Shreyas S

49_Phase1_ESA_Report

Quick Submit

Quick Submit

PES University

Document Details

Submission ID trn:oid:::1:3111142467	25 Pages
Submission Date Dec 11, 2024, 11:54 AM GMT+5:30	4,932 Words
Download Date Dec 11, 2024, 11:57 AM GMT+5:30	29,434 Characters
File Name 49_Phase1_ESA_Report.docx	
File Size 126.7 KB	

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

ABSTRACT

CCTV systems are an absolute necessity in modern surveillance, but their use is very vast covering everything from banking to transportation, healthcare to public safety. But these systems are becoming increasingly vulnerable to cyber threats, where replay attacks being one of the main threats. An alteration of video authentication can happen due to replay attacks, which involve capturing any valid stream and then re-recording it and putting it into the system to deceive the system and providing access to the camera, which could change the video and compromise the whole security of the system. This highlights the need for better security especially around communication protocols that which aren't strict enough

To tackle these challenges, we are proposing an AI-based detection and response system specifically designed to mitigate replay attacks in CCTV networks. By integrating machine learning and cryptographic security measures, the system aims to detect, prevent, and respond to replay attacks in real-time, due to which we can rely on cctv systems without any fear.

The main components are:

1. AI-Powered Anomaly Detection: We will be utilizing ML models to analyze video streams and network traffic for anomalies that indicate replay attacks, such as inconsistencies in timestamps and frame sequences.

2. Secure Communication Protocols: We plan on mplementing encryption and/or digital signatures in order to ensure secure data transmission and to verify that video streams are not tampered with, and that only legitimate data is processed.

3. Real-Time Automated Response: We will be working on a threat response module that takes appropriate action in near-real time upon detecting an attack, including alerting administrators, isolating compromised devices, and blocking malicious traffic.

4. Modular Design: We will try our best to design this system so that it can seamlessly integrate with existing CCTV systems, ensuring compatibility with a lot of hardware and software configurations.

This project will nvolve a comprehensive vulnerability assessment of current CCTV systems, training ML models on datasets simulating replay attacks, and testing in controlled environments. The goal is to make a scalable, effective and user friendly system.

It is anticipated that effective implementation will yield better detection of replay attacks, thus resulting in enhanced security in CCTV systems, reduced susceptibility to cyber threats, and thus making surveillance technologies more reliable. Hence the project is a step forward towards intelligent, adaptable and self-Secured surveillance technologies

INTRODUCTION

CCTV systems have become an integral part of security infrastructures, utilities that offer real-time surveillance and recording capabilities to deter threats and protect sensitive surroundings such as banks, data hubs, transportation hubs, and public areas. But these systems are vulnerable to replay attacks, a sophisticated type of cyberattack in which hackers intercept and capture real video footage or commands sent by the system, and retransmit the data at some point in the future. By replaying old footage or commands, attackers can deceive systems into displaying false information as live data, and thus bypass real-time monitoring mechanisms.

Replay attacks exploit the weaknesses in communication protocols that aren’t secured properly or old/legacy CCTV systems that don’t have modern safeguards such as strong encryption, authentication, or tamper detection mechanisms. This can lead to really bad consequences, including:

1. Bypassing Real-Time Surveillance:
Attackers may be able to replace live(legitimate) video streams with previously recorded footage(tampered data), masking their current activities or making the system believe that everyting is normal while intrusions or unauthorized actions happen. This compromises of system’s ability to detect and respond to real-time threats.

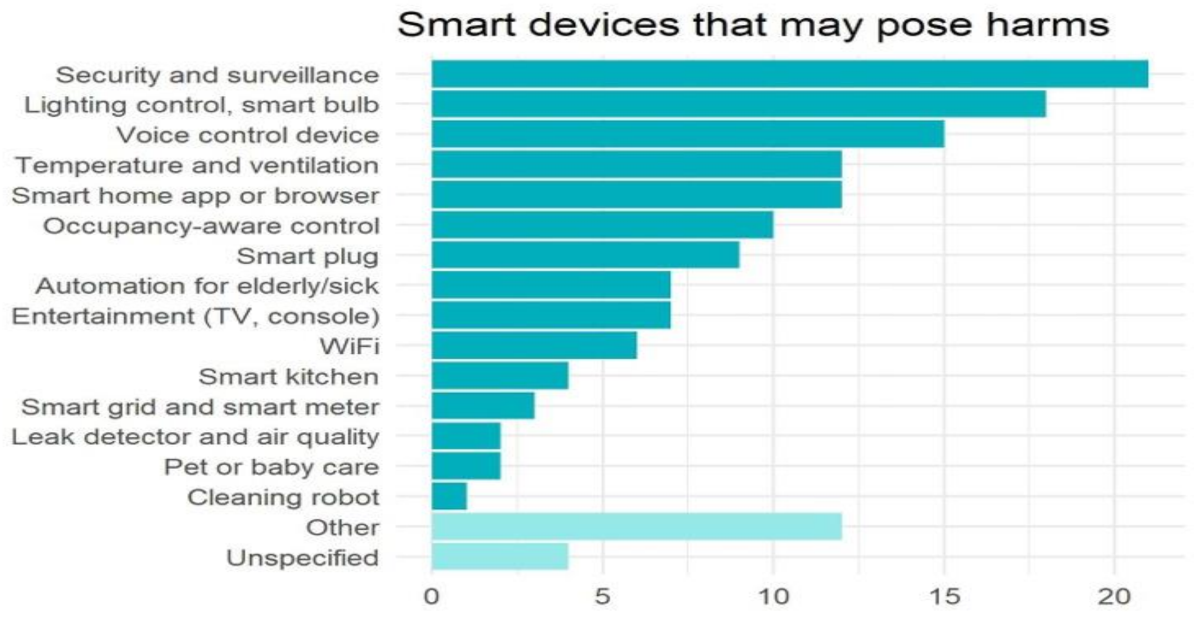
2. Creating Security Blind Spots:
By replaying old footage, hackers may acquire the ability to hide unauthorized access or any movements in sensitive areas such as secure bank vaults, server rooms, or restricted zones in airports and other such areas. These undetected intrusions can lead to theft, sabotage, or unauthorized access to critical information and devices.

3. Manipulating Evidence:
Surveillance footage is used many times as evidence in legal investigations and cases. Replay attacks can tamper with original recordings, leading to timelines that aren’t accurate, display of events that never occurred, or data can go missing, which potentially derail investigations and undermine judicial processes.

4. Exploiting Access Control Systems:
Quite a few of the modern access control systems are integrated with CCTV systems for enhanceing the security, such as monitoring entries and exits. Replay attacks may exploit this integration by retransmitting any old footage of authorized entries, thus granting attackers unauthorized access without raising any alarms.

5. Targeting Legacy Systems:
Older CCTV cameras have outdated firmware which may lead to high exposure. Threat actors can easily attack these CCTV cameras and do replay attacks on the CCTV cameras and do replay

attacks. They can exploit both physical and digital parts of the system. This shows that we have to ensure that proper protocols are implemented and all the firmwares are updated inorder to prevent any kinds of replay attacks from threat actors in future.



This graph shows us about the different smart devices that might be vulnerable to security threats in real life. We found out that security and surveillance (like CCTV cameras and other surveillance devices). This encouraged us to focus on security and surveillance for our capstone project. The graph and data according to the research paper which we have reffered and the link is given here: https://arxiv.org/abs/2209.05458v1

PROBLEM STATEMENT

“Detection and Mitigation of Replay Attacks on CCTV Systems”

SCOPE

The utilization of artificial intelligence (AI) in surveillance systems is a transformative method of dealing with security threats like replay attacks which are detected and mitigated. Replay attacks, which involves retransmitting intercepted footage to manipulate surveillance systems, pose severe risks to the integrity and reliability of critical security infrastructure. Our project focuses on using AI to build a good detection and response framework against replay attacks, ensuring that there is proper safety trust especially among the sectors where trust and security play a very vital role.

Applications of AI in Securing Surveillance Systems
Urban Security and Smart Cities
AI can play a very role in city-wide surveillance systems by ensuring continuous, real-time protection of public spaces. These systems often form the backbone of law enforcement and crowd management in urban environments. AI-powered solutions can:

Analyze live video streams for inconsistencies, such as repeating patterns or irregular timestamps.
Generating real-time alerts so that an incident threat system can be employed to detect these attacks
Safeguarding critical data used in smart city applications like emergency response and urban planning.

Retail and Commercial Security

In retail environments, CCTV systems are very important for theft prevention and customer safety, replay attacks can also enable fraud activities which is a big very threat to security and integrity. AI-based solutions provide:

Advanced anomaly detection can help in detecting if the footage is tampered or there is presence of any artificial movement in the video footage
Cross-verification of surveillance footage with transaction records to ensure alignment.
Real-time incident detection, aiding in loss prevention and dispute resolution.
Enhanced accountability and insights for staff training and operational improvements.

Traffic Monitoring and Law Enforcement

Traffic surveillance system has a very important in managing urban mobility and it also ensures that there is r road safety and prevent things like accidents. Replay attacks targeting traffic monitoring systems can lead to false violations or coverup the accidents that occured
AI enhances traffic monitoring by:

Validating video timestamps so that it can go well with real-time incident response system
Detecting environmental discrepancies. Ensuring that there is enough and proper evidence for traffic violations and accidents.We can improve the accuracy of traffic analytics for better urban planning.

Banking and Financial Security

In banking institutions CCTV cameras play a very pivotal role. Also important in ATMs to check out for any illegal transactions. They are very essential for tracking movement of people around the bank and also check essecntial places like vaults or any other unauthorized areas to prevent any kind of unauthorized access

AI provides:

Continuous validation of video streams so that we can continuously detect if there is any tampering in the video
Secure monitoring in high-security zones like vaults so that we can prevent situations like robbery
Precision fraud detection through cross-analysis of CCTV footage and transaction logs.

Conclusion

The integration of AI in surveillance systems offers a lot of capabilities in detecting and preventing replay attacks across multiple domains. By applying ML algorithms and real-time anomaly detection, this project aims to provide security of critical infrastructures, protect important data, and ensure that there is proper safety of surveillance footage.

Conclusion

This proves us that implementation of AI systems in the present day CCTV camera systems for the detection and mitigation will help us prevent replay attacks. By applying Machine learning algorithms we can protect critical infrastructure and important confidential data which are essential to an individual. Also it will help in telling us the authenticity of the footage. This project had scope not only in trafiic camera sectors but also in other sectors which will help to establish a more reliable and secure ecosystem.

CHALLENGES

Data Quality

Ensuring a good-quality and an error free data for training the AI model is very important as it helps in proper anamoly detection. Poor data quality can often lead to more false positives due to which the system incorrectly classifies normal or benign activities as replay attakcs due to which we can miss the actual replay attacks.Abnormalities in the data can affect the AI's ability to effectively detect replay attacks, so proper pre-processing of data is important and must.

Integration with Existing Systems

Integrating AI into existing CCTV infrastructures is a very difficult and time taking process. The Legacy systems being old may not be compatible as integrating AI is tough, leading to integration issues. The integration process requires proper testing and validation so that the AI system seamlessly interfaces with the existing hardware and software, without causing disruptions or performance degradation.

Privacy Concerns

Using AI in surveillance can also raise a lot of privacy concerns, particularly regarding data protection and compliance with regulations such as GDPR. In the context of this project, ensuring that the AI system sticks to privacy standards is very important. The system must designed in such a way that it can handle surveillance data more properly. It’s also important to maintain transparency with stakeholders about data usage and ensure that the surveillance practices are legal and proper.

Evolving Threats

Cyber attackers are constantly finding new ways and vulnerabilities in the current system to take advantage and benefit from that which makes it very challenging for to keep the AI system up to date, also this will add up to the cost of mainatainence. The AI systems should have reinforcement learning, which is basically learning from each attack and making sure it has enough information on how to prevent the next attack which may come in the future.

Cost

The implementation and the maintenance of advanced AI systems to detect replay is very expensive. In the context of our project, the financial investment includes purchasing AI hardware, developing and training the models, integrating the system with existing CCTV infrastructures, and maintaining its operation. Balancing the along with the benefits is very important and proper budgeting should take and also try exploring funding options as it helps in better finance management.

OBJECTIVES

Our primary objective, and that of this project is to design and implement an AI-powered system to detect and mitigate replay attacks in CCTV surveillance systemss. Our aim will be to ensure the authenticity and reliability of video footage, protecting critical infrastructures and making modern surveillance systems more trustworthy. To achieve these goals, we have identified the following objectives:

Developing an AI-Based Detection Framework

Design and train ML models capable of identifying anomalies in video streams that indicate replay attacks.

Leveraging advanced algorithms to differentiate between live(real) footage and replayed or tampered (fake/malicious) video data.

Implementing Real-Time Monitoring and Alerts

Enable continuous, near-real-time monitoring of CCTV feeds for threat detection.

Generate automated alerts to notify security team about potential replay attacks, thus ensuring swift responses.

Enhancing Data Integrity in Surveillance Systems

Implementing mechanisms so that integrity of video streams can be validated: by analyzing timestamps, environmental contexts, and camera metadata.

Protect surveillance data from tampering so that it is reliable for law enforcement, legal proceedings, and operational decision-making.

Ensuring Adaptability Across Multiple Sectors

Designing the system so that it can cover many use cases, including urban surveillance, retail security, traffic management, and banking. But focus will be on urban surveillance and traffic management.

Incorporate scalability so that many levels of security infrastructure can be supported: from small-scale setups to large, city-wide networks.

Integrate IoT and AI Technologies

Utilizing IoT-enabled CCTV systems to facilitate seamless data collection.

Employing AI-driven analytics so that resource allocation can be optimized, such as focusing monitoring efforts on high-risk zones.

Minimizing False Positives and False Negatives

Ensure the accuracy of the detection system by reducing false alarms and missed detections.
Promoting Automation in Cybersecurity Responses

Developing automated responses to mitigate replay attacks, such as isolating compromised cameras or reconfiguring network protocols, along with alerting the concerned teams.
Ensure that these responses are both effective and cause very minimal disturbance to ongoing surveillance operations.

LITERATURE SURVEY

3.1 A Data-Driven Framework for Verified Detection of Replay Attacks on Industrial Control Systems

3.1.1 Introduction

The paper proposes a data-driven approach to detection of replay attacks on industrial control systems and a verification framework. To address this challenge, the authors Sara Gargoum, Negar Yassaie, Ahmad W. Al-Dabbagh and Chen Feng propose a two-stage framework that utilizes advanced detection and verification techniques to improve the reliability of such systems.

3.1.2 Characteristics and Implementation

The framework employs:
Data from sensors in real time: Anomaly detection using change-point detection based on matrix profile
Spatio-temporal feature extraction: Achieved using short-time Fourier transform (STFT) for visualization via spectrograms.
DL Methods: Understanding Replay Attacks using Conv-STM-AE (Convolution-based Long Short-Term Memory Autoencoder) by analyzing the reconstruction error
This method leverages statistical analysis and deep learning to gather comprehensive coverage of range vectors.

3.1.3 Features

- It confirms the feasibility of the framework with a 100% verification rate for replay attack detection across different scenarios from the simulation model of Tennessee Eastman Process.
Reliability: Offers a low false alarm rate and low delay in detection with practical utility in real industrial environments.
Scalability: Engineered with industrial systems in mind, the capability of adapting itself to complex, large-scale operations.

3.1.4 Evaluation

By evaluating the framework, the following was found:
Advantages:
Perform well in detection and verification of replay attacks with a low false positive.

Limitations:
Trains on normal data, which may not be available in an attack scenario (real-world deployment where attacks are rare).
The verification stage has a computational cost that may limit its scalability, especially in large deployments.
The risks of overfitting to specific attack patterns, potentially failing to recognize diverse or novel attack types.

3.2 Replay Attack Detection for Cyber-Physical Control Systems: A Dynamical Delay Estimation Method

3.2.1 Introduction

“A Dynamical Delay Estimation Method for Replay Attack Detection in Cyber-Physical Control Systems”Dong Zhao, Bo Yang, Yueyang Li, and Hui Zhang. It appeared in the journal IEEE Transactions on Industrial Electronics.

3.2.2 Characteristics and Implementation

The paper has proposed an approach, Dynamical Delay Estimation (DDE), that unifies system dynamics and data driven approaches. It uses sliding window methods to estimate delays between inputs to a system and outputs from that system. The delay estimations are initialized using a randomized algorithm and a window-adaptive heuristic performs the real-time detection. It concentrates on time-series correlating and variations of delay to detect replay attack anomalies.

3.2.3 Features

The method, according to the authors, was successful in detecting replay attacks in a distillation column experiment with high accuracy (90.7%). It also outperformed other anomaly detection methods like SVM, Isolation Forest, LOF, and LSTM in terms of precision (99.8%), recall (83.9%), and F1-score (91.2%). The approach demonstrated robustness against signal noise and network-induced disruptions.

3.2.4 Evaluation

Stability of the dynamics of the control system during operation is a requirement for the method that may not hold true in general. Initial Delay Range Estimation - One requires domain-specific knowledge or offline training in order to know the appropriate delay range in the first place. Although the computational complexity is lower than deep learning models, systems with heterogeneous or non-stationary dynamics are a limitation of the method. If detection is based on artificial global delay thresholds that are predetermined quite precisely, this gives little flexibility in different applications.

3.3 An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Networks

3.3.1 Introduction

The authors : Pichamuthu R, A Sathishkumar, N Khadirkumar, Wrote the paper titled “An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Networks”, and was published in this journal: Solid State Technology Volume 63, Issue 4 (2020)

3.3.2 Characteristics and Implementation

A hybrid approach using LSTM (Long Short-Term Memory) and Decision trees was proposed by the authors to detect replay attacks in WSNs. Anomalies were detected by using packet length and group delay features. Towards noise reduction and feature extraction, Gaussian blur and FFT were used on multimedia packets. The ASV Spoof 2017 dataset was used to train the metho

3.3.3 Features

This approach, according to the authors, achieved a 0% error rate on both the development and evaluation sets for packet replay detection. Decision trees demonstrated high precision and detection rates, with replay attacks achieving 99% True Positive Rate (TPR) and 0% False Positive Rate (FPR).

3.3.4 Evaluation

The approach is focused solely on WSNs, limiting its direct applicability to CCTV systems. It requires significant computational resources, making it less feasible for real-time or resource-constrained environments. Additionally, the evaluation was performed on a limited dataset, lacking testing on diverse, real-world attack scenarios.

3.4 Lightweight 3D-StudentNet for Defending Against Face Replay Attacks

3.4.1 Introduction

The paper, titled "Lightweight 3D-StudentNet for Defending Against Face Replay Attacks", is authored by Preethi Jayappa Seegenhalli and B. Niranjana Krupa. It was published in Signal, Image and Video Processing (2024).

3.4.2 Characteristics and Implementation

The study proposed 3D-ArrowNet, a deep neural network leveraging spatial and temporal features, and introduced 3D-StudentNet, a lightweight version using knowledge distillation to reduce computational complexity. The models were tested on Replay-Attack, Replay-Mobile, and combined datasets. HSV color space was used for input to enhance color texture differentiation between real and spoof attacks.

3.4.3 Features

The models achieved 100% accuracy on the Replay-Attack dataset and 99.66% accuracy with an ACER (Average Classification Error Rate) of 0.45 on the Replay-Mobile dataset. Combined dataset accuracy was reported as 99.23%.

3.4.4 Evaluation

The 3D-ArrowNet's computational complexity is high due to large kernel sizes (e.g., 11×11×11), making it intensive for real-time applications. The approach is limited to facial replay attacks, lacking evaluation on broader datasets like those for CCTV systems. There are potential generalization issues for novel or unseen attack types, such as 3D mask attacks or partial face region attacks.

3.5 Sequential Detection of Replay Attacks

3.5.1 Introduction

Sequential Detection of Replay Attacks Author:Arunava Naha, André Teixeira, Anders Ahlén, Subhrakanti Dey IEEE, Conference: Transactions on Automatic Control, Vol. 68, No. 3, March 2023

3.5.2 Characteristics and Implementation

1. Introduced a replay attack detection scheme using cumulative sum (CUSUM) tests.
2. Employed a joint statistical analysis of the innovation and watermarking signals.
3. Derived Kullback–Leibler divergence (KLD) for joint distributions before and after the attack.
4. Presented an optimization technique for watermarking signal variance to maximize KLD.
5. Proposed a strategy to improve detection for systems with a relative degree greater than one by incorporating delayed watermarking signals.

3.5.3 Features

Achieved reduced detection delay compared to state-of-the-art methods like Neyman–Pearson-based χ^2 detectors.

Improved detection efficiency by optimizing watermarking signals for minimal cost.
Demonstrated effectiveness through simulations with multiple system models, including linear time-invariant and time-varying systems.

3.5.4 Evaluation

1. Assumes attacker does not access watermarking signals.
2. Some models rely heavily on system-specific parameters, which might limit generalizability.
3. Techniques like suboptimal CUSUM tests may lead to non-optimal detection in certain scenarios.
4. High relative-degree systems may experience reduced KLD, necessitating additional measures for improvement.

3.6 Optimal Chi-squared Detector of Replay Attacks on Cyber-Physical Systems

3.6.1 Introduction

Optimal Chi-squared Detector of Replay Attacks on Cyber-Physical Systems,Authors :Aaqib Patel, Md. Zafar Ali Khan Conference: 2021 9th International Conference on Systems and Control (ICSC)

3.6.2 Characteristics and Implementation

1. Designed an optimal chi-squared detector by adding random authentication signals to control inputs.
2. Optimized the covariance matrix of the authentication signal to maximize detection performance while controlling false alarms.
3. Conducted hypothesis testing to distinguish between normal and replayed data based on test statistics.

3.6.3 Features

1. Improved detection performance compared to suboptimal methods by optimizing the covariance matrix.
2. Demonstrated through simulations that the optimized approach achieves higher detection probability with lower false alarms, even under tight constraints.

3.6.4 Evaluation

1. Assumes the attacker has limited ability to anticipate or bypass random signals.
2. The method relies on strict assumptions about system stability and noise characteristics.
3. May not be directly applicable to non-linear or dynamic systems without significant adaptation.

3.7 Reinforcement Learning Solution for Cyber-Physical Systems Security Against Replay Attacks

3.7.1 Introduction

Reinforcement Learning Solution for Cyber-Physical Systems Security Against Replay Attacks
Authors: Yan Yu, Wen Yang, Wenjie Ding, Jiayu Zhou
Journal: IEEE Transactions on Information Forensics and Security, Vol. 18, 2023

3.7.2 Characteristics and Implementation

1. Proposed a model-free reinforcement learning-based framework for detecting replay attacks.
2. Formulated the detection as a Markov Decision Process (MDP).
3. Utilized Q-learning to optimize attack-defense strategies dynamically.

3.7.3 Features

1. Demonstrated high detection accuracy and adaptability to evolving attack strategies.
2. Enhanced estimation performance in CPS under replay attacks.
3. Showed robustness against intelligent attackers in simulations.

3.7.4 Evaluation

1. Focused on Cyber-Physical Systems (CPS), requiring adaptation for CCTV systems.
2. Computational complexity in real-time large-scale networks.
3. Assumes knowledge of system parameters for attack-defense interactions.

3.8 A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City

3.8.1 Introduction

A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City
Authors: Asmaa A. Elsaeidy, Abbas Jamalipour, Kumudu S. Munasinghe
Journal: IEEE Access, Vol. 9, 2021
DOI: 10.1109/ACCESS.2021.3128701

3.8.2 Characteristics and Implementation

1. Proposed a hybrid deep learning model combining Restricted Boltzmann Machines (RBM) for feature learning and CNN for classification.
2. Used time-series data from smart city systems (environmental, river, soil) and simulated replay/DDoS attacks.

3.8.3 Features

1. Achieved high accuracy: 98.37% (environmental), 98.13% (river), and 99.51% (soil datasets).
2. Outperformed other models in detecting attacks effectively.
3. Focused on IoT-based smart city datasets; may need adaptation for CCTV systems.
4. Computationally intensive, requiring powerful hardware for real-time application.

RESEARCH / TECHNOLOGY GAP AND CHALLENGES

1. Lack of Focus on Real-Time Streaming Data:

- **Current State:** Most existing research on replay attacks in CCTV systems primarily focuses on offline analysis of recorded footage. This approach is not suitable for real-time surveillance where immediate detection and response are crucial.

- **Gap:** There is a significant gap in developing systems that can analyze and respond to threats in real-time as the data is being streamed. Real-time analysis is essential for timely intervention and preventing potential security breaches.

2. Implementation of Reinforcement Learning:

- **Current State:** Traditional machine learning models used in surveillance systems are often static and require periodic retraining with new data to stay effective.
- **Gap:** Reinforcement learning (RL) offers a dynamic approach where the AI model can continuously learn and adapt from new incidents in real-time. The flexibility is extremely important for good accuracy and efficiency of anomaly detection over time. However, the integration of RL in surveillance systems is still in its early stages and it still requires more research and development.

3. Non-Existent Incident Response System:

- Current State: Multiple CCTV surveillance systems don’t have a proper incident response system. While the detection of anomalies is possible, mitigation and response to these incidents are often manual and time-consuming.

- Gap: There is a need for automated incident response systems that can not only detect anomalies but also take immediate corrective actions, such as alerting security personnel, locking down areas, or initiating lockdown protocols. Such systems would significantly enhance the overall security posture and reduce the response time to potential threats.

Overview of Datasets

1. Link 1: Highway Traffic Videos Dataset
   Source – Kaggle
   Size – 92.45 MB

2. Link 2: Replay-Attack — EN
   Source – Idiap
   Size – 90 MB

3. Link 3: Urban Tracker: Suivi multiobjets en milieu urbain
   Source – Urban Tracker
   Size – 120 MB

4.1 Description

Link 1: This a video database of a traffic footage on a highway. The video shows that it was taken over two days from a stationary camera overlooking a traffic at the highway. The videos were labeled manually as light, medium, and heavy traffic.

Link 2: The dataset has real clients accessing a laptop with web-camera and spoofing attacks through photos or videos. Videos (320x240, 25Hz) were recorded on a MacBook in controlled and adverse lighting conditions. For spoofing attacks, high-resolution photos or 720p videos of the victim captured using a static or handheld camera (Canon PowerShot) were used by the attacker. Files are in ". mov" format, and compatible with standard video tools in all active continents.

4.2 Database Attributes/Features

1. Link 1: info.txt - more information about each video
ImageMaster - the index number and class for each video
ImageMaster.mat - MATLAB file of ImageMaster

EvalSet_train - each row is a training set

EvalSet_test - each row is a test set for the corresponding training set

EvalSet.mat - MATLAB file of EvalSets

video/ - the traffic videos

traffic_patches.mat - traffic patches of video

traffic_patches_reg.mat - traffic patches, registered by hand

-- LOCATION --

Source: http://www.wsdot.wa.gov/

City: Seattle, WA.

Location: I-5 S 188th St.

Direction: looking south

Traffic: Southbound traffic

Date: 08/05/2004 to 08/06/2004

CONCLUSION OF PROJECT PHASE 1

Our project aims to address the critical security challenge posed by replay attacks in CCTV systems, which is a growing concern in modern surveillance systems. We aim to leverage AI-powered anomaly detection, secure communication protocols, and real-time automated responses. We are aiming to provide a robust defense mechanism to enhance reliability and integrity of surveillance systems. We also aim to design our system in a modular way, so that we can allow seamless integration of our solution with existing infrastructures. Our project is aiming to focus on live real-time streaming, thus demonstrating the potential of advanced AI-driven techniques to safeguard sensitive environments and increase public safety. We aim to set a strong foundation for future innovations in intelligent, adaptive security measures for an increasingly connected world.

PLAN OF WORK FOR CAPSTONE PHASE 2

1.Acquiring/Creating relevant datasets

1.Choosing the appropriate software tools that will be used for the project

2.Creating a detailed workflow

3.Creating a prototype based on the datasets collected

4.High-Level Design

REFERENCES AND BIBLIOGRAPHY

[1] Seegehalli, P.J., Krupa, B.N. Lightweight 3D-StudentNet for defending against face replay attacks. *SIViP* **18**, 6613–6629 (2024). https://doi.org/10.1007/s11760-024-03339-2

[2] S. Gargoum, N. Yassaie, A. W. Al-Dabbagh, and C. Feng, "A Data-Driven Framework for Verified Detection of Replay Attacks on Industrial Control Systems," IEEE Transactions on Automation Science and Engineering, pp. 1–13, 2024, DOI: 10.1109/TASE.2024.3394315.

[3] D. Zhao, B. Yang, Y. Li, and H. Zhang, "Replay Attack Detection for Cyber-Physical Control Systems: A Dynamical Delay Estimation Method," IEEE Transactions on Industrial Electronics, vol. 71, no. 6, pp. 6263-6273, Jun. 2024, doi: 10.1109/TIE.2024.3406859.

[4] R. Pichamuthu, S. A., and N. Khadirkumar, "An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network," Solid State Technology, vol. 63, no. 4, pp. 8-22, 2020.

[5] A. Naha, A. Teixeira, A. Ahlén, and S. Dey, "Sequential Detection of Replay Attacks," IEEE Transactions on Automatic Control, vol. 68, no. 3, pp. 1247–1258, Mar. 2023. DOI: 10.1109/TAC.2022.1234567.

[6] A. Patel and M. Z. A. Khan, "Optimal Chi-squared Detector of Replay Attacks on Cyber-Physical Systems," in Proc. 2021 9th Int. Conf. Systems and Control (ICSC), Caen, France, 2021, pp. 338–343. DOI:10.1109/ICSC50472.2021.9666502.

[7] Y. Yu, W. Yang, W. Ding, and J. Zhou, "Reinforcement Learning Solution for Cyber-Physical Systems Security Against Replay Attacks," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2583–2594, 2023, doi: 10.1109/TIFS.2023.3268532.

[8] A. A. Elsaeidy, A. Jamalipour, and K. S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City," IEEE Access, vol. 9, pp. 154864-154875, Nov. 2021, doi: 10.1109/ACCESS.2021.3128701.

APPENDIX

Data anonymization is the process of protecting personal or sensitive data by removing or altering identifiable elements so that the individuals to whom the data pertains cannot be identified. It is a critical practice for maintaining privacy and complying with regulations such as the GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act).

Reinforcement Learning (RL) is a type of machine learning where an agent learns to make decisions by performing actions in an environment to maximize some notion of cumulative reward. It is inspired by behavioral psychology and operates on the principles of trial and error, learning from feedback based on actions taken.

DDoS - *attack* is a type of cyberattack in which multiple systems, often part of a network of compromised devices (botnet), overwhelm a target system, server, or network with a flood of traffic. The goal is to disrupt the normal functioning of the target, making it inaccessible to legitimate users.

ACRONYMS

CCTV: Closed Circuit Television

DDoS: Distributed Denial Of Service

GDPR: General Data Protection Regulation

IOT: Internet of Things

HIPAA: Health Insurance Portability and Accountability Act

STFT – Short Term Fourier Transform

ConvLSTM – Convolutional Long Short – Term Memory Autoencoder

LOF – Local Outlier FactorDDE – Dynamic Delay Estimation

ACER – Average Classification Error Rate

WSN – Wireless Sensor Network

FFT – Fast Fourier Transform