a hardware-based method that establishes a shared secret key using the laws of quantum physics (the behavior of photons/light particles) over a dedicated channel. Any attempt by an eavesdropper to observe the quantum state of the photons will cause detectable interference. This differs from PQC, which is a software-based approach. PQC relies on complex mathematical problems (like lattice-based cryptography) that are assumed to be difficult for quantum computers to solve. While PQC works on standard internet infrastructure, QKD often requires specialized quantum hardware.

Question 2:

In a standard TLS 1.3 protocol, what are the primary goals of the "Handshake" phase before application data is sent? (3 Marks)

Answer: The primary goals of the TLS 1.3 handshake are:

1. Negotiation: The client and server agree on supported cryptographic versions and ciphersuites to ensure compatibility.
2. Authentication: The parties verify each other's identities using digital certificates and signatures to prevent Man-in-the-Middle (MitM) attacks.
3. Key Exchange: Both parties perform a key exchange to establish a shared "handshake secret," which is then used to derive the symmetric keys that will encrypt all subsequent application data.

Question 3:

How does predictive analytics improve cloud service reliability? (5 Marks)

Answer :

- Uses historical data collection.
- Trains machine learning model.
- Predicts reliability in real time.
- Formula:
  R_predicted = ML_Model(Predict(data_real-time))

- Proactive measures taken if reliability falls below threshold.
- Reduces downtime.

Question 4: (3 Marks)

Explain how Deep Learning models can be used for malware detection and network anomaly identification.

Answer:

Deep Learning models are widely used in network security for detecting malware and abnormal network behavior.

For malware detection, Convolutional Neural Networks (CNN) can analyze binary or structured input data and automatically extract important features. CNN effectively classifies files as malicious or benign based on learned patterns.

For network anomaly detection, Long Short-Term Memory (LSTM) networks are used. Since network traffic data is sequential in nature, LSTM can capture temporal dependencies and identify deviations from normal behavior.

These deep learning techniques improve detection accuracy and reduce false alarms compared to traditional rule-based systems.

Question 5:(3 Marks)

Discuss the advantages of using AI-based approaches over traditional security systems in network protection.

Answer:

AI-based approaches provide several advantages over traditional rule-based security systems. Traditional systems rely on predefined signatures and static rules, which are ineffective against new and evolving threats. In contrast, AI-based systems learn from data and can detect unknown or zero-day attacks by identifying abnormal patterns.

AI techniques improve detection accuracy and significantly reduce false positive rates. Additionally, AI-based systems can adapt to changing attack behaviors through continuous learning. This adaptability and intelligence make AI-based security solutions more effective for modern network environments.

Question 6:

How can CNN and LSTM be used together in intrusion detection systems? 3

Answer:

- CNN extracts spatial features and local patterns from network traffic data.
- LSTM analyzes temporal dependencies and time-based sequences in the traffic flow.
- Combining both helps the model detect complex cyberattacks more accurately and effectively

Question 7:

What are the main steps usually done to prepare network traffic data before training a deep learning model for intrusion detection? 3

Answer:

- Remove useless columns → like timestamp or some flags that don't help find attacks.
- Clean the data → fill missing values (NaN) with 0 and fix or remove strange/infinite numbers.
- Make numbers ready for the model → scale all numbers between 0 and 1 (normalization), and change attack names/labels into numbers or one-hot format so the deep learning model can understand them easily.

Question 8: (4 Marks)

Explain the impact of AI-driven automated incident response systems on cybersecurity performance with statistical evidence.

Answer:

AI-driven automated incident response systems significantly improve cybersecurity performance by reducing detection time, response time, and error rates.

• Average incident detection time reduced from 350 seconds to 120 seconds.

• Incident response time decreased from 45 minutes to 10 minutes.

• False positives reduced from 500 to 150 per month.

• False negatives reduced from 200 to 60 per month.

• Successful mitigation rate increased from 75% to 95%.

These improvements demonstrate that AI enhances speed, accuracy, and overall network resilience, making cybersecurity systems more proactive and efficient.

Question 9: (3 Marks)

Compare traditional rule-based systems with AI-based models for cyber threat detection.

Answer:

Traditional rule-based systems have lower accuracy and higher error rates compared to AI-based models.

• Traditional system detection accuracy: 78%.

• Machine Learning model accuracy: 89%.

• Deep Learning model accuracy: 96%.

AI-based systems, especially deep learning models, provide better threat detection, fewer false alarms, and improved overall cybersecurity performance.

Question 10:

What specific feature engineering techniques were employed to prepare the NSL-KDD dataset for model training?

Answer:

To improve the efficiency and performance of the intrusion detection models, the researchers applied several key feature engineering methods to the NSL-KDD dataset:

- One-Hot Encoding: Used to convert categorical variables into binary (0 or 1) vectors that models can process.
- Feature Scaling: Involved standardizing or using min-max scaling on numerical attributes to ensure algorithm efficiency.
- Dimensionality Reduction: Utilized Principal Component Analysis (PCA) to reduce the number of features in the dataset while retaining the most critical information.
- Handling Imbalanced Data: Employed techniques such as oversampling, under sampling, or synthetic data production to address class imbalances within the network traffic data.