Dissertation Title:

AI-Driven Adaptive Security and Recovery Pipeline

**Course No.:** [**S2-24\_SEZG628T**](https://taxila-aws.bits-pilani.ac.in/course/view.php?id=13815)

**Course Title: Dissertation**

**Dissertation Work Done by:** **Dabhade Pooja Bhanudas**

**Student Name: Dabhade Pooja Bhanudas**

**BITS ID: 2023MT93089**

**Degree Program: M.Tech. Software Engineering**

**Research Area: Cyber Security and Machine learning**

**Dissertation / Project Work carried out at:**

**BITS PILANI**



**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

## VIDYA VIHAR, PILANI, RAJASTHAN - 333031.

**(January 2025)**

**Contents**

[1. Broad Area of Work 3](#_Toc188191718)

[2. Background 4](#_Toc188191719)

[3. Objectives 4](#_Toc188191720)

[4. Scope of Work 4](#_Toc188191721)

[5. Plan of Work 5](#_Toc188191722)

[6. Literature References 7](#_Toc188191723)

[7. Particulars of the Supervisor and Examiner 8](#_Toc188191724)

[8. Remarks of the Supervisor 9](#_Toc188191725)

# Broad Area of Work

The project will consist of the following four stages:

1. **Monitoring:**
   * Utilize AI-based anomaly detection models (e.g., LSTMs) to monitor system logs, network traffic, and hardware performance.
   * Integrate real-time dashboards for visualizing system health and potential threats.
   * **Tools:** Elastic Stack (ELK) for log monitoring, Grafana for dashboards, and Prometheus for performance metrics.
2. **Detection:**
   * Implement supervised and unsupervised machine learning models to classify and prioritize threats based on severity and potential impact.
   * Develop a hybrid detection system combining signature-based and behavioral analytics.
   * **Tools:** TensorFlow or PyTorch for ML model implementation, Snort or Suricata for signature-based detection, and OpenAI API for behavioral analysis.
3. **Quarantine:**
   * Introduce a sandboxing mechanism for isolating suspected binaries and processes.
   * Maintain a secure repository of verified binaries using digital signatures and hash verification or certificate-based validation to ensure data integrity. Additionally, blockchain integration can be considered as an advanced option for tamper-proof storage and management.
   * **Tools:** Firejail or Cuckoo Sandbox for process isolation, HashiCorp Vault for secure repository management, and OpenSSL for digital signature verification.
4. **Resolution:**
   * Employ containerization (e.g., Docker) for rapid deployment of fresh, secure components.
   * Implement automated rollback mechanisms using immutable snapshots and transaction logs.
   * Use AI-driven decision-making to prioritize and execute recovery actions.
   * **Tools:** Docker or Kubernetes for containerization, AWS Backup for snapshots, and AI-based decision engines like IBM Watson for recovery actions.

**Research Areas**

The project spans multiple research domains, including:

* Cybersecurity: Intrusion detection, ransomware resilience, and incident response.
* Artificial Intelligence: Anomaly detection, threat classification, and autonomous decision-making.
* Machine Learning: Supervised/unsupervised learning and ensemble methods.
* System Resilience: Self-healing systems and disaster recovery.
* Digital Signatures and Certificate Validation: Ensuring data integrity and secure backup storage. Blockchain: Advanced option for tamper-proof backup solutions.

# Background

In an era of rapidly evolving cyber threats and increasing system vulnerabilities, ensuring robust security and resilience for software systems is paramount. Current cybersecurity solutions often focus on specific aspects such as endpoint protection, centralized log management, or malware detection, leaving gaps in handling diverse attack vectors and ensuring seamless recovery. This project aims to address these limitations by developing an AI-driven Adaptive Security and Recovery Pipeline (ASRP) that integrates monitoring, detection, quarantine, and resolution mechanisms for comprehensive protection against a wide range of attacks, including digital, ransomware, system hardware failures, and software vulnerabilities.

# Objectives

The primary objective of the project is to design and implement a modular, scalable, and AI-powered pipeline capable of:

1. Monitoring systems for suspicious activities across hardware, software, and networks.
2. Detecting fraudulent or malicious activities in real-time.
3. Quarantining compromised binaries and isolating affected systems autonomously.
4. Resolving incidents by automatically replacing compromised components with verified, secure versions, ensuring minimal downtime and system integrity.

# Scope of Work

1. A fully functional prototype of the Adaptive Security and Recovery Pipeline for a sample application like Notepad++ or any sample directory attack.
2. Demonstration of the pipeline’s effectiveness in detecting, isolating, and recovering from diverse attack scenarios.
3. Comprehensive documentation and performance evaluation, comparing it with existing cybersecurity solutions.

# Plan of Work

|  |  |  |
| --- | --- | --- |
| **Phases** | **Start Date-End Date** | **Work to be done** |
| Dissertation Outline | 18th January 2025 - 25th January 2025 | Literature Review and prepare Dissertation Outline |
| Design & Development in phases | 25th January 2025 – 10th March 2025 | Design & Development Activity |
| Testing of work done | 10th March 2025 – 20th March 2025 | Software Testing, User Evaluation & Conclusion |
| Mid-Semester progress report | 20th March 2025 - 27th March 2025 | Submit Dissertation to Supervisor & Additional Examiner for review and feedback |
| Incorporating feedback after review | 31st March 2025 - 17th April 2025 | Incorporating and modifying report or work after examiner’s review. |
| Final Dissertation Report | 17th April 2025 - 24th April 2025 | Final Review and submission of Dissertation |

# Literature References

The following are referred journals from the preliminary literature review.

1. *A. Manoharan and M. Sarker, ‘‘Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and ML for next-generation threat detection,’’ Tech. Rep., 2023, doi: 10.56726/IRJMETS32644.*
2. *M. Asmar and A. Tuqan, ‘‘Integrating machine learning for sustaining cybersecurity in digital banks,’’ Heliyon, vol. 10, no. 17, Sep. 2024, Art. no. e37571.*
3. *I. Kara and M. Aydos, "Cyber fraud: Detection and analysis of the crypto-ransomware", Proc. 11th IEEE Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON), pp. 764-769, Oct. 2020.*
4. *I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks", Exp. Syst. Appl., vol. 190, Mar. 2022.*
5. *A. M. Maigida, S. M. Abdulhamid, M. Olalere, J. K. Alhassan, H. Chiroma and E. G. Dada, "Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms", J. Reliable Intell. Environ., vol. 5, no. 2, pp. 67-89, Jul. 2019.*

# Particulars of the Supervisor and Examiner

|  |  |  |
| --- | --- | --- |
|  | **Supervisor** | **Additional Examiner** |
| Name | Rupam Kumar Kundu | Rupam Kumar Kundu |
| Qualification | MTech in Advanced Communication System from National Institute of Technology, Warangal (July. 2018 – June 2020) | MTech in Advanced Communication System from National Institute of Technology, Warangal (July. 2018 – June 2020) |
| Designation | Senior Software Engineer at Dell Technologies | Senior Software Engineer at Dell Technologies |
| Employing Organization and Location | Dell Technologies  Bagmane World Technology Center, KR Puram Marathahalli North Ring Road Hobli, Doddanekundi, Mahadevapura, Bengaluru, Karnataka 560048 | Dell Technologies  Bagmane World Technology Center, KR Puram Marathahalli North Ring Road Hobli, Doddanekundi, Mahadevapura, Bengaluru, Karnataka 560048 |
| Phone No.(with STD Code) | +91 7603005922 | +91 7603005922 |
| Email Address | rkkundu90@gmail.com | rkkundu90@gmail.com |

# Remarks of the Supervisor

The **"AI-driven Adaptive Security and Recovery Pipeline"** is a groundbreaking initiative that tackles an urgent and ever-expanding global challenge in cybersecurity. By harnessing the power of AI to automate threat detection, classification, and recovery, the project has the potential to revolutionize the field, setting new standards for efficiency and resilience. Its modular design and comprehensive scope position it not only as a game-changer for current cybersecurity practices but also as a pivotal framework for shaping the future of secure systems across industries. With proper execution, this pipeline can significantly enhance the ability to defend against and recover from sophisticated cyberattacks, fostering innovation and bolstering global trust in digital infrastructures.

This project aims to bridge the gaps in current cybersecurity systems by delivering an innovative, AI-powered solution that enhances system resilience and security. By combining advanced monitoring, detection, quarantine, and recovery capabilities, the Adaptive Security and Recovery Pipeline will set a new standard in automated cybersecurity and recovery systems.

After an initial discussion with the student, I was impressed by her diligence, determination, and technical acumen. She has demonstrated the requisite skills and commitment to execute this project within the standard research paradigm effectively. As the supervisor, I am pleased to approve this promising project, confident in its potential to contribute meaningfully to the field of cybersecurity.

**Information about the Supervisor:**

|  |  |
| --- | --- |
| Supervisor's Name: | Rupam Kumar Kundu |
| Supervisor's Email: | rkkundu90@gmail.com |
| Supervisor's Qualification: | 1) **MTech in Advanced Communication System** from **National Institute of Technology, Warangal** (July. 2018 – June 2020)  2) **BTech in Electronics and Communication Engineering** from **Asansol Engineering College Asansol, West Bengal**(July. 2008 – June 2012) |
| Supervisor's Designation & Address: | Senior Software Engineer at Dell Technologies  [Address](https://www.google.com/search?sca_esv=22e2dfd6070c855c&rlz=1C1GCCO_en&cs=0&sxsrf=ADLYWILsy1gURQdYWgBC-vJsQqRSjqj6NQ:1733283619227&q=dell+emc+corporation+address&ludocid=9987224758953981771&sa=X&ved=2ahUKEwilqqrTmI2KAxVfS2wGHW-OHFIQ6BN6BAgWEAI):  Bagmane World Technology Center, KR Puram Marathahalli North Ring Road Hobli,  Doddanekundi, Mahadevapura, Bengaluru, Karnataka 560048 |
| Supervisor's Phone No. (with STD code): | +91 7603005922 |

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**WORK INTEGRATED LEARNING PROGRAMMES (WILP) DIVISION**

**SECOND SEMESTER OF ACADEMIC YEAR 2024-2025**

[**S2-24\_SEZG628T**](https://taxila-aws.bits-pilani.ac.in/course/view.php?id=13815)**: DISSERTATION OUTLINE**

|  |  |
| --- | --- |
| **STUDENT ID No.** | 2023MT93089 |
| **NAME OF THE STUDENT** | Dabhade Pooja Bhanudas |
| **STUDENT'S EMAIL ADDRESS** | 2023mt93089@wilp.bits-pilani.ac.in |
| **STUDENT’S EMPLOYING ORGANIZATION & LOCATION** | Dell Technologies, Pune |
| **SUPERVISOR’S NAME** | Rupam Kumar Kundu |
| **SUPERVISOR’S EMPLOYING ORGANIZATION & LOCATION** | Dell Technologies, Bangalore |
| **SUPERVISOR’S EMAIL ADDRESS** | rkkundu90@gmail.com |
| **ADDITIONAL EXAMINAER’S NAME** | Rupam Kumar Kundu |
| **ADDITIONAL EXAMINER’S EMPLOYING ORGANIZATION & LOCATION** | Dell Technologies, Bangalore |
| **ADDITIONAL EXAMINER’S EMAIL ADDRESS** | rkkundu90@gmail.com |
| **DISSERTATION TITLE** | AI-driven Adaptive Security and Recovery Pipeline |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Signature of Student** | **Signature of Supervisor** | **Signature of Additional Examiner** |
| **Name: Dabhade Pooja Bhanudas** | **Name: Rupam Kumar Kundu** | **Name: Rupam Kumar Kundu** |