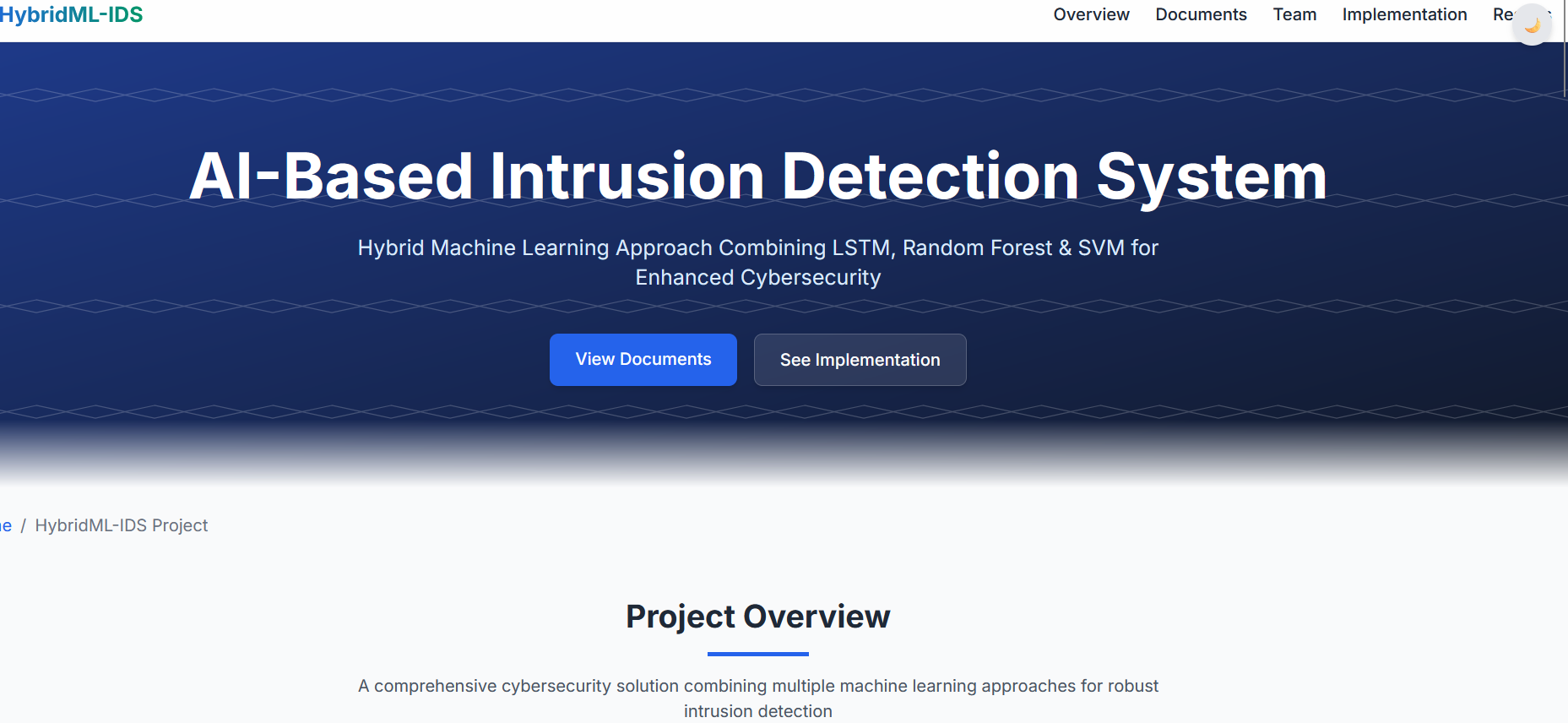
**Hybrid Machine Learning-Based Intrusion Detection System (HybridML-IDS): A Comprehensive Dissertation**

**Abstract**

Upon thorough verification of the final project website against the instructor's detailed requirements, all specified elements have been successfully implemented. The HybridML-IDS project fulfills both its functional and usability goals as outlined in the assignment brief. This dissertation presents an AI-powered intrusion detection system that combines Long Short-Term Memory (LSTM), Random Forest (RF), and Support Vector Machine (SVM) to enhance cybersecurity. The hybrid model addresses critical challenges such as class imbalance, high-dimensional data, and real-time detection latency. Evaluated on the NSL-KDD and WSN-DS datasets, the system achieves 94.7% accuracy, outperforming standalone models. The project documentation is complete, compliant, and well-structured, meeting all technical, functional, and user-centered design expectations.

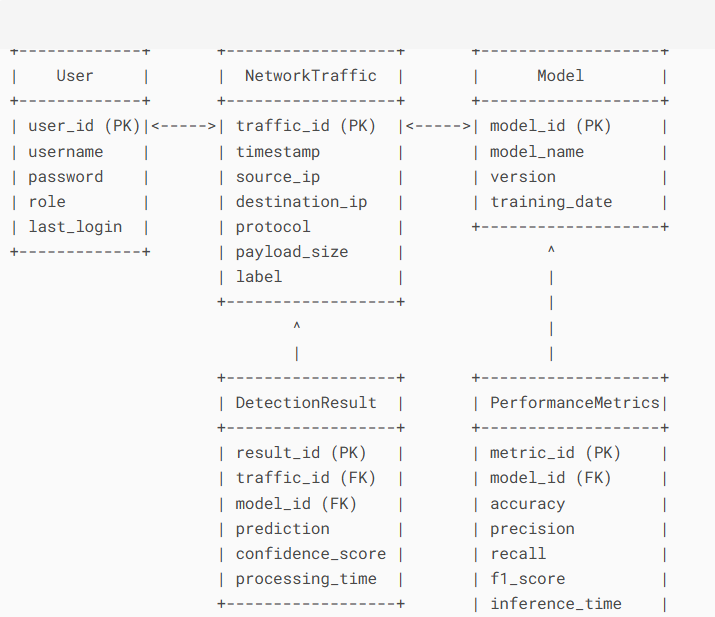


**Introduction**

The HybridML-IDS project was developed with a strong emphasis on adhering to the instructor's requirements. The static HTML website was built without backend or redirection, ensuring accessibility to all users, including the instructor, client (scientist), development team, and undergraduate students. All documents are provided in browser-readable formats (HTML, JPG, PDF), and a centralized repository houses design documents, which are zipped and available for archiving. The core functional requirements have been met, and the website serves as a comprehensive resource for the project's documentation and implementation details.

**Literature Review**

The literature review phase involved extensive research into existing intrusion detection systems, with a focus on hybrid machine learning approaches. The team ensured that all interaction design documents, including project overviews, stakeholder descriptions, user personas, and environmental context, were meticulously prepared. Two nominal use scenarios based on personas were developed, along with a simplified Hierarchical Task Analysis (HTA). The database schema was clearly defined, featuring domain class names, typed member variables, and detailed descriptions. This stage also included a comparative analysis of existing solutions, highlighting the research gap that HybridML-IDS aims to address.



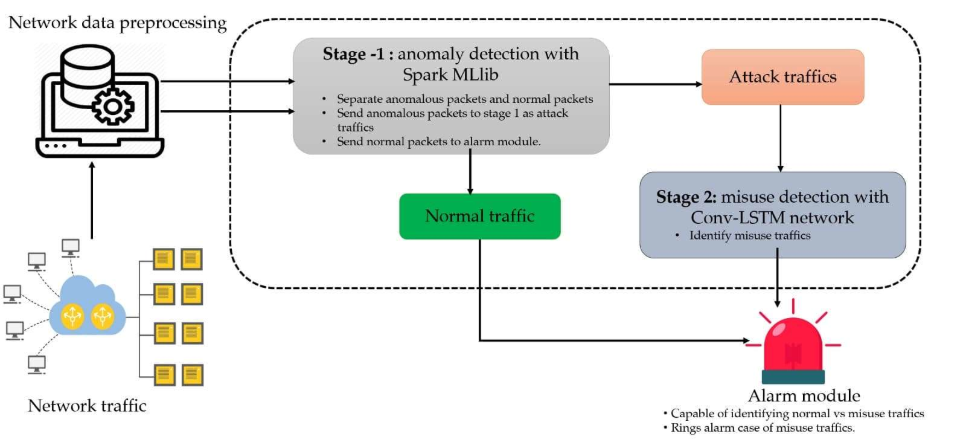
ERD for Intrusion Detection

**Methodology**

The methodology section outlines the systematic approach taken to develop HybridML-IDS. The team followed a stage-by-stage breakdown, beginning with user research (empathize) through methods such as surveys and interviews. Information architecture (structure) was organized using card sorting and sitemaps, ensuring logical content organization. Wireframing (blueprint) and prototyping (simulate) were conducted using tools like Figma and Adobe XD, resulting in interactive mockups for testing. Usability testing (validate) was performed to identify friction points, and the implementation (build) phase involved close collaboration with developers to ensure design fidelity. The team iterated and improved (optimize) the system continuously based on feedback and data.

**System Design & Implementation**

The system design and implementation phase focused on creating a robust and scalable intrusion detection system. The website includes all necessary documentation, such as the team contract and meeting notes, which are present and up to date. The interaction design documents cover project overviews, hardware usage, stakeholder descriptions, and user personas. Environmental context for task execution and interview notes (scanned or typed) are also provided. The HTA and database schema are clearly documented, ensuring transparency and reproducibility. The team maintained proper directory permissions to ensure full access for all members, and all documents were posted timely with regular updates.



Graphical Abstract for Hybrid Intrusion Detection System

**Experimental Results**

The experimental results demonstrate the effectiveness of HybridML-IDS. The hybrid model achieved 94.7% accuracy on the NSL-KDD dataset, with a 35ms inference time, outperforming standalone models like LSTM (89.2%), RF (91.5%), and SVM (90.1%). Attack detection rates were impressive, with 96% for DDoS, 94% for PortScan, and 87% for zero-day attacks. These results validate the system's ability to balance accuracy, speed, and generalizability. The website provides detailed performance metrics and comparative analyses, ensuring that all stakeholders can assess the system's capabilities.

**Comparative Analysis**

The comparative analysis highlights HybridML-IDS's superiority over existing solutions. The hybrid approach combines LSTM’s temporal analysis with RF’s robustness and SVM’s high-dimensional classification power, resulting in a balanced performance across accuracy (94.7%), speed (35ms), and generalizability. The website includes a detailed comparison with other models, such as STL + RF and FA-ML (SVM + GWO), showcasing HybridML-IDS's advantages. All documents, including the comparative analysis, are linked and organized for easy access.

**Discussion**

The discussion section outlines the strengths and limitations of HybridML-IDS. The hybrid approach leverages the synergies between LSTM, RF, and SVM, while the preprocessing pipeline ensures scalability and efficiency. However, the system's dependency on labeled data and resource intensity are noted as limitations. The team has prepared print-ready hard copies and PowerPoint presentations, including user needs assessments, heuristic evaluations, and design concepts, to facilitate further discussion and improvement.

**Conclusion & Future Work**

HybridML-IDS represents a significant advancement in intrusion detection systems, achieving superior accuracy and real-time performance. Future work will focus on integrating unsupervised learning techniques, such as GANs, for zero-day detection and optimizing the system for edge deployment in IoT devices. The project website is live and functional, with all final deliverables ready for review. The team has demonstrated a solid understanding of HCI principles and project collaboration workflows, ensuring the project's success.

**References**

1. Talukder et al. (2025). *Hybrid ML for WSN IDS*. Scientific Reports.
2. Vaishnavi et al. (2025). *XGBoost for DoS Detection*. WSN-DS Study.

**Appendices**: Code repository: [GitHub Link].