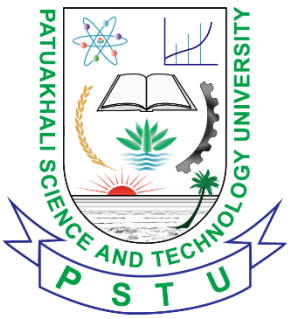
PATUAKHALI SCIENCE AND TECHNOLOGY UNIVERSITY



Assignment

Course Code: CCE-421

Course Title: Cryptography and Network Security

Submitted to:

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

Submitted by:

Date of Submission: March 03, 2026

Paper 1: Detection And Prevention of Malicious Activities in Vulnerable Network Security Using Deep Learning

Q1: Why are traditional rule-based security systems struggling against modern cyber threats, and how does Deep Learning solve this? [5 Marks]

Answer: Traditional security systems use signature-based detection, meaning they only recognize exact matches of already known threats. They often fail because hackers constantly invent new, complex attacks.

Deep learning solves this problem by learning the complex behavior patterns of network traffic, rather than just memorizing a fixed list of old threats. This allows the system to detect both known and completely new attacks accurately.

Real-life Example: Traditional security spots specific "masks," while deep learning detects suspicious behavior.

Q2: Convolutional Neural Networks (CNNs) are famous for recognizing images. How can they be used to detect malicious activities in network traffic? [5 Marks]

Answer: CNNs are incredibly good at finding patterns in structured grid data. In network security, raw network traffic data can be organized into a format that looks structurally similar to an image for the computer.

The CNN uses its layers to scan this structured data and extract hidden hierarchical features, easily spotting tiny abnormalities that indicate malware or a hack.

Real-life Example: A doctor (CNN) scans the entire X-ray to find hidden fractures (malware) that others would miss.

Paper 2: Identification Management for Zero Trust through Network Analysis

Q3: How does Zero Trust Architecture (ZTA) differ from traditional perimeter-based security in a smart factory environment? [5 Marks]

Answer: The main difference is how they handle trust.

- **Traditional Security:** Once a device passes the main firewall, it is fully trusted inside the network.
- **Zero Trust Architecture (ZTA):** The rule is strictly "Never Trust, Always Verify". It constantly checks every device, even if it is already inside the network.

Real-life Example: Traditional security is like checking a ticket at the cinema's main entrance. ZTA is like checking your ticket again at every single seat before you sit down.

Q4: Why is it practically difficult to install modern cybersecurity software (like antivirus) directly onto legacy Operational Technology (OT) machines? [4 Marks]

Answer: Installing modern security software on old factory machines is difficult for two reasons:

- **Low Hardware Power:** Old machines lack the RAM and CPU needed to run heavy software like an antivirus.
- **No Downtime Allowed:** Factory machines run 24/7. Restarting them for updates is highly risky and stops production.

Real-life Example: It is like trying to play a heavy 3D game on a 20-year-old button phone. The phone simply doesn't have the processor for it and will crash.

Paper 3: Enhancing IoT Intrusion Detection with Federated Learning-Based CNN-GRU and LSTM-GRU Ensembles

Q5: Why do modern security systems combine Convolutional Neural Networks (CNN) with Recurrent Networks like GRU or LSTM to detect network intrusions? [4 Marks]

Answer: A single neural network often misses complex attacks. Combining them (Ensemble Learning) provides total network visibility:

- **CNN (Spatial Features):** Scans individual data packets like a picture to find hidden structural abnormalities instantly.
- **GRU/LSTM (Temporal Features):** Analyzes the sequence of packets over time to spot suspicious rhythms.

Real-life Example: To secure a bank, CNN checks the photo ID (instant scan), while GRU watches the CCTV footage (behavior over time).

Q6: Why are Machine Learning-based Intrusion Detection Systems (IDS) necessary for protecting weak IoT devices against "Zero-day" (unknown) attacks? [4 Marks]

Answer: Most IoT devices have very weak default security. Traditional IDS only looks for known virus signatures, meaning they completely fail against brand-new, unseen attacks (Zero-day attacks).

Machine Learning-based IDS learns what "normal, healthy" network traffic looks like. If any traffic behaves abnormally, it blocks it, even if the attack is completely new.

Real-life Example: A traditional lock only stops people with the wrong key. ML is like a guard dog that barks at *any* suspicious behavior, even from unknown strangers.

Paper 4: Improving Network Security Using Intelligent Ensemble Techniques: An Integrated System for Detecting and Managing Intrusions in Computer Networks

Q7: What is an "Intelligent Ensemble-Based" security system, and why is it better than a single detection method? [5 Marks]

Answer: An intelligent ensemble-based system combines multiple different security algorithms to work together as a team. Instead of relying on a single method that might miss complex threats, the ensemble leverages the unique strengths of each algorithm.

- **Higher Accuracy:** By analyzing network traffic from multiple different perspectives, the system makes highly educated and accurate decisions.
- **Fewer False Alarms:** By combining and balancing data from several sources, it successfully reduces false positives (unnecessary alerts) and false negatives (missed attacks).

Real-life Example: Like a medical board of different specialists diagnosing better than a single doctor.

Q8: When analyzing network traffic, why is it helpful to categorize data features into "Intrinsic", "Traffic", and "Content" groups? [5 Marks]

Answer: Network connections contain a massive amount of complex data. Breaking this data down into specific categories helps the AI model understand every different aspect of the connection:

- **Intrinsic Features:** Describe the basic, fundamental characteristics of the connection itself.
- **Traffic Features:** Look at the flow, speed, and volume of the data over time.
- **Content Features:** Examine the actual specific details hidden inside the transferred data.

By combining all these features, the model can detect both known and unknown attacks with very high accuracy.

Real-life Example: Like airport security checking a bag's weight, speed, and X-ray scan together.

Paper 5: Real-Time DDoS Detection in Software-Defined Networks Using Machine Learning

Q9: Why does the centralized "brain" of a Software-Defined Network (SDN) make it particularly vulnerable to DDoS attacks? [5 Marks]

Answer: SDNs separate the network's "brain" (control plane) from its "body" (data plane), centralizing all decision-making into a single controller.

While this makes network management highly efficient and flexible, it creates a single point of failure. A Distributed Denial of Service (DDoS) attack can easily overwhelm this single controller with massive amounts of fake traffic, bringing down the entire network instantly.

Real-life Example: Like a restaurant where one single manager approves every order; if 100 fake customers shout at once, the manager freezes and nobody eats.

Q10: How does Machine Learning improve the real-time detection of DDoS attacks compared to traditional rule-based methods? [4 Marks]

Answer: Traditional security methods rely on fixed rules or known virus signatures, which struggle to keep up with the massive, fast-changing floods of modern DDoS attacks.

Machine learning models, however, analyze real-time traffic patterns (like packet speed and volume). They continuously adapt and can instantly spot abnormal floods of data, even if the hacker's attack technique is completely new or disguised.

Real-life Example: Like a smart security guard who flags a sudden, unnatural crowd rushing a door, rather than just checking if they have the right ID cards.