Individual Design Report

Secure Data Management of a CCTV System

Author:	Rishabh Arora
Group:	ELEC6200 Group 10
Supervisor:	Dr Son Hoang
Examiner:	Dr Andrea Lecchini-Visintini
Date:	January 20, 2025

University of Southampton
Faculty of Engineering and Physical Sciences

Summary

My individual efforts to the Group Design Project on Secure Data Management of a CCTV System are presented in this paper. The project aimed to create a prototype system able to guarantee for treaty verification the integrity, security, and openness of video data. System threat analysis, hardware design, project documentation, and implementation of solutions to improve the resilience of the system constituted my main obligations. Every contribution was meant to solve particular problems in line with the objectives of the project and external partner criteria. Reflecting the technical depth and management elements of the project, this paper presents a comprehensive picture of my work.

Overview

Designed to solve the difficulties guaranteeing video data integrity and trustworthiness in untrusted environments, the Secure Data Management of a CCTV System project was commissioned by AWE, the external partner. To satisfy strict criteria for data integrity and compliance, the system sought to combine sophisticated solutions including hardware tamper detection, transparent architecture, and secure transmission protocols.

Focusing on threat analysis, hardware upgrades, documentation, and bridging technical design and implementation, I participated in several facets of the project. The efforts made to reach these goals and their effects on the final output are described in this paper.

Technical Assistance

Background Research and Current Remarks on Solutions

Extensive study of current solutions and their flaws helped shape the design of the secure CCTV system. This study guided the construction of a more robust and secure systm and provided important new perspectives on critical issues [1].

An Overview of the Main Security Concerns in Current IP Cameras

- **Reolink P2P Cameras:** Strengths include SSL encryption and remote access free from port forwarding. However, using hard-coded keys exposes data on local networks, posing a significant user vulnerability[2].

- **Bosch IP Cameras:** Features end-to-end encryption and a ”secure-by-default” design philosophy to handle many typical security issues. However, reliance on a vulnerable microcontroller prone to side-channel attacks allows unauthorised access and compromises system trust [3].

- **General IP Cameras:** Many rely on default login credentials that users often neglect to change, exposing them to hacking attempts. Unsecured feeds are easily available online, allowing attackers to view private video without restrictions[4].

Important Research Findings

- Convenience often takes precedence over security in existing solutions, greatly increasing data exposure risks.
- Many cameras lack systems for consistent security updates, leaving vulnerabilities unpatched and systems at risk.
- General solutions fall short in addressing specific use cases like treaty verification, which requires transparency and updatable security elements.

System Design Implications

The knowledge gained from this study directly influenced the threat analysis and highlighted critical areas requiring redesign:

- Tamper-proofing and secure encryption mechanisms are central to preventing video manipulation.
- Modular and updatable cryptographic solutions ensure long-term resilience.
- Strong default security settings with features encouraging users to update credentials and apply best practices improve user awareness.
- Enhanced defense against physical and side-channel attacks through tamper sensors and secure microcontrollers.

Learning from the flaws in Reolink, Bosch, and other IP camera systems, our design included more robust security measures that fit the needs of the external partner and so address common risks in current systems.

Threat Analysis

Threat analysis was a key element of the project that helped shape a secure system architecture. My contributions included:

- **Examination of Threats:** Careful analysis of potential physical and cyber threats, including hardware components, storage, and data transmission vulnerabilities.
- **Classification of Threats:** Identified risks like denial-of-service (DoS) attacks, eavesdropping, replay attacks, and tampering, evaluating their likelihood and potential impact.
- **Suggested Mitigations:** Recommended timestamped handshakes to reduce replay attacks, tamper-proof hardware enclosures, and network segmentation to limit cyber threat exposure.
- **Collaboration with Teams:** Presented findings to hardware and software teams to address vulnerabilities during implementation.

The knowledge acquired from this study helped to shape the design of the system and guarantees a strong security mechanism [5], [6].

Identified Threats and Mitigations

Threat	Description	Likelihood	Impact	Mitigation Strategies
Private Key Compromise	Attackers can authenticate false data or decode video.	Medium	High	Secure hardware storage, consistent key rotation.
Insider Threat	Unauthorised access by foreign server insiders.	Medium	High	Encrypt data in transit.
Side-Channel Attacks	Extraction of private keys via timing or power analysis.	Low	High	Use side-channel resistant cryptographic libraries.
Denial-of-Service	Network/server overload disrupting video feed.	Medium	Medium	Implement rate limiting, monitor traffic, use intrusion detection.

Table 1: Identified Threats and Mitigation Strategies

Integration and Hardware Design

The functionality and adaptability of the system were much improved with the help of my hardware design. Main initiatives consisted in:

- **Hardware Upgrades:** Upgraded from Raspberry Pi Zero to Raspberry Pi 3 and 4 to address performance limitations. Donated my personal Raspberry Pi 3 to support the project.
- **3D-Printed Enclosure Design:** Designed a custom enclosure using Fusion 360, incorporating ventilation systems and cable management.
- **Hardware Integration:** Collaborated with the team to optimise the placement of components within the enclosure, balancing thermal control and accessibility.

These guarantees made sure the hardware of the system was dependable, scalable, and fit for the performance criteria of the project [7].

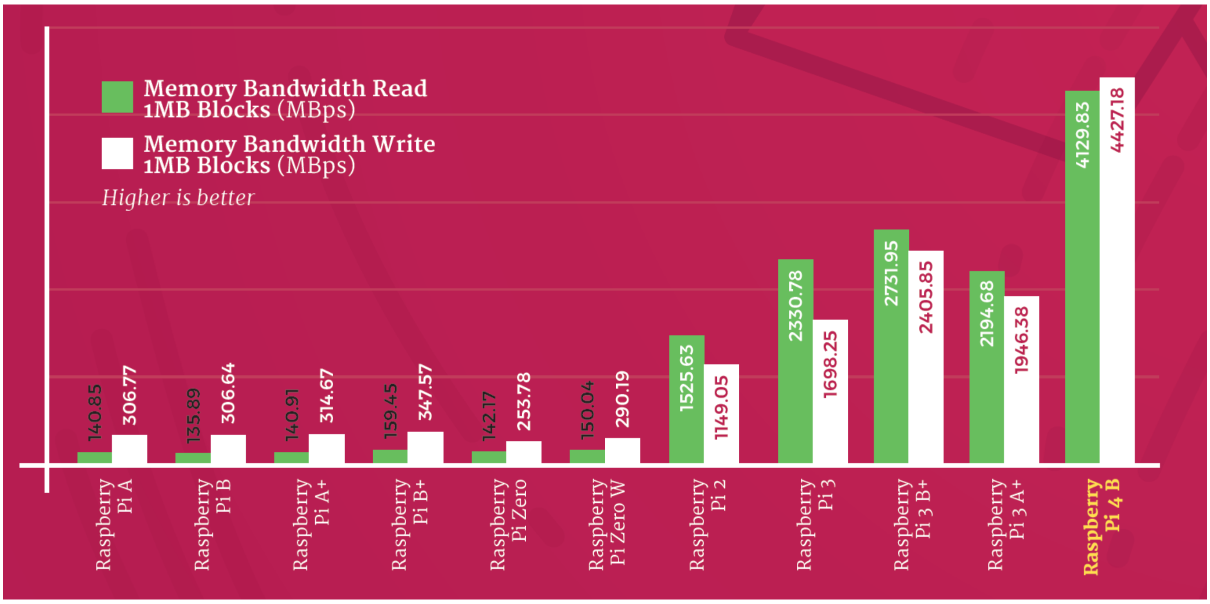


Figure 1: SysBench Memory Throughput Benchmark: Higher is Better

Figure 1 illustrates the memory throughput benchmarks for various Raspberry Pi models, highlighting the read and write bandwidth performance for 1MB blocks. The RAMspeed/SMP tool was used for this measurement. This data was sourced from The MagPi Magazine [8].

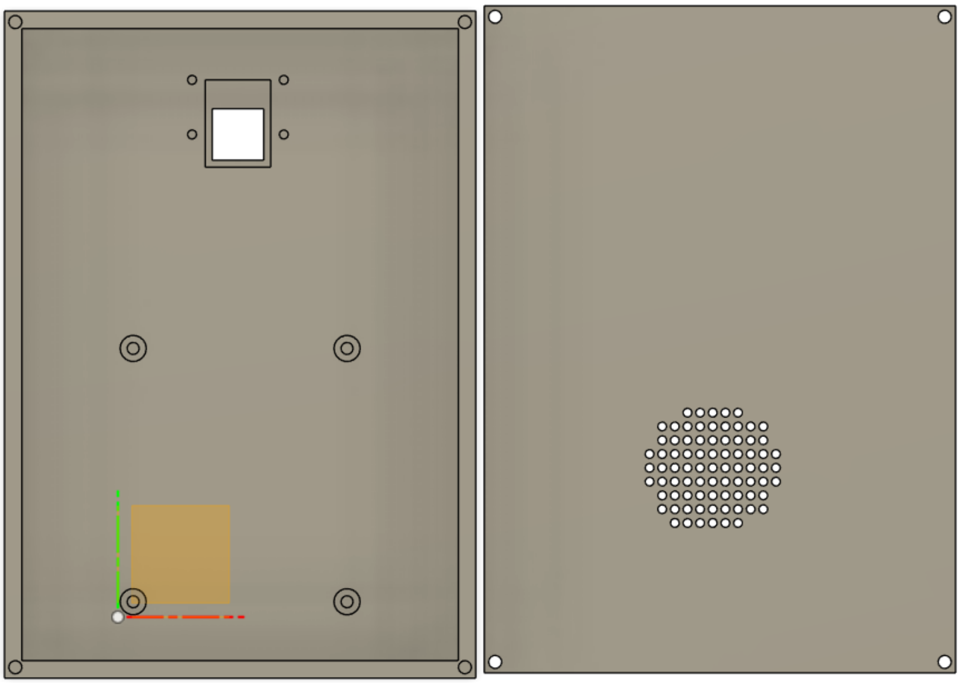


Figure 2: Top views of the final enclosure, including ventilation features and component placement.

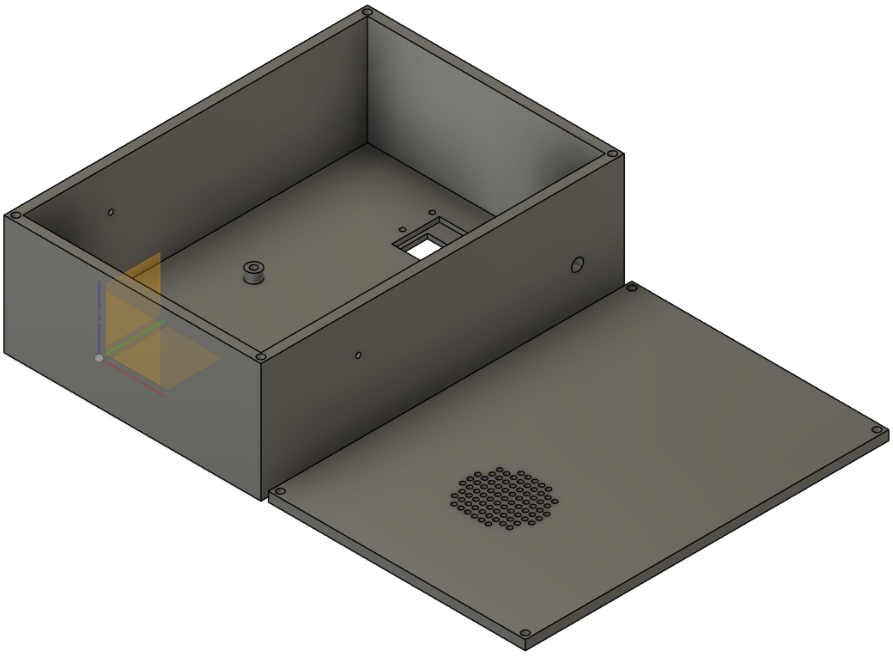


Figure 3: 3D view of the enclosure with an open lid, showing the internal configuration and ventilation layout.

The detailed enclosure design, as illustrated in Figures 2 and 3, highlights both the external and internal features essential for the system's functionality. Figure 2 presents the top views of the enclosure, showcasing the strategic placement of ventilation perforations and component slots for optimal airflow and ease of assembly. Meanwhile, Figure 3 provides a 3D perspective with an open lid, revealing the internal layout designed for efficient component placement and accessibility. Together, these figures exemplify the thoughtful integration of functional and aesthetic considerations in the enclosure's design.

Contributions to Independent Management

Organisation and Planning

Progress and overcoming obstacles required my independent contributions to project management. Main initiatives consisted in:

- Maintained a detailed record of personal tasks to ensure alignment with the group timeline.
- Adjusted schedules to accommodate unexpected delays, such as hardware delivery issues.
- Coordinated tasks among team members to optimise efficiency.
- Documented technical decisions, progress, and results for use in group reports and future projects.

Communication with Stakeholders

Throughout the project, maintaining open lines of contact with stakeholders took front stage:

- Presented hardware upgrades and threat analysis findings to AWE during meetings.
- Regularly interacted with the project supervisor to incorporate feedback into technical and management processes.

Obstacles and Solutions

Technical Challenges

- Hardware Performance Particularly in enclosure design and thermal management, the change from Raspberry Pi Zero to Pi 3 and Pi 4 demanded major adaptation. Stress testing and iterative design enhancements helped to address these issues.
- Regarding system integration first challenges were ensuring flawless communication between upgraded hardware parts and the software system. Working with the software team helped to solve compatibility problems.

Design Iterations

- Creating a 3D-printed enclosure that struck a mix between adaptability, durability, and utility needed several rounds. Refining the design depended much on the comments of team members and superiors.
- The mitigating threat is, Taking care of vulnerabilities found during threat analysis required close cooperation with the development team to apply sensible solutions without sacrificing performance.

Team Collaboration Issues

- One major obstacle I faced during the project was a team member I was closely collaborating with turning unresponsive. Our jobs were connected, and their lack of communication caused a deadlock that slowed down advancement. The matter stayed unresolved even with my best attempts to get in touch by emails and messages.
- I told the project supervisor about the matter after patiently trying to fix it alone. Making this crucial choice guarantees the project stays on course and does not stray too far. The manager stepped in and, following team negotiations, we were able to realign the project calendar.
- The delay made the team run twice the speed to meet the expected targets. I stayed calm and concentrated on keeping a cooperative approach even if I was frustrated and under pressure to make up lost time. This episode underlined the need of timely escalation and proactive communication as well as my capacity to professionally and successfully handle personal problems.

Reflections and Essential Learnings

Technical Expansion

This project gave me great chances to deepen my knowledge of threat analysis, hardware integration, and secure system design. The iterative design process for the enclosure greatly improved my command of Fusion 360 and hardware adaptation.

Management Strategies

Juggling individual efforts with team cooperation brought attention to the need of thorough documentation, effective communication, and flexibility. Navigating difficulties and guaranteeing the success of the project depend on these abilities, which proved indispensable.

Suggestions for Future Projects

- Explore more powerful and energy-efficient hardware solutions.
- Conduct extensive real-world testing to assess system resilience.
- Incorporate modular components into enclosure designs for easier maintenance and assembly.

Conclusion

This paper showcases my individual contributions to the Secure Data Management of a CCTV System project. By focusing on threat analysis, hardware design, and system integration, I significantly contributed to solving challenges and achieving project goals. These experiences not only enhanced the project but also sharpened my technical expertise and problem-solving abilities.

The project outcomes align with the external partner's requirements, laying the foundation for future advancements in secure system architecture. The knowledge gained will guide my approach to future projects, particularly those involving multidisciplinary collaboration and complex technical challenges.

Working on this project has solidified my interest in secure system design and hardware integration. The iterative nature of the design process taught me the value of continuous improvement and attention to detail. I also realised the importance of anticipating the needs of stakeholders, ensuring the system's scalability without compromising its core functionality. Overall, this project not only allowed me to contribute meaningfully to the group's success but also equipped me with technical and soft skills that will guide my future endeavours in engineering and secure system development.

References

[1] A. Costin, “Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations,” in *Proceedings of the 9th ACM Conference on Trust and Trustworthy Computing (TrustED’16)*, Vienna, Austria: ACM, Oct. 2016. DOI: `10.1145/2995289.2995290`. [Online]. Available: `https://doi.org/10.1145/2995289.2995290`.

[2] Cybersecurity and Infrastructure Security Agency (CISA). “Ics advisory (icsa-21-019-02): Vulnerabilities in ip cameras.” Accessed: 2025-01-19. (2021), [Online]. Available: `https://www.cisa.gov/news-events/ics-advisories/icsa-21-019-02` (visited on 01/19/2025).

[3] B. P. S. I. R. T. (PSIRT). “Security advisory: Bosch-sa-762869-bt.” Accessed: 2025-01-19. (2021), [Online]. Available: `https://psirt.bosch.com/security-advisories/bosch-sa-762869-bt.html` (visited on 01/19/2025).

[4] iSpyConnect Documentation Team. “Default camera passwords - ispyconnect.” Accessed: 2025-01-19. (2025), [Online]. Available: `https://www.ispyconnect.com/docs/ispy/default-camera-passwords` (visited on 01/19/2025).

[5] P. Perera and V. M. Patel, “Learning deep features for one-class classification,” *arXiv preprint arXiv:1910.10749*, 2019. [Online]. Available: `https://arxiv.org/abs/1910.10749`.

[6] P. Vennam, P. T. C., T. B. M., Y.-G. Kim, and P. K. B. N., “Attacks and preventive measures on video surveillance systems: A review,” *Applied Sciences*, vol. 11, no. 12, p. 5571, 2021. DOI: `10.3390/app11125571`. [Online]. Available: `https://doi.org/10.3390/app11125571`.

[7] F. Varghese and P. Sasikala, “A detailed review based on secure data transmission using cryptography and steganography,” *Wireless Personal Communications*, vol. 129, pp. 2291–2318, 2023. DOI: `10.1007/s11277-023-10183-z`. [Online]. Available: `https://link.springer.com/article/10.1007/s11277-023-10183-z`.

[8] T. M. Magazine. “Raspberry pi specs and benchmarks.” Accessed: 2025-01-19. (2025), [Online]. Available: `https://magpi.raspberrypi.com/articles/raspberry-pi-specs-benchmarks` (visited on 01/19/2025).

Appendix

A Weekly Journals

Week 1 - 4th October
During this week, I was able to integrate myself into the essential attributes of project management and collaboration during our first supervisor meeting. We solidified our strategies regarding proper communication with AWE by agreeing on a midweek email, along with scheduling meetings for every Friday. In addition, the workload was easier to focus on after I dived deep into the project description and researched the various threats and attacks that the CCTV system head to highlight which was the scope of the project.

Week 2 - 11th October
This week, I was present during a meeting with our industrial partner, AWE, where I was briefed on the specifics of the key objectives they outlined for the project. In the course of the discussions, I aimed to discern their user requirements, in particular, how to design the architecture of a CCTV capable of maintaining data integrity during its storage, transmission and subsequent processing. I also examined means to mitigate the threats of both physical and cyber attacks on the system and the security of video feeds and its peripheral devices. This week defined the technical objectives which we have to meet in the course of our work and adjusted the vision of the project to the plans of AWE.

Week 3 – 18 October
What I primarily concentrated on this week was threat analysis and report writing. While trying to offer help in coding tasks, I managed to get desynchronized, as other team members had already started coding. So, playing catch up turned out to be a lengthy exercise. Therefore, I focused on project documentation by threat analyzing and writing relevant sections of the report. As a team, we had discussions that aimed to assess the status of the project items such as TCP functionality, heartbeat mechanisms, and camera integration development. I also aided in the synchronisation of the group work with the Gantt chart, assisting to plan subsequent actions.

Week 4 – 25 October
Threat analysis was what I started research on in the previous week, and this week I drew up notable documentation that outlines the types of attacks that our system is able to withstand while also determining weaknesses it has. In a bid to ensure my analysis is in sync with the project development, I spoke to some of the team members involved with the coding and sought to find out their satisfaction or dissatisfaction with the current stage of the system. I gathered such insights and conducted an in-depth analysis of the system and indicated current issues from the two perspectives. For each of the faults that I found, I suggested some of the solutions using other models or looking for solutions on the internet. Doing so averts a deviation from the overall team strategy and maintains the integrity of the project design.

Week 5 - 1st November
This week, I refined the overall system design and explored potential solutions to improve security and functionality. I revisited earlier ideas and attempted to apply them to the current stage of the project. However, some approaches did not yield the expected

results, prompting me to explore alternative methods and collaborate with team members for additional insights. Although progress was incremental, these efforts identified areas for improvement and informed the direction for future work. I also contributed to discussions on aligning the technical implementation with the broader project objectives, ensuring that our approach remains robust and adaptable.

Week 6 - 8th November
This week, my primary focus was preparing for the upcoming presentation to our supervisor and second supervisor. I was tasked with researching existing solutions similar to our project, which aligned with my ongoing work on threat analysis. My role involved identifying systems designed to address similar problems, analysing their approaches, and uncovering any flaws or limitations they presented. This research aimed to ensure our project would avoid these pitfalls and incorporate more robust solutions. Additionally, I contributed to team discussions about cryptography, data protection, and camera feed integration. These insights were incorporated into the presentation, where I addressed the shortcomings of existing solutions. This week provided an opportunity to align my research with the project's goals and strengthen our presentation for next week.

Week 7 - 15th November
This week was dedicated to preparing and rehearsing for our group presentation. My efforts focused on refining the content to effectively communicate the project's progress and highlighting the research I conducted on existing solutions and their flaws. I participated in team rehearsals, working collaboratively to fine-tune the delivery and address feedback to ensure a polished final presentation. This week was crucial in presenting a cohesive overview of the project and aligning the team's understanding of goals and challenges moving forward.

Week 8 - 22nd November
This week, I built on previous research and applied insights gained in earlier weeks to enhance the project. Specifically, I explored potential improvements to the security framework, particularly through redactable signatures, and evaluated their feasibility for our system. While experimenting with approaches such as analysing computational efficiency and integration possibilities, the outcomes were inconclusive, and none provided a fully viable solution. Additionally, I reviewed hardware security module options and evaluated their potential to improve the project's security features. This included researching devices like Zymkey for tamper detection and cryptographic operations, although practical limitations posed challenges to immediate implementation. Despite these setbacks, this week deepened my understanding of the project's complexities and highlighted areas for further development in the coming weeks.

Week 9 - 29th November
This week was productive as we upgraded our hardware to meet the project's computational requirements. Due to insufficient performance from the Pi Zero, we transitioned to the Pi 3 and Pi 4 models. I contributed my personal Pi 3 to the project, while the team purchased a Pi 4, working within budget constraints. To further support progress, I took on additional responsibilities by assisting on the hardware side. I began designing a 3D-printed enclosure for the system and dedicated time to learning Fusion 360 to complete the task effectively. My involvement included adapting the enclosure design to

fit the upgraded hardware and ensuring it could accommodate future adjustments. I collaborated with team members to finalise the box design, which is set to be printed soon. Additionally, I started outlining key sections of my individual report. Despite challenges, this week marked significant strides toward improving the system's functionality while preparing for upcoming milestones such as lab camera testing and updating AWE on our progress.

Week 10 - 6th December
This week, I focused on mastering Fusion 360 to finalise the enclosure for our project. I dedicated significant time to refining my skills, ensuring the design met technical requirements and addressed feedback from the team and supervisor. I also contributed to discussions on optimising the placement of electronic components within the enclosure for proper functionality. By the end of the week, I completed the design and had it 3D printed. The process involved multiple iterations based on feedback, which improved the final product. I was particularly satisfied that the design perfectly accommodated the electronics, marking a significant milestone in the project's hardware development. This week's efforts advanced the project toward a fully functional prototype while strengthening my design skills.

Week 11 - 13th December
This week, my primary focus was writing the individual report and contributing to the group report. I also addressed minor adjustments required for the 3D-printed enclosure. The design was modified to accommodate a new battery, which did not fit in the original box, and to improve ventilation by adding a grill and a mechanism for an exhaust fan. Although the fan design was successfully implemented, it was not integrated by the hardware team due to the complexity of the electronics and limited time remaining. Nonetheless, I was satisfied with the progress, as the updated enclosure design addressed most hardware requirements. This week balanced reporting tasks and design refinements, contributing to both documentation and hardware improvement.

B Attack Threat Model

Threat Report on Secure Data Management for a CCTV System

January 20, 2025

1 Overview

This report details the security threat analysis for a secure video feed system that transmits footage from authenticated cameras to a home server, with an intermediate foreign server. The system uses OpenSSL, TLS, and digital signatures to ensure data authenticity, confidentiality, and integrity throughout transmission and storage. The report covers potential threats, associated risks, and mitigation strategies to strengthen system security and minimize vulnerabilities.

2 System Security Objectives

- **Mutual Authentication**: Authenticate cameras and servers to prevent unauthorized devices from connecting, primarily to the home server.
- **Data Integrity**: Ensure that transmitted video footage is free from tampering.
- **Confidentiality**: Protect video footage from unauthorized access or interception.

3 Key Security Components

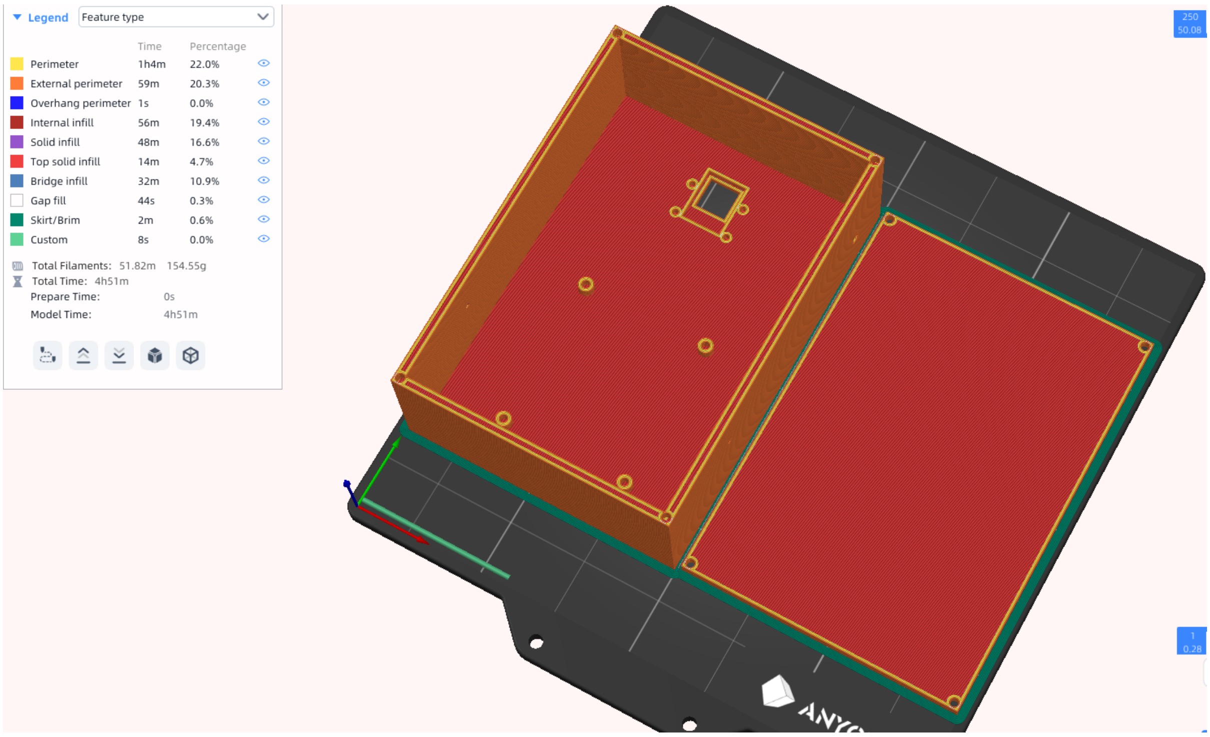
- **Digital Signatures**: Used to authenticate and verify the integrity of video data at the source (camera).
- **TLS Encryption**: Protects all communications between the cameras, foreign server, and the home server, ensuring secure end-to-end transit.
- **Timestamping and Sequence Numbers**: Prevent replay attacks by embedding timestamps in video packets, validated by the server.

4 Identified Threats and Mitigations

Threat	**Description**	**Likelihood**	**Impact**	**Mitigation Strategies**
Private Key Compromise (Camera/Server)	If the private key generation protocol on a camera or server is compromised, attackers could authenticate false data or decrypt footage.	Medium	High	Store private keys in secure hardware (TEE/TPM) and implement regular key rotation policies to limit key exposure risk.
Insider Threat on Foreign Server	Foreign server insiders could misuse access to video feeds.	Medium	High	Encrypt data in transit from the foreign server to the home server.

Side-Channel Attacks	Side-channel attacks aimed at extracting private keys from camera hardware via timing or power analysis.	Low	High	Use cryptographic libraries with side-channel resistance and store keys in TEE/TPM. Perform sensitive operations in secure hardware.
Denial of Service (DoS) Attack	Attackers flood the server or network, disrupting video feed transmission or storage.	Medium	Medium	Implement rate limiting and monitor traffic patterns to detect and mitigate DoS attacks, especially on the home server.

C Hardware Design File



Legend: Feature type

		Time	Percentage
🟨	Perimeter	1h4m	22.0%
🟧	External perimeter	59m	20.3%
🟦	Overhang perimeter	1s	0.0%
🟥	Internal infill	56m	19.4%
🟪	Solid infill	48m	16.6%
🟥	Top solid infill	14m	4.7%
🟦	Bridge infill	32m	10.9%
⬜	Gap fill	44s	0.3%
🟩	Skirt/Brim	2m	0.6%
🟩	Custom	8s	0.0%

Total Filaments: 51.82m 154.55g

Total Time: 4h51m

Prepare Time: 0s

Model Time: 4h51m

Figure 4: Slicer visualisation showing filament usage, printing time, and the internal structure of the model.