CS 6500 Network Security

Jan-May 2025 – Course Project

Version 1 – 5th March 2025

The Goal of this project are as follows:

a) Gain deeper network security related knowledge in one of the applicable domains
b) Review 4-6 survey papers/literature papers, identify a suitable implementable problem statement in one of the "Current Research Areas" given in Section 1. The survey study result and identified problem statement will be first stage report generated with a short presentation.
c) Implement a solution to the identified problem statement, perform analysis and prepare a detailed report. Report must capture the methodology / approach taken to solve the problem, justify why the method chosen was identified as appropriate, and showcase with analysis the derived results.
d) Final report to be shared in typical IEEE conference paper format - https://www.ieee.org/conferences/publishing/templates.html

1. Current Research Areas

1. **AI-Driven Security Solutions**
    - **Focus**: Using artificial intelligence and machine learning to detect and respond to cyber threats in real-time.
    - **Literature**: "AI in Cybersecurity: Threat Detection and Response"1.
2. **Zero Trust Architecture**
    - **Focus**: Implementing a security model that requires continuous verification of every user and device.
    - **Literature**: "Zero Trust Networks: Building Secure Systems in Untrusted Networks"2.
3. **Blockchain Security**
    - **Focus**: Leveraging blockchain technology to enhance security in various applications, including secure communication and data integrity.
    - **Literature**: "Blockchain-Based Security Solutions: A Survey"3.
4. **Post-Quantum Cryptography**
    - **Focus**: Developing cryptographic algorithms that are secure against quantum computing attacks.

- **Literature**: "Post-Quantum Cryptography: Current State and Future Directions"4.

5. **IoT Security**
    - **Focus**: Addressing security challenges in the Internet of Things (IoT) devices and networks.
    - **Literature**: "Security Protocols for Internet of Things: A Survey"5.
6. **Ransomware Detection and Mitigation**
    - **Focus**: Developing techniques to detect and mitigate ransomware attacks.
    - **Literature**: "Ransomware: Detection, Prevention, and Mitigation"6.
7. **Secure Cloud Computing**
    - **Focus**: Enhancing security in cloud environments, including data protection and secure access control.
    - **Literature**: "Cloud Security: A Comprehensive Guide to Secure Cloud Computing".
8. **Privacy-Preserving Data Sharing**
    - **Focus**: Developing methods to share data securely while preserving privacy.
    - **Literature**: "Privacy-Preserving Data Sharing: Techniques and Applications".
9. **Cyber-Physical System Security**
    - **Focus**: Securing systems that integrate physical processes with computation and networking.
    - **Literature**: "Cyber-Physical System Security: A Survey".
10. **Network Traffic Analysis**
    - **Focus**: Analysing network traffic to detect anomalies and potential threats.
    - **Literature**: "Network Traffic Analysis: Techniques and Tools".

Relevant Literature for Further Study

1. "AI in Cybersecurity: Threat Detection and Response"1
2. "Zero Trust Networks: Building Secure Systems in Untrusted Networks"2
3. "Blockchain-Based Security Solutions: A Survey"3
4. "Post-Quantum Cryptography: Current State and Future Directions"4
5. "Security Protocols for Internet of Things: A Survey"5
6. "Ransomware: Detection, Prevention, and Mitigation"6
7. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing"

8. "Privacy-Preserving Data Sharing: Techniques and Applications"
9. "Cyber-Physical System Security: A Survey"
10. "Network Traffic Analysis: Techniques and Tools"

Examples of possible survey papers/literature in some of the research areas:

2. "AI-Driven Security Solutions"

1. **AI-Driven Network Intrusion Detection Systems: A Comprehensive Survey**
    - **Summary**: This paper surveys various AI-driven techniques for network intrusion detection systems (NIDS). It covers machine learning, deep learning, and hybrid approaches, highlighting their effectiveness in detecting and mitigating network intrusions.
    - **Link**: Read the paper1.
2. **Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions**
    - **Summary**: This paper explores the role of AI and machine learning in enhancing cybersecurity defences against sophisticated cyber threats. It addresses challenges such as data privacy, continuous training of AI models, manipulation risks, and ethical concerns.
    - **Link**: Read the paper2.
3. **Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques**
    - **Summary**: This paper reviews AI-driven detection techniques, including machine learning and deep learning, for identifying and responding to cyber threats. It examines over sixty recent studies to measure the effectiveness of these AI tools in detecting various cyberattacks such as malware, network intrusions, and spam.
    - **Link**: Read the paper3.
4. **Artificial Intelligence for System Security Assurance: A Systematic Literature Review**
    - **Summary**: This systematic literature review assesses the current state of AI in system security assurance (SSA), identifying key areas where AI contributes to improving SSA processes, highlighting the limitations of current methodologies, and providing guidance for future advancements.
    - **Link**: Read the paper.
5. AI-Driven Anomaly Detection in Network Traffic: Techniques and Applications

- Summary: This paper explores various AI-driven techniques for anomaly detection in network traffic. It discusses the application of machine learning and deep learning models to identify unusual patterns and potential threats in network data.
- **Link: Read the paper**

6. **Machine Learning Approaches to Ransomware Detection: A Comprehensive Review**
    - **Summary**: This paper provides a comprehensive review of ransomware detection methods, with a focus on machine learning-driven approaches. It discusses various techniques and their effectiveness in identifying ransomware attacks.
    - **Link**: https://iieta.org/journals/ijsse/paper/10.18280/ijsse.140630

3. Zero Trust Architecture

1. **ZT-SDN: An ML-powered Zero-Trust Architecture for Software-Defined Networks**
    - **Summary**: This paper proposes ZT-SDN, an automated framework for learning and enforcing network access control in Software-Defined Networks (SDNs). It uses machine learning to extract transaction patterns from network data and generate access control rules, enhancing security by detecting abnormal network accesses and abuses.
    - **Link**: Read the paper1.
2. **Modelling and Analysing Zero Trust Architectures Regarding Performance and Security**
    - **Summary**: This paper introduces a novel ZTA metamodel based on literature and industry applications. It provides a model instance using the Palladio Component Model (PCM) to simulate performance impact and analyse the correct implementation of zero trust principles at the architectural level.
    - **Link**: Read the paper2.
3. **TrustZero - Open, Verifiable, and Scalable Zero-Trust**
    - **Summary**: This paper presents a passport-level trust token for Europe, addressing the need for a paradigm shift in security models due to escalating cyber threats. It emphasizes the importance of open, verifiable, and scalable zero-trust solutions to counter advanced attacks.
    - **Link**: Read the paper3.
4. **Zero Trust Architecture for Cloud Environments: Challenges and Solutions**
    - **Summary**: This paper explores the implementation of Zero Trust Architecture in cloud environments, discussing the unique challenges and proposing solutions to enhance security in cloud-based systems.
    - **Link**: Read the paper.
5. **Zero Trust Network Access: A Comprehensive Survey**

- **Summary**: This survey paper reviews various approaches to Zero Trust Network Access (ZTNA), highlighting the benefits and limitations of different methods and providing a comprehensive overview of the current state of ZTNA.
- **Link**: Read the paper.

6. **Implementing Zero Trust in Industrial Control Systems**
    - **Summary**: This paper discusses the application of Zero Trust principles in industrial control systems (ICS), addressing the specific security challenges and proposing a framework for implementing Zero Trust in ICS environments.
    - **Link**: Read the paper.

4. Ransomware detection and mitigation applied w.r.to network security

1. **RansomGuard: A Framework for Proactive Detection and Mitigation of Cryptographic Windows Ransomware**
    - **Summary**: This paper proposes RansomGuard, a framework that utilizes both static and dynamic machine learning components to detect and mitigate ransomware attacks. It analyses events captured from the Windows kernel using Event Tracing for Windows (ETW) logs to identify malicious activities. The framework achieved up to 99.87% accuracy in detecting ransomware.
    - **Link**: Read the paper1.
2. **Machine Learning Approaches to Ransomware Detection: A Comprehensive Review**
    - **Summary**: This paper provides a comprehensive review of ransomware detection methods, with a focus on machine learning-driven approaches. It discusses various techniques and their effectiveness in identifying ransomware attacks.
    - **Link**: Read the paper2.
3. **Ransomware Detection using Machine Learning with eBPF for Linux**
    - **Summary**: This paper explores the use of extended Berkeley Packet Filter (eBPF) and machine learning to detect ransomware on Linux systems. It highlights the effectiveness of combining eBPF's low-level monitoring capabilities with machine learning for real-time ransomware detection.
    - **Link**: Read the paper3.

5. IoT Security and network challenges for IoT

1. **Internet of Things (IoT) Applications Security Trends and Challenges**
    - **Summary**: This paper analyses the current architecture of the Internet of Things, focusing on the risks and vulnerabilities associated with IoT-enabled devices. It discusses effective real-time IoT applications, highlights the latest improvements in IoT security, and outlines outstanding problems for future research.

- **Link**: Read the paper1.

2. **Internet of Things Technology, Research, and Challenges: A Survey**

    - **Summary**: This survey paper reviews recent and past technologies used for IoT optimization models, such as IoT with Blockchain, IoT with WSN, IoT with ML, and IoT with big data analysis. It discusses security, interoperability, standards, scalability, complexity, data management, and quality of service (QoS) in IoT.

    - **Link**: Read the paper2.

3. **Current Challenges in IoT Security and Forensics**

    - **Summary**: This paper addresses the expanding vulnerabilities in IoT technology, ranging from the exploitation of individual devices to large-scale breaches of network security. It highlights the challenges in securing IoT devices and networks and discusses potential forensic approaches.

    - **Link**: Read the paper3.

6. secure cloud computing and network security

1. **Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies**

    - **Summary**: This paper provides a comprehensive review of cloud computing security, focusing on threats such as DDoS attacks, account hijacking, malware attacks, and data breaches. It also explores mitigation strategies, including security awareness training, vulnerability management, SIEM, IAM, and encryption techniques. The paper discusses emerging trends like AI and ML integration, serverless computing, and containerization.

    - **Link**: Read the paper1.

2. **Cloud Computing Security: Threats and Mitigation Strategies**

    - **Summary**: This paper highlights common threats related to cloud computing security and explores various mitigation strategies. It emphasizes the importance of user awareness and the impact of emerging technologies on cloud security.

    - **Link**: Read the paper2.

3. **Cloud Security: A Comprehensive Guide to Secure Cloud Computing**

    - **Summary**: This paper provides an extensive review of security and privacy issues in cloud computing. It discusses different security approaches proposed in the literature to tackle present security flaws.

    - **Link**: Read the paper3.

7. post quantum cryptography as applied to networks

1. **Migrating Software Systems towards Post-Quantum-Cryptography -- A Systematic Literature Review**
    - **Summary**: This paper provides a systematic literature review on migrating software systems towards post-quantum cryptography. It addresses the challenges and approaches for migrating IP networks to PQC, highlighting the need for standardized terminology, migration steps, and roles. The review also discusses real-world implementations and the major challenges faced by adopters.
    - **Link**: Read the paper1.
2. **Post-Quantum Cryptography and Quantum Key Distribution: An In-Depth Survey of Techniques, Comparative Study, and Future Trends**
    - **Summary**: This paper surveys post-quantum cryptography (PQC) and quantum key distribution (QKD) techniques. It provides a comparative analysis of their strengths, weaknesses, and deployment scenarios, and explores current challenges and future directions in the field.
    - **Link**: Read the paper2.
3. **Post-Quantum Cryptography for Internet of Things: A Survey on Performance for Resource-Constrained Devices**
    - **Summary**: This paper surveys the performance of PQC algorithms in resource-constrained devices, such as those used in the Internet of Things (IoT). It reviews recent proposals to optimize PQC algorithms for these devices, addressing the challenges of implementing PQC in resource-limited environments.
    - **Link**: Read the paper3.

8. Possible Project Statements

1. **AI-Driven Intrusion Detection Systems (IDS)**
    - Develop an IDS using machine learning algorithms to detect and classify network intrusions in real-time.
2. **Blockchain-Based Secure Communication**
    - Implement a secure communication protocol using blockchain technology to ensure data integrity and confidentiality.
3. **Zero Trust Architecture Implementation**

- Design and implement a zero trust network architecture for an enterprise environment, focusing on continuous verification and least privilege access.

4. **Ransomware Detection and Mitigation**
    - Create a system to detect and mitigate ransomware attacks using behavioural analysis and machine learning techniques.
5. **Secure IoT Device Communication**
    - Develop a secure communication framework for IoT devices, addressing challenges such as authentication, encryption, and data integrity.
6. **Firewall Optimization and Management**
    - Analyse and optimize firewall rules and configurations to enhance network security while maintaining performance.
7. **Secure Cloud Storage Solutions**
    - Design a secure cloud storage solution that ensures data confidentiality, integrity, and availability using encryption and access control mechanisms.
8. **Network Traffic Analysis for Threat Detection**
    - Implement a network traffic analysis tool to detect and respond to potential threats using deep packet inspection and anomaly detection.
9. **Post-Quantum Cryptography**
    - Explore and implement post-quantum cryptographic algorithms to secure network communications against quantum computing threats.
10. **Privacy-Preserving Data Sharing**
    - Develop a privacy-preserving data sharing protocol using homomorphic encryption or secure multi-party computation.

11. **Adaptive Security Policies**

- Create an adaptive security policy framework that dynamically adjusts security measures based on real-time threat intelligence and network conditions.

12. **Secure Mobile Payment Systems**

- Design and implement a secure mobile payment system that protects against fraud and ensures transaction integrity.

(If your team membership is not yet confirmed, please do so , latest by Monday – 10th March 10 PM. No change after that.).