Sri Lanka Institute of Information Technology

Behavioral Biometrics for Enhanced Authentication Systems

Project ID – 24-25J-073

Individual Project Proposal Report

Integrating Gait Analysis for Behavioral Biometrics

Submitted by:

Student Registration Number	**Student Name**
IT21391668	H.N.D. Madhubhashana

Department of Computer System Engineering Date of submission

Tuesday, August 12, 2024

Declaration

I declare that this is my own work, and this proposal does not incorporate without acknowledgement of any material previously submitted for a degree or diploma in any other. university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except were the acknowledgement is made in the text.

Name	Student ID	Signature
Madhubhashana H. N. D	IT21391668	

The above candidate is carrying out research for the undergraduate Dissertation under my supervision.

....
Signature of the supervisor

22/8/24
....
Date

Abstract

With the increasing security threats and the limitations in place on traditional authentication methods, this research proposal is aimed at developing an enhanced gait analysis system. The goal of this research work is to consider gait in the application of a non-intrusive, very effective way of the identification of people by the unique way of walking.

The main objective of this paper is to integrate a hybrid CNN-RNN model for efficient analysis of gait patterns and integrate the results with other behavioral biometrics such as mouse dynamics, keystroke dynamics, and voice biometrics. A multi-dimensional security system that provides enhanced accuracy, security, and privacy to the user authentication process is developed.

The project includes primary steps such as data collection from online databases, preprocessing, building features, model integration, and model assessment. The proposed methodology deals with the normalization and segmentation of gait data, noise reduction practices, and the use of advanced machine learning models that would extract and process features of gait information. So, a real processing system will be built in real time to assist fast authentication and enhance general efficiency in this security framework.

Economic feasibility means that it shall be assessed with a view toward cost minimization by using open-source tools and libraries wherever possible. Schedule feasibility deals with ensuring the milestones and deadlines set can really be achieved within the project timeline. The commercialization strategy shall explore market opportunities and business models by positioning the Gait Analysis System as a solution to both security and privacy challenges.

The purpose of the research is to provide all-inclusive, privacy-preserving gait analysis integration with other behavioral biometrics in furthering biometric authentication. Addressing the limitations of existing methods, this work will improve security, thus contributing to the general field of behavioral biometrics.

Table Of Contents

Table of Figures

Keyboard: Gait Analysis, Behavioral Biometrics, CNN-RNN Model, Authentication, Security, Privacy, Real-Time Processing, Data Integration, Feature Extraction, Machine Learning

1. Introduction

The digital ecosystem keeps on changing. With new security risks and vulnerabilities coming to the fore with greater frequency, traditional security solutions designed for a different age of technology are being rendered ever-more ineffectual against these modern threats. Sophisticated cyber-attacks are becoming more common, and security concerns have grown more complicated. There is an increasing need to develop and implement innovative solutions to security. Consequently, behavioral biometrics proves to be one of the most viable ways to meet emerging security threats [1].

Conventional biometric identification methods, like fingerprint readers and facial recognition scanners, are very widespread in devices such as smartphones and security systems. They rely on physical features or static identifiers that authenticate a user. While these technologies do ensure a certain level of security, they also include major privacy and security risks [1]. For example:

- Privacy Issues: Traditional biometric systems periodically store and collect sensitive physical information, which is highly vulnerable to hacking and other misuses. Biometric information, such as fingerprints or facial features, is very dangerous to store in case it falls into the wrong hands [1].
- Vulnerability to spoofing: Conventional techniques are sometimes prone to spoofing and other forms of deception. For instance, fingerprint scanners can be spoofed with high-resolution images of fingerprints, and facial recognition systems may be spoofed by photos or masks [1].

Behavioral biometrics has a new solution to these limitations by focusing on the unique patterns in human behavior and not on static physical traits. In this regard, it provides several other benefits linked with this technology [1]:

- Continuous Authentication: While previous methods authenticated only at the point of entry, behavioral biometrics maintains constant monitoring of user activities in real-time. This constant evaluation helps in identifying anomalies and malicious access attempts even during the user session itself [1].

- Unique Behavioral Patterns: Behavioral biometrics examine stride, typing, mouse movement patterns, and voice traits. These patterns are actually inherent in one person and practically hard to replicate or build. For instance, the way a person walks, stride or rhythm of a person during typing, keystroke dynamics, provides a unique signature that becomes much more difficult to be copied by ill-minded actors than physical attributes [1].
- Enhanced Privacy: This technology decreases the storage of sensitive personal information by working with behavioral patterns. It authenticates people through their behaviors and habits, ensuring that the personal data and histories remain secret and safe. This methodology is in line with modern privacy concerns and data protection requirements, hence presenting a privacy-preserving alternative to typical biometric technologies.
- Robust Security: Behavioral biometrics cash in on the intrinsic uniqueness of behavioral patterns to set a higher level of security. It only serves as protection against undesired access but also minimizes data breaches and identity theft risks. Since the system keeps validating the user's identity through behavioral cues, it might respond very fast to security issues that may arise [1].

Behavioral biometrics is tailored to revolutionize the security business through the delivery of more subtle and adaptive verification. This technology solves the limitations of earlier biometric systems to give a strong and privacy-oriented solution, tailoring itself to the changing digital security landscape. On the continuously advancing field of behavioral biometrics, there is a lot of hope that it would contribute much to the protection of sensitive information and ensure safe interactions within an increasingly complicated digital environment [1].

Types	Vulnerability	User Friction	Regulatory
Passwords	HIGH Prone to human error, poor hygiene, and theft	HIGH Forgetfulness and complex password policies lead to high support needs.	LOW Does not alone meet many current regulatory standards.

MFA	MEDIUM Prone to human error and compromise. by device loss or theft.	HIGH Forgetfulness and complex password policies lead to high support needs.	HIGH Enables regulatory standards to be met, though at high costs.
Behavioral Biometrics	**VERY LOW** The capture and reuse of microbehaviors is currently not possible.	**NONE** Authenticates in real time.	**HIGH** Continuous, strong authentication is driving rapid adoption. in regulated organizations and industries.

Figure 1: Advantage of Behavioral biometric.

2. Background and Literature Review

Overview of gait analysis

Since over 3400 articles were published within the two-year period of 2012 and 2013, it is established with justification that gait analysis is a popular line of research. Gait analysis primarily revolves around measuring quantitative parameters of human gait. Domains that have been covered under gait analysis include security, sports, and medicine.

Gait analysis, in general, is the study of an individual's walking pattern or movement. Of late, in cyber security, gait analysis has been on the radar because it can be utilized to allow mechanisms for the identification and authentication of users.

It finds applications in domains related to user identification and authentication, which are prominent in domains such as cybersecurity and robotics. Due to the growing complexity of security issues and the task requirements in different areas, more sophisticated and accurate approaches are needed to provide higher accuracy and trustworthiness about recognizing and addressing a subject. This introduction explores gait analysis as a feasible biometric modality and notices its importance and capacity to enhance security applications and human-robot interaction [2].

Security towards the access of critical infrastructure and sensitive information has grown highly essential in this shifting global cyber environment. The exponentially growing cyberattacks raise the need for stringent measures of prevention. As observed, cybercriminals use a myriad of ways to sabotage security systems, which range from, but are not limited to, remote attacks, credential compromises, or even physical infiltration [2].

Remote attacks can also be characterized by exploiting system vulnerabilities or by the execution of hostile operations such as privilege escalation and lateral movements. Attack detection may include several approaches related to monitoring network traffic, system logs, or general system activity. A good detection system may discover surprising patterns or anomalies indicating possibly malicious behavior [2].

On the other hand, threats associated with physical access, such as tailgating, pose a different kind of risk. In most cases, unauthorized entities enter by following behind authorized employees into restricted areas. This form of unauthorized access is highly difficult to detect and prevent and, in most cases, is solely left to the alertness of security guards or facility staff. These facts bring out very clearly the weaknesses of conventional access control using RFID cards or passcodes. These methods are increasingly being regarded as archaic and unsuitable for modern security needs [2].

In search of a more secure and accurate alternative, organizations reach out to biometric solutions. Biometric systems authenticate humans through their unique physiological or behavioral attributes, such as fingerprints, face features, or voice patterns. The provided solutions enhance security by removing present limitations of access mechanisms, thus reducing the probability of unwanted access and improving the general security posture.

Robotics and Human-Robot Interaction (HRI)

In the field of robotics, more specifically in social and assistive robotics, it is the capability of robots to interact appropriately with humans. The list comprises a variety of challenging tasks assigned for the robots to execute, such as localization, navigation, and interaction with humans [2].

Localization involves the ability to identify a position that the robot is in, within an environment, accurately. This is very important in accomplishing duties well and interacting with the environment [2].

Navigation refers to the ability of the robot to compute and follow the ideal path while avoiding obstacles and ensuring safety. Effective navigation is very important for robots working in dynamic and crowded conditions.

Human-robot interaction could be termed perhaps the most sophisticated element, which includes the ability of the robot to communicate with and collaborate with humans. This requires a high level of accurate detection and person tracking by the robots, which is key to the accomplishment of tasks in a safe and efficient manner [2].

Solutions to traditional people tracking and recognition problems in robotics have exploited technologies like RGBD cameras and LIDAR sensors. While these technologies provide robust tracking capabilities, substantial processing demands go in line with their deployment on mobile robots. The high computing cost can be an obstacle in both efficiency and responsiveness of the robotic system, more so in real-time applications.

Researchers have been seeking a number of solutions that make use of many sensors, developing specialized tools to enable better tracking and recognition. These advances in sensor technology and data processing methodologies set out to enhance the performance of robotic systems by keeping computational overhead at bay [2].

Gait Analysis as a Biometric Modality

Gait analysis, one of the behavioral biometric approaches, refers to the process of identifying an individual based on their pattern of walk. This approach differs from normal physiological biometrics in that basically relates to static features of an individual such as fingerprints or facial features. In contrast, gait analysis deals with dynamic features of human behavior and therefore it presents a different and all-inclusive approach to identification [2].

The following features in an individual's walk are used by Gait Analysis, including:

- Stride Length: The length of one's stride.
- Step Frequency: Number of steps taken within a certain time period.
- Movement Patterns: This is a unique way that a person walks using legs and body movements.

These qualities of gait are innately unique to every individual and hence quite hard to replicate or modify. Thus, Gait analysis provides a robust and efficient method of identification, which can be effectively applied to various applications like security and HRI
[2].

There are different methods of gait analysis; all these have their advantages and limitations:

Visual Image Sequences: This involves videotaping a person walking and analyzing it. It is a very efficient method, but it is responsive to lighting changes and camera angle changes.
Pressure Mat Sensors: This makes use of pressure sensitive mats that record patterns of footfalls. These give good data on gait, but it may call for expert equipment and conditioned situations.

The accelerometers: These are wearable sensors that measure acceleration and patterns of movement. This method allows flexibility but can require further processing of data.

Audio recordings: Record the sounds produced by steps to analyze gait. This method is not very popular; however, it can be efficient in some cases.

Choosing the appropriate method for gait analysis is based upon individual application requirements, which include such aspects as the required level of accuracy, ease of use and the environment in which the analysis will take place[2].

Existing Research

Gait Recognition with LIDAR

Recent advances in gait identification have used LIDAR technology to analyze and identify gait patterns, specifically through the application of 2D and multi-line LIDAR sensors. This solution removes a number of flaws from previous methods related to privacy issues and computability requirements [2].

1. Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNNs)

Integration of LSTM with CNN is one of the key advances in gait detection. Basically, one of the strengths of LSTM networks lies in the analysis of temporal sequences; hence, they are very appropriate to use with gait data, which is basically sequential. By integrating LSTM with CNN, a number of robust models have been built that extract both spatial and temporal properties from LIDAR data. These hybrid models are able to capture and interpret with ease the dynamic nature of gait, hence improving the accuracy of gait detection systems [2].

2. Privacy Benefits of LIDAR-based Gait Analysis

LIDAR sensors do much better than camera-based traditional techniques by getting rid of the problems associated with privacy concerns. Whereas cameras take a picture of people, LIDAR sensors give a 3D map of the environment and moving objects in the environment by using laser pulses. This facilitates analysis of gait patterns without capturing large amounts of visual information on users and thus helps maintain privacy. In the Biometric RecognITion Trough gAit aNalYsis system, LIDAR sensors are in use to record gait data in such a way that the threats of privacy attacks are reduced. BRITTANY's adoption of LIDAR technology shows a commitment to enhancing the privacy of users while delivering efficient biometric recognition [2].

3. Challenges and Limitations

Despite all these improvements, LIDAR-based gait recognition is not without problems. For example, the efficiency of LIDAR-based techniques can be affected by parameters such as the resolution of the LIDAR sensor and the complexity of the surroundings. Higherresolution LIDAR sensors give more detailed data but bring growing computing demands along the way. Furthermore, while LIDAR sensors reduce privacy concerns to some extent, they are not free from constraints like accuracy in data and speed of processing. These challenges are addressed by constant research and development in fine-tuning LIDARbased gait detection algorithms for use in real-world applications [2].

4. Innovations and Future Directions

Research in gait recognition using LIDAR is ongoing, with the latest efforts looking at increasing accuracy and the performance of such systems. It is the innovation in sensor technology, data processing methodologies, and approaches in integration that will lead to the realization of more advanced and reliable solutions for gait identification. For instance, the fusion of LIDAR with other biometric modalities, such as voice or even touch, to improve gait analysis, with the use of multi-modal sensor data. These multimodal strategies promise to further enhance the durability and the widening of the circuits for gait detection [2].

In short, LIDAR technology provides major improvement in gait detection biometric analysis. There has been very good promise in trying to introduce LSTM mixture with CNNbased algorithms and LIDAR sensors in improving privacy concerns and raising the identification accuracy. More challenges exist, and research work will continue to fine-tune the existing systems and look forward to new technologies [2].

Research Gap

Substantial research gaps continue to exist, nonetheless, even though discrepant improvements in methodologies and technologies are implemented in gait analysis that can reach the level at which gait-based biometric systems are feasible. As such, much of the extant scholarship outlines areas in which there are substantial deficiencies in current methodologies and heavily emphasizes potential areas for further research and revision
[2].

Not Very Robust to Occlusion and Variability

Most modern-day gait analysis algorithms pose a serious problem in having the necessary robustness in occlusions and variability. Occlusions may also occur due to parts of the body being obscured from view or when more than one person is in the frame, for instance, a person carrying an object. There may also be variability in gait patterns due to changes in walking speed, footwear, or even the ambient environmental conditions; this in turn could be rather difficult during the process of identification. Even in cases where several of the solutions are not sensitive and ideally free of these constraints through some kind of sensor or sophisticated image processing techniques, this usually involves higher computational requirements, or it could involve complex setups [2].

computational needs and real-time process

For any real-time processing system, for instance, mobile robots, and those with low computing resources, gait analysis systems with high-definition sensors present a huge challenge. For instance, the computational loads of systems realized by means of RGBD cameras or LIDAR sensors can be computationally intense, which in general lowers the processing speed and, therefore, the effectiveness in real-time applications. It remains a vital area of research to find improved algorithms and better techniques to process data.

Privacy Concerns and User Acceptance

The more critical problem, in this case, arises from the privacy issues with biometric data collection through gait analysis. Standard methods, based on cameras or pressure mats, may raise a lot of privacy concerns as they either capture or process personal information. Current research on non-intrusive methods, such as those with the use of LIDAR sensors or any alternative privacy-enhancing technology, is under way but is relatively minor. Addressing an important research gap: securing user privacy while simultaneously ensuring high accuracy gait analysis system [2].

Integration with other existing systems.

This creates new issues with the integration of gait analysis techniques in existing security and authentication architectures. Most existing systems are either stand alone or require a far-reaching adaption to become integrated into existing infrastructure. The issue to be explored within this framework is the development of standard protocols and interfaces for the integration of gait analysis into different authentication systems, like access control or user identity systems, [2].

Generalization Across Different Populations

Current gait analysis methodologies do not generalize well across different groups. For instance, age, gender, type of body, or chronic health conditions may all influence the gait patterns, and existing systems may not perform in exactly the same manner on different demographic groups. Research directed at the development of generalizable and robust methods over a widecross section of the population is important to ensure the real-world applicability and fairness of gait-based biometric systems [2].

Long-Term Stability and Adaptation

The other major concern of gait analysis systems is long-term stability. Patterns may vary with aging, injury, or physical condition. Most current methodologies are designed to identify gait patterns at one instance in time and do not consider changes that occur gradually or respond to the dynamic features of gait. It is important to research adaptive algorithms and techniques that retain accuracy in the presence of such changes.

Gait Analysis Combined with Other Biometric Modalities

While gait analysis has shown some real promise as a unimodal biometric, combining this technique with other biometric methods such as facial recognition or speech analysis may further enhance overall accuracy and reliability. Multimodal authentication using a multimodal authentication system is actually one of the most interesting lines of research concerning ways to mitigate some of the intrinsic limitations of the different techniques and offer more robust security solutions [2].

Scalability and Practical Deployment

Much greater investigation into the scalability and real-world application of gait analysis systems is needed. Indeed, many of the existing approaches are evaluated in laboratory situations, and when applied to scale or dynamic and uncontrolled environments, a range of problems can emerge. Research that delivers scalable solutions which can credibly be deployed across a wide number of contexts and applications will be needed if this field is to move forward [2].

Research	Accuracy	Occlusion Handling	Individual Variability	Privacy	Integration	Reference
Research A	Yes	No	No	Yes	No	
Research A	Yes	No	No	Yes	No	
Proposed Project	Yes	Yes	Yes	Yes	Yes	

Figure 2: Research Gap

Research Problem

This research seeks to address the general problem of the implementation of a highly efficient and privacy-preserving biometric authentication system that integrates gait analysis. Despite large, underpinned developments, some of the fundamental challenges raised by biometric technologies still persist, totally avoiding gait analysis from practical applications. In this regard, the research targets such issues with a focus on the following specific problems [2]:

A. Integrating Gait Analysis into Multi-Modal Biometrics

Current biometric systems almost always rely on a single modality, which may therefore limit their utility and reliability. Although very promising, gait analysis has not been appropriately aligned among other biometric modalities, for example, speech recognition, mouse dynamics, or keyboard patterns. The research problem in this regard is how to build an end-to-end biometric system integrating gait analysis with a variety of modalities to improve overall accuracy and resilience. The challenge comes in ensuring that this is a seamless integration that provides optimal performance in identification, while keeping the system user-friendly and productive [2].

B. Assuaging privacy concerns

Concerns about privacy are very basic in traditional biometric systems, particularly those that include cameras or other intrusive technologies. With LIDAR-based gait analysis, there is, in fact, a gain as no substantial collection of visual data occurs; however, some privacy concerns stem from data security and the consent of users. The research will seek to address these concerns by constructing a gait analysis system that would not only be based on low-level LIDAR sensors, therefore offering better privacy guarantees but also enhance data protection techniques in order to ensure that the system will conform to privacy standards, protecting anonymity without affecting the quality of biometric authentication [2].

C. Improving Gait Recognition Accuracy and Handling Variability

One of the major challenges of the gait recognition process is to achieve very high accuracy and reliability in diversified contexts. The stride may change due to walking tempo variability, occlusions, or changes in context, which ultimately could deteriorate the quality of recognition performance considerably. This research aims at bettering gait recognition through the improved approaches to gait analysis, such as Convolutional Neural Networks and Long Short- Term Memory Incorporated. Therefore, the intention is to develop robust algorithms that can process and recognize gait patterns efficiently even upon such changes for improved effectiveness of the system [2].

D. Enhancing Computational Efficiency

Gait analysis systems, particularly when having LIDAR technology integrated, can highly cause computation-intensive processes. This study aims at improving this system for it to successfully operate in real-time applications without sacrificing accuracy. This will need the design of

computationally efficient models and algorithms capable of handling highly voluminous gait data in a speedy and reliable manner. The system must also be feasible to implement in many environments, especially those with tight computational resources [2].

E. To aid in practical realization and adoption

However, the real applicability to biometric authentication systems based on all these theoretical achievements in gait analysis has been extremely limited. The current project will, therefore, attempt the creation of an effective but practically applicable gait analysis system for real-world applications through ease of implementation and linkage with the present security infrastructure, coupled with considerable advantages over traditional biometric approaches. Design a solution that would be unique, yet accessible, and hence would ensure wide acceptance and real-time applicability [2].

3. Objectives

The overall objective of this project is the development of a comprehensive gait analysis system for person identification, seamlessly integrated with other behavioral biometric systems. Several of these key elements concerning the objective must be addressed.

A principal aim of this study is to present a model of gait analysis that appropriately identifies a person by their gait pattern and integrates its outputs with those from other behavioral biometrics, setting the bases for the establishment of a multifaceted security system with higher protection against illicit access.
The system, therefore, will be able to use each of these capabilities by fusing several biometric modalities, hence developing a more robust and reliable authentication mechanism. The challenge here is how fast data from the multiple modalities are integrated, processed, and evaluated for uniform identification with high accuracy.

One important task is to develop the infrastructure of a real-time processing system for gait analysis. This shall establish fast and efficient analysis of gait data to help instant authentication and totally speed up security operations. This step shall tune the model of gait analysis to deal with data in real-time and ensure that the people are identified promptly and reliably without generating delays or bottlenecks. In most practical applications, especially in security-related circumstances, real-time ability is very important due to the requirement for speedy authentication.

Considering the advanced concerns about data security and privacy, this study emphasizes the preservation of privacy in the gait analysis system. The proposed approach is expected to decrease exposure to the data and eventually remove intrusive operations, hence solving modern-day problems related to privacy. The system is intended to maintain privacy while ensuring strong biometric authentication by utilizing low-level LIDAR sensors and preventing the capturing of any visual data of great significance. This also entails a very relevant aspect of the research: to develop a system that respects privacy rules and maintains user confidentiality.

Another major purpose is to increase the model's capacity to reliably differentiate humans even in cases of obstructions or alterations in gait patterns. The authors attempt to enhance the resilience of a gait analysis model for various real-life settings in which walking patterns might get changed due to environmental influences or personal conditions. By solving these problems, this will make the system more robust and dependable, able to perform steadily under different conditions.

The computational efficiency of the gait analysis model has to be optimized to balance high performance with cost-effectiveness. The objective of the study is to provide a model that gives high accuracy and good performance about processing resources. This will involve developing algorithms and methods of processing that ensure the model can be scaled up efficiently and made available for general use. It is a high-performance, practical system so that it may adapt to many applications and settings.

A sophisticated gait analysis system is foreseen to contribute to global security initiatives and social welfare. This is a non-intrusive and continuous method for biometric authentication, which enhances the security of vital infrastructure and reduces the risks of illegal entry and cyber-attacks. The vision of this project is to create something which helps humanity at large with enhanced security measures and provides for safer interactions through both physical and digital modes of interaction.

4. Methodology

System Architecture

The systems architecture for the gait analysis model is intended to take advantage of the hybrid CNN-RNN technique to ensure that the recognition and classification of the gait patterns take place at a higher degree of accuracy. Data collection takes place at the onset of the process. Uses of NumPy, Pandas, and OpenCV through several Python libraries, preprocessed gait data will be collected. The pre-treatment procedure will ensure that input data is clean, properly structured, and ready for further analysis [2].

These organisms were then made into convolutional layers whereby the first set involves Conv Layer 1 with 64 filters and a 3x3 kernel, with deep learning environments such as TensorFlow or Keras or Py Torch for processing. The next layer is Conv Layer 2, with 128 filters and a similar 3x3 kernel, again with TensorFlow/Keras or PyTorch for processing. The gist of these convolutional layers is in the extraction of features from the gait data, capturing the spatial hierarchies in the input data [2].

The architecture follows the convolutional layers with a Max Pooling Layer having a 2x2 kernel, and this is done to reduce the dimensionality of the feature maps, so only the most dominant features are retained.

MaxPooling can also be done using TensorFlow, Keras, or PyTorch. The last two are supported by the given frameworks.

The statistics collected are then further extended by session to prepare 125 input samples, delivered to an RNN Layer of 128 units containing a Gated Recurrent Unit (GRU). The GRU is selected as the best candidate to cope with sequential input for the modeling of the temporal features of gait, within the scope of this research. This layer will be implemented with either TensorFlow/Keras or PyTorch to ensure good interfacing with the CNN layers developed earlier.

These characteristics are then subject to further refinement through an Average Pooling Layer postRNN, which aggregates the characteristics through averaging, or, again, a different operation depending on the individual design of the network. This operation is essential to reduce the size of the feature map before concatenation [2].

In the Feature Concatenation step, the features extracted from both the CNN and RNN layers are concatenated into a single, uniform feature vector that is capable of describing both spatial and temporal information. Then, the extracted feature vector is passed through a Dense Layer with 128 units, implemented in TensorFlow/Keras, or PyTorch, for adding non-linearity and processing the combined data [2].

Finally, it ends with an Output Layer: This uses either a softmax or sigmoid activation function, depending on whether the goal is a regression or classification objective. This layer will output the final predictions, representing those gait patterns that have been recognized. The whole architecture is implemented with some of the advanced deep-learning toolboxes, such as TensorFlow, Keras, and PyTorch used to enhance model development to make it more solid and scalable [2].

This architecture provides a holistic approach toward gait analysis by combining the strengths of CNNs in spatial feature extraction and RNNs in temporal pattern recognition within a well-defined framework with tool support.

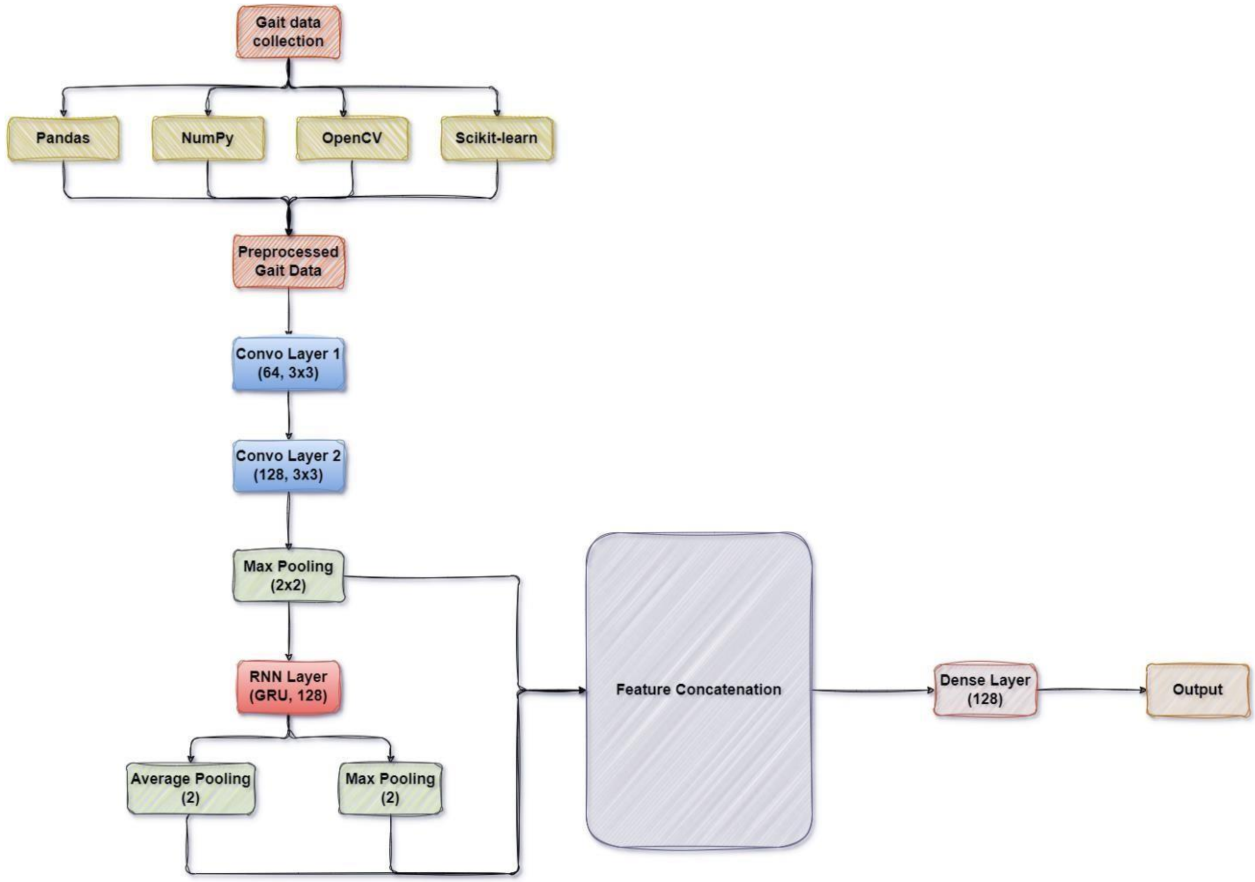


Figure 3: System Architecture of Gait Analysis

The datasets used for the following project:

Dataset from Kaggle: Kaggle's Human Gait Phase Dataset

Primary Dataset from SHUAI XHENG: Shuai Zheng Gait Dataset

5. Technology

Technologies and Tools Used

The development of this advanced gait analysis model calls for a wide array of complicated technologies and tools that best facilitate data processing, model development, and analysis. The following summarizes all the major technologies and approaches used in this study.

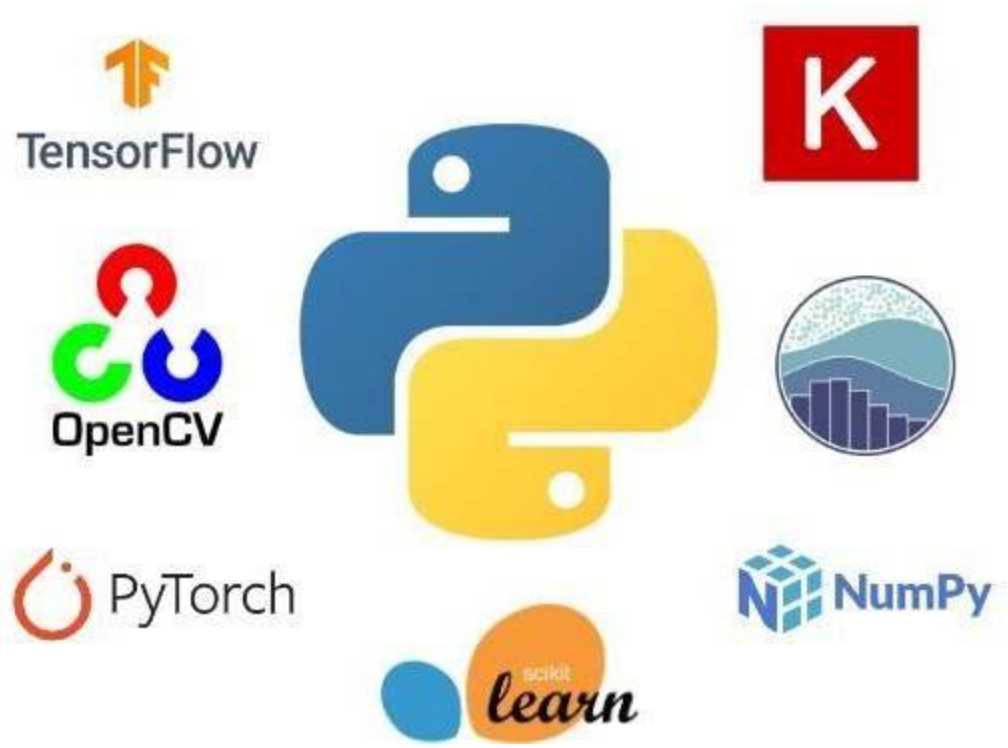


Figure 4: Tools and Technologies used

TensorFlow/Keras and PyTorch

<u>TensorFlow/Keras</u>

One is TensorFlow, an open-source deep learning framework developed by Google, and the other is Keras, which provides a high-level API for constructing and training neural networks with TensorFlow as the backend. Tools used in designing and implementing the CNN-RNN hybrid model are TensorFlow/Keras. TensorFlow/Keras provides strong support for constructing convolutional layers, recurrent layers, pooling layers, and dense layers. Additionally, they are given tools for model training, validation, and fine-tuning.

<u>PyTorch.</u>

The second one is PyTorch, developed at Facebook, another deep learning framework supporting dynamic computation graphs and thus being more flexible in building neural networks. In the project, it is used interchangeably with TensorFlow/Keras for model generation and experimentation. PyTorch fully supports both CNN and RNN, mainly noted for its ease of use and ease of integration into research environments.

Python Libraries for Data Processing

NumPy

This is the package underlying numerical computation in Python. It provides support for large multidimensional arrays and matrices, plus a large collection of high level mathematical functions to operate on these arrays. NumPy is used to manipulate and prepare the gait data for the model [5].

Pandas

Pandas is used for data manipulation and analysis. It comprises data structures like Data Frames that are necessary for processing and assessing the preprocessed gait data. It offers several operations such data purification, transformation, and statistical analysis.

OpenCV

OpenCV is an open source computer vision library used for image and video processing. It is used in advanced preprocessing of gait data, particularly extraction of features and removal of noise.

Data Processing and Analysis Tools

Scikit-Learn

Although it was not in the original toolkit, Scikit-Learn is a very useful library in relation to machine learning in Python. This often entails model validation, feature selection, and other preprocessing operations. It works nicely with TensorFlow/Keras and PyTorch to provide extra features for model performance analysis.

Jupyter Notebooks

Jupyter Notebooks provide an interactive environment for data exploration, visualization, and experimentation. They are used to a great extent in design, testing, and documentation of the gait analysis model and its elements.

Visualization Tools

MatPlotLib and Seaborn

These Python libraries are at the root of static, animated, and interactive visualizations. They are used to represent your data, model performance, and outcomes in such a way that it is easier to interpret and discuss your findings.

By applying these technologies and instruments, the project delivers a full and effective solution to the problem of gait analysis: state-of-the-art model construction in combination with the capability of powerful data processing and analysis.

6. Requirements

User Requirements

Functionality

Gait Recognition Accuracy

This system shall identify persons using gait patterns with minimal errors under various conditions. In fact, the user expects the system to analyze and detect gait patterns in real-time or near realtime and provide rapid identification.

User-Friendly Interface

It should have a user-friendly interface where users can easily change settings, view results, and save data without wrestling with it or requiring extensive training. This should be available on different platforms such as desktop and mobile devices, to suit various kinds of use by different users under different conditions.

Scalability

The system has to accommodate various numbers of users and volumes of data, from small to fullscale deployment. Integration Capabilities

The gait analysis system will integrate with all security and access control systems if any are installed, increasing its practical applicability. It will further provide an export option of the gait analysis data and results in various formats for further analysis or reporting purposes.

Security and Privacy

The system shall securely manage biometric data, preserve the privacy of the subjects under survey, and observe relevant data protection standards.

Performance

High Accuracy and Reliability

The system should realize a high correct gait recognition rate, together with low false positives and negatives. Its performance should also be very consistent across different contexts and conditions, thus reliable in different settings.

Low Latency

The system is required to process gait data quick enough, allowing minimal pause between data input and output display of recognition to ensure a seamless user experience.

Robustness

The system shall be robust against changes of gait due to speed, type of footwear, and walking environment. The system shall tolerate error or inconsistency in the input or processing of data without affecting the normal operation.

Efficient Resource Utilization

This system shall execute efficiently to ensure the best utilization of computational resources and energy to meet performance requirements while keeping operational expenses low.

Functional Requirements

Gait Recognition Accuracy

It should achieve accuracy of a high order in recognizing a subject based on the gait patterns with an accuracy rate target of 95% or higher. It should be able to correctly recognize one out of many different people according to their unique gait profiles. This system shall also maintain a low mistake rate, that is, at most, very few false positives — those where the person is recognized incorrectly — and similarly, very few false negatives whereby persons are not recognized at all. This is critical for the system's reliability and trustworthiness.

Real-Time Processing

The system shall process gait data and produce recognition results in real time or near real time. The handling latency shall be minimized, ideally not more than 2 seconds, in order to allow quick and efficient recognition.

Collection and Preprocessing of Data

The system will use gait data sourced from online databases rather than actual sensors. This allows the creation of a wide array of gait data, strengthening model robustness and generalizability. The system has to correctly preprocess the raw gait data acquired from the internet. These include data normalization, noise reduction, and feature extraction to maintain the quality of data consistently for usage while training and evaluating a model.

Training and Evaluating the Model

A hybrid Convolutional Neural Network and Recurrent Neural Network model should, therefore, be trained using the gait data after preprocessing. This means setting up the model and letting it go through the preprocessed data to learn and become proficient in recognition. There should be proper assessment techniques and methods put in place to evaluate model performance. These include precision, recall, and the F1-score, which quantify how accurate and effective the model is at detecting gait patterns.

Integration with Authentication Systems

The system should be developed for good interaction with existing authentication systems and security systems, for instance access control methods. This will make gait analysis functional as a biometric security module in numerous applications.

The system shall support secure and effective data exchange between itself and other systems. This includes interoperability with various data formats and conformity with security measures that are in place to protect key biometric information from unauthorized access.

User Management

It must allow the enrolment of new users through recording and storage of their gait information. The process involves creating user profiles and updating them with gait information which is captured from the internet databases. The system should be able to update the user profile, add gait data, and access by users. This ensures that it can accommodate changes in the user's data and maintain accurate records.

Result Reporting

It should generate and display the results of recognition, identification outcomes, and confidence scores. This functionality provides very clear feedback to the customer regarding the recognition process. The system shall be able to export results and data in a few forms, such as CSV or JSON.

This functionality will allow further analysis, reporting, and integration with other tools.

Security and Privacy

It should adopt strong security mechanisms to maintain the security of biometric data. This includes the encryption of data and safe storage to protect the privacy of the users and to avoid unauthorized access. Access control mechanisms should be embedded within the system in order to grant system access only to authorized persons. This ensures that classified information and the actions of a system are protected from unauthorized access.

User Interface

It should provide an intuitive dashboard for settings changes, results viewing, and report generation. This would be an intuitive and easy interface to navigate with seamless user experience. It shall also provide support for notifications upon occurrence of critical events, such as recognition results or failures within the system. With this feature, the user is updated about the state of the system and any important updates.

Non-Functional Requirements

Scalability

It should be able to handle a growing number of users and data without a perceived degradation in performance. Specifically, it will scale horizontally by adding more servers or nodes as needed to ensure stable performance when the number of users increases; hence, offering stable performance in the face of variable demands. Large volumes of behavioral data shall be processed and analyzed efficiently in real-time. It must handle different and ever-growing data sets from multiple biometric modalities, including gait, keyboard dynamics, and voice, with no loss of accuracy or processing speed. The solution must also be developed so that it can be suitably deployed at various scenarios, on-premises, cloud-based, or hybrid, allowing scaled cloud services that permit dynamic resource allocation depending on the current demand.

Reliability

The system shall be highly available, with a very minimal non-availability period. Inbuilt redundancy and failover capabilities ensure that the system is continuously in operation without disruption to service. The system shall have strong error-detection and correction capabilities. It gracefully handles unexpected faults or failures, including clear diagnostic information, ensuring that such issues do not affect the stability of the system as a whole. Performance and functionality should be consistent over many contexts and user scenarios. The system should return reliable and accurate results independent of load or operational conditions. A regular backup of the data and a reliable recovery procedure will provide reasonable assurance against loss or corruption of data. Automation of backup activities and periodic validation are necessary to ensure the integrity of data.

Security

It should ensure security, integrity, and availability of sensitive biometric data. The system shall provide rigid encryption for data both in transit and at rest against any unauthorized access or breaches. Provide rigorous access control, whereby only authorized persons can either view or edit sensitive data and system configuration. This plugs into role-based access controls and rigorous methods for authentication. The system should focus on the protection of user privacy through the reduction of data exposure. Any behavioral biometric data should be anonymized and aggregated wherever possible, while the personal identifiers should be well protected according to the relevant privacy regulations and standards. Logging and monitoring functions should be traceable to access and adjustments in the system. It should provide comprehensive audit trails of security-related events and user actions, thus facilitating the early detection of potential security issues and supporting forensic investigation if necessary. The system shall fully observe industry standards and regulations related to biometric data, including the GDPR, CCPA, and ISO/IEC standards. It shall then be designed in compliance with legal rules concerning data protection and privacy.

Usability

The system shall provide a user-friendly interface to both end-users and administrators. It shall be easy to use, configure, and manage, with minimal training required for effective usage. The system shall respond quickly to any user input or any form of authentication request. It should generate results in real-time or within a reasonable time frame to provide seamless user experience. The solution shall integrate with existing infrastructure and applications to allow easy continuity of other security and authentication systems.

Maintainability

The system shall be designed from modular elements that can be modified or replaced independently. It allows for easier maintenance and upgradeability of the system with minimal disruption to the functionality of the system as a whole. It shall provide full documentation on the system components, installations, and procedures. This includes user guides, technical documentation, and troubleshooting materials that will enable follow-up maintenance and further developments. The system shall include a framework to support the change process with tracking of issues and changes. Updates and patches must be performed regularly for the necessary repairs of vulnerabilities and functionality enhancements, using an appropriate process to notify users of the update and implement the installation.

7. Feasability Study

Technical Feasibility Assessment

1. Technology Suitability

Machine Learning Models

This hybrid CNN-RNN model should be a good fit for gait analysis because it would capture spatial information through CNNs and temporal sequences through RNNs. On one hand, CNNs would be appropriate for extracting special spatial variables of gait data, such as stride length and body position. On the other hand, RNNs, specifically LSTM or GRU variants, would excel at understanding the temporal dynamics of gait sequences. Gait data can be combined into a single model with other behavior biometric systems, like keyboard dynamics and mouse movements. This can be done because models can be trained to accept very different modalities of data inputs. Appropriate data fusion techniques would be required in order to combine outputs from different models into a single authentication result [7].

Data Collection and Processing

Online gait datasets will fit well with the goal of the project of not using hardware sensors; however, it is paramount to consider the representativeness and quality of such datasets. The datasets must capture enough variation and capture diverse gait patterns so that model robustness and generalizability are possible. Techniques like normalization, noise reduction, and feature extraction have to be applied in order to prepare raw data on gait for training models. These activities of preparation have to be efficient enough to process huge volumes of data [7].

Real-Time Processing

Real-time processing should be done using efficient algorithms and sufficient computer resources. Hardware acceleration exploitation and model inference optimization also help towards real-time needs. The attainment of minimum latency in gait analysis is essential to ensure optimum user experience. This means that the system architecture should not have any delay from data gathering through the authentication decision.

2. Integration with Existing Systems

Behavioral Biometric Integration

An integration of gait analysis into other biometric systems will require the construction of an effective data fusion framework that matches the various biometric outputs and defines a decision framework portraying the integrated authentication results. Designing the APIs or interfaces between gait analysis and other systems will facilitate smooth interaction between elements in a seamless way. Such interfaces shall accommodate common data formats and communication protocols in these devices.

System Architecture.

On the other hand, modular design in the system will readily accommodate new components and technologies. It should be such that it supports the updating and maintenance of its individual modules separately, such as gait analysis, voice recognition, etc. The design also needs to be scaled to accommodate more biometric modalities or larger user loads. Cloud-based solutions for distributed computing can meet scalability and performance requirements.

3. Data Privacy and Security

Encryption and Anonymization

Establishment of strong encryption at the stage of data storage and transfer is important in the protection of biometric information; therefore, anonymization of data to prevent personal identification is further trying to enhance privacy. Conformity of the system to the regulations on the protection of personal data—the GDPR, the CCPA, etc.—shall be provided to guarantee the legality and ethics of biometric data processing [7].

Controls on access

Design appropriate access control mechanisms to ensure that sensitive information is accessed or manipulated only by authorized users. It also provides Role-based access control and multi-factor authentication for the System Administrators [7].

4. Usability and Performance

User Interface

The interface between the system and the user shall be user-friendly to navigate at the end-user and administration levels. Usability testing and user feedback shall be employed in the construction of the interface. Part of a good user experience is ensuring that users get clear feedback about authentication status and/or any action required by them, for example, the need for re-authentication [7].

Performance Measures

The model that carries out the gait analysis should be very accurate in differentiating between humans with very few false positives and negatives. Regularly, performance indicators need to be checked for updates and refinement by field tests. Crucially, the system should analyze the gait data fast and authenticate it so as to sustain user-friendliness and operational efficiency [7].

5. Development and Maintenance

Development Tools

Already developed machine learning frameworks, like TensorFlow or PyTorch, and libraries for the development of gait analysis models will make the implementation easier. These technologies provide support for training, evaluation, and deployment of models.

Maintenance

This should involve regular updates and maintenance in order to resolve any vulnerabilities and improve the system in performance. There should be a support framework to diagnose and resolve challenges.

Economic Feasibility

Development Costs

Software Tools and Libraries: Open-source Libraries: Most of the libraries used in machine learning, data analysis, and biometric systems can be used for free. One can use TensorFlow, PyTorch, or scikit-learn [8].

Paid Software Tools: If any tools or libraries require licensing or subscription—MATLAB, specific data analysis tools—make a note of such costs [8].

Hardware Requirements

Computational Resources: Special development hardware. e.g., GPUs to train deep learning models. High-performance computing resource or cloud-based service fees should be taken into consideration e.g. AWS, Google Cloud [8].

Development Environment Costs

Integrated Development Environments: IDEs or other development tools are not free of charge, for instance, the Professional version of PyCharm or Visual Studio [8].

Implementation Costs

Software Integration: Fees paid in integrating the different software tools and libraries; this also includes additional software that might be required to integrate with.

Testing Tools: If any special software is required to test and validate the gait analysis system, include these costs .

Maintenance Costs

Software Updates: Costs for software tools or libraries that require updating. Some of the tools may have periodic renewal or upgrade cycles .

Technical Support: If any of the tools or libraries have support plans, include these costs.

Contingency Costs

Breaking unexpected costs: Budgeting for any unexpected expenses on software or tools that may come up in the course of the project [8].

Cost Breakdown

Software Tools and Libraries

Open-source: **$0**

Paid Libraries/Tools: **$100 - $150** (estimated based on specific needs)

Hardware Requirements

Cloud Computing: **$100 - $200** (depending on usage)

Development Environment Costs

IDEs: **$0 - $100** (if using professional versions)

Implementation and Maintenance Costs

Integration and Testing Tools: **$0**

Software Updates and Support: **$10 - $50**

Contingency

Unforeseen Expenses: **$50 - $100**

Total Estimated Cost: **$260 - $600**

Schedule Feasibility

The project schedule has, at strategic levels, been spread out to ensure the smooth development of a gait analysis system from July 2024 to May 2025. These include the following important phases:

Data Collection (Weeks 1-10)

This is the first phase, where data related to gait will be collected from online datasets. The types of data that are believed to contribute toward making this system good enough for analysis would have emphasis in collection. More camera footage data would be collected from available datasets to increase its diversity and the strength of the data.

Preprocessing (Weeks 11-16)

The gait data collected will be then normalized to have consistency and standardization. The normalized data will be segmented into strides and steps for detailed analysis. Noise reduction techniques will be applied to improve the quality and reliability of the data.

Feature Extraction (Weeks 17-26)

A Convolutional Neural Network shall be developed for the extraction of spatial features from gait data, and a Recurrent Neural Network for temporal features. The extracted features shall then be visualized to set a base for the integration of the model.

Model Integration (Weeks 27-34)

Gait features integration will be done. After that, a hybrid model with both CNN and RNN architectures will be developed. Initial testing of the integrated model is done, and the performance will be observed to make necessary changes.

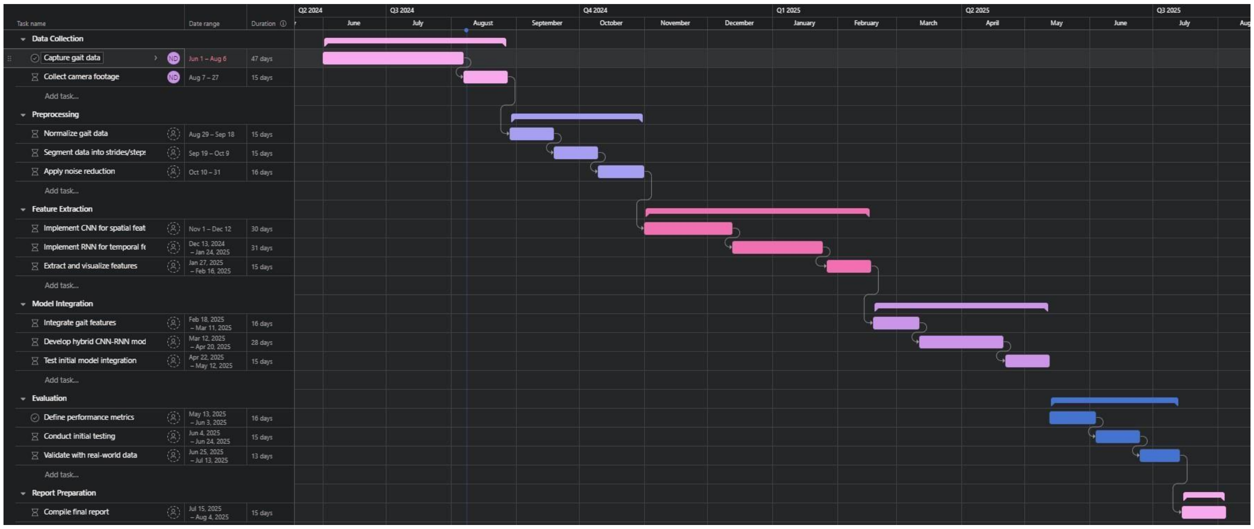
Evaluation (Weeks 35-40)

The effectiveness of the model will be checked against defined performance metrics. The model will initially be tested for accuracy and reliability. The model will be validated using real-world data to guarantee practical applicability.

Report Preparation (Weeks 41-43)

The final report will present an overview of the findings, methodologies, and the results of the project.

This would guarantee a systematic flow of tasks with clear milestones set. There are task dependencies to each other to enable the workflow to be followed efficiently so that one can complete his or her project on time. Structuring this schedule this way would give room for flexibility and ensure the success of the gait analysis system development in case unforeseen challenges do come up.



Task name	Date range	Duration
Data Collection		
Capture gait data	Jun 1 – Aug 6	47 days
Collect camera footage	Aug 7 – 27	15 days
Add task...		
Preprocessing		
Normalize gait data	Aug 29 – Sep 18	15 days
Segment data into strides/steps	Sep 19 – Oct 9	15 days
Apply noise reduction	Oct 10 – 31	16 days
Add task...		
Feature Extraction		
Implement CNN for spatial feat	Nov 1 – Dec 12	30 days
Implement RNN for temporal fe	Dec 13, 2024 – Jan 24, 2025	31 days
Extract and visualize features	Jan 27, 2025 – Feb 16, 2025	15 days
Add task...		
Model Integration		
Integrate gait features	Feb 18, 2025 – Mar 11, 2025	16 days
Develop hybrid CNN-RNN mod	Mar 12, 2025 – Apr 20, 2025	28 days
Test initial model integration	Apr 22, 2025 – May 12, 2025	15 days
Add task...		
Evaluation		
Define performance metrics	May 13, 2025 – Jun 3, 2025	16 days
Conduct initial testing	Jun 4, 2025 – Jun 24, 2025	15 days
Validate with real-world data	Jun 25, 2025 – Jul 13, 2025	13 days
Add task...		
Report Preparation		
Compile final report	Jul 15, 2025 – Aug 4, 2025	15 days

Figure 5: Gantt Chart for Gait Analysis

8. Budget

1. Data Acquisition

Online Datasets

Cost of purchasing or accessing gait data datasets from online repositories or academic sources. Estimated Cost: **$50**

2. Software Tools

Development Tools and Libraries

Machine Learning Libraries: Licensing fees or subscription costs for libraries such as TensorFlow, PyTorch, and scikit-learn.

Data Analysis Tools: Software for data cleaning, preprocessing, and visualization (e.g., MATLAB or Python libraries).

Estimated Cost: **$50**

Integrated Development Environment (IDE)

Tools and plugins needed for coding and development. Estimated

Cost: **$0**

Version Control and Collaboration Tools

Costs associated with platforms like GitHub or Bitbucket for code management and collaboration.

Estimated Cost: **$0**

3. Hardware

Computing Resources

Cloud computing services for model training and evaluation.

Estimated Cost: **$100**

4. Miscellaneous Expenses

Documentation and Reporting

Costs related to printing, binding, or creating professional reports and presentations. Estimated Cost:

$10

Contingency Fund

Reserved for unforeseen expenses or additional requirements that may arise during the project. Estimated

Cost: **$50**

Expense Category	Estimated Cost
Online Datasets	**$50**
Development Tools and Libraries	**$50**
Integrated Development Environment	**$0**
Version Control and Collaboration Tools	**$0**
Computing Resources	**$100**

Documentation and Reporting	**$10**
Contingency Fund	**$50**
Total Cost	**$260**

Figure 6: Budget.

9. Commercialization

The gait analysis system, combined with other behavioral biometric models, provides an innovative improvement in authentication technology. To effectively commercialize this system, numerous potential approaches and business models can be explored. This approach will span the entire project, from creation to market launch, providing a deliberate road to success.

1. Market Opportunities Cybersecurity Sector

It provides a system's ability to constantly offer nonintrusive verification, and therefore, it is extremely beneficial to the security of mission-critical information and assets. As the level of regulatory compliance to data privacy laws all over the world becomes stringent, businesses are keen to explore innovative methods of meeting these demands, and this gait analysis solution can be advanced as a robust system in attaining such high-level security requirements.

Robotics and HRI

Gait analysis can enable robots to enhance their interactions with users by properly detecting and adapting to them. Some key areas in which this would be very handy are social robots, assistive technology, and autonomous systems. The application of gait analysis to security robots adds another layer of protection in risky areas by allowing for access control and monitoring.

It can also be taken a step further into health monitoring systems, e.g., detecting gait irregularities that could suggest a health issue or administration of some treatment solutions. Moreover, the next step in gait analysis would be to integrate personal safety features into products, particularly a smartphone or wearable devices, which guarantee safe access and monitoring.

Smart Environments and IoT

The incorporation of smart building systems with gait analysis allows for increased security and user experience personalization, that is, modification of lights, temperature, and access with the associated or identified person. This integrates gait analysis into IoT devices to provide a strong additional measure of security and flexibility for smart home environments.

2. Business Models

Licensing Model

License gait analysis technology to cybersecurity firms, robotics manufacturers, and healthcare providers. This model enables recurring revenues by way of enabling partners to integrate the technology into their solutions, more so for access to the system's capabilities via an API so that third-party developers can integrate the gait analysis into their applications. A subscription model is a business model in which a customer pays a subscription price at regular intervals to use a product or service.

Offer the gait analysis system on a paid subscription basis. The model can turn out to be quite alluring for businesses that are seeking scalable solutions, which are regularly updated and supported. Offer advanced analytics and reporting services that can be conducted with data from gait, with different subscription tiers offering different service levels and data insight levels.

Partnerships and Joint Ventures

Partner with companies manufacturing biometric hardware or robotics to integrate the former's technology into their products, thus creating a bundled offering that enhances their value proposition. Academic and research institutions can be used for cooperation to develop the technology further to reach the aim of using their expertise and networks to enter the market.

Direct Sales

Directly market and sell the gait analysis system to large enterprises, security firms, and technology providers. Tailor solutions to specific industry demands and give customizable possibilities. Develop and market consumer-facing products that integrate gait analysis, like secure access solutions for personal use or advanced health monitoring devices.

3. Implementation and Growth Strategy

Market Entry Strategy

Initiate pilot projects with key industry players to demonstrate the system's effectiveness and gather real-world feedback. Showcase the technology at industry events to attract potential partners and customers.

Marketing and Promotion

Run targeted marketing campaigns highlighting the unique benefits and advantages of the gait analysis system for different sectors. Publish case studies and success stories to create trust and illustrate the system's worth in real-world situations.

Scalability

Ensure the system is designed for scalability, allowing for easy adaptation and integration with current technologies and infrastructure. Explore chances for worldwide expansion by finding markets with significant demand for advanced biometric solutions.

10. Description of personnel and facilities

Student Number	Name	Feature

IT21391668	Madhubhashana H. N. D	Collect and curate gait data from online datasets. Normalize gait data to ensure consistency. Segment the data into strides and steps for detailed analysis. Apply noise reduction techniques to clean the data. Implement Convolutional Neural Networks (CNN) to extract spatial features from the gait data. Develop Recurrent Neural Networks (RNN) to capture temporal features from the gait data. Integrate the features extracted from both CNN and RNN into a hybrid model. Develop and test the hybrid CNN-RNN model to assess its performance.

Figure 7: Personnel and Facilities

11. References

[1] Plurilock, "Behavioral Biometrics," [Online]. Available: https://plurilock.com/what-isbehavioral- biometrics/. [Accessed 31 07 2024].

[2] C. Álvarez-Aparicio, M. Á. Guerrero-Higueras, M. Á. González-Santamarta,, A. Campazas-Vega,, V. Matellán and . C. Fernández-Llamas , "Biometric recognition through gait analysis," 25 08 2022. [Online]. Available: https://www.nature.com/articles/s41598-022-18806-4. [Accessed 10 08 2024].

[3] WIKIPEDIA, "TensorFlow," 11 06 2024. [Online]. Available: https://en.wikipedia.org/wiki/TensorFlow. [Accessed 12 08 2024].

[4] WIKIPEDIA, "PyTorch," 10 05 2024. [Online]. Available: https://en.wikipedia.org/wiki/PyTorch. [Accessed 12 08 2024].

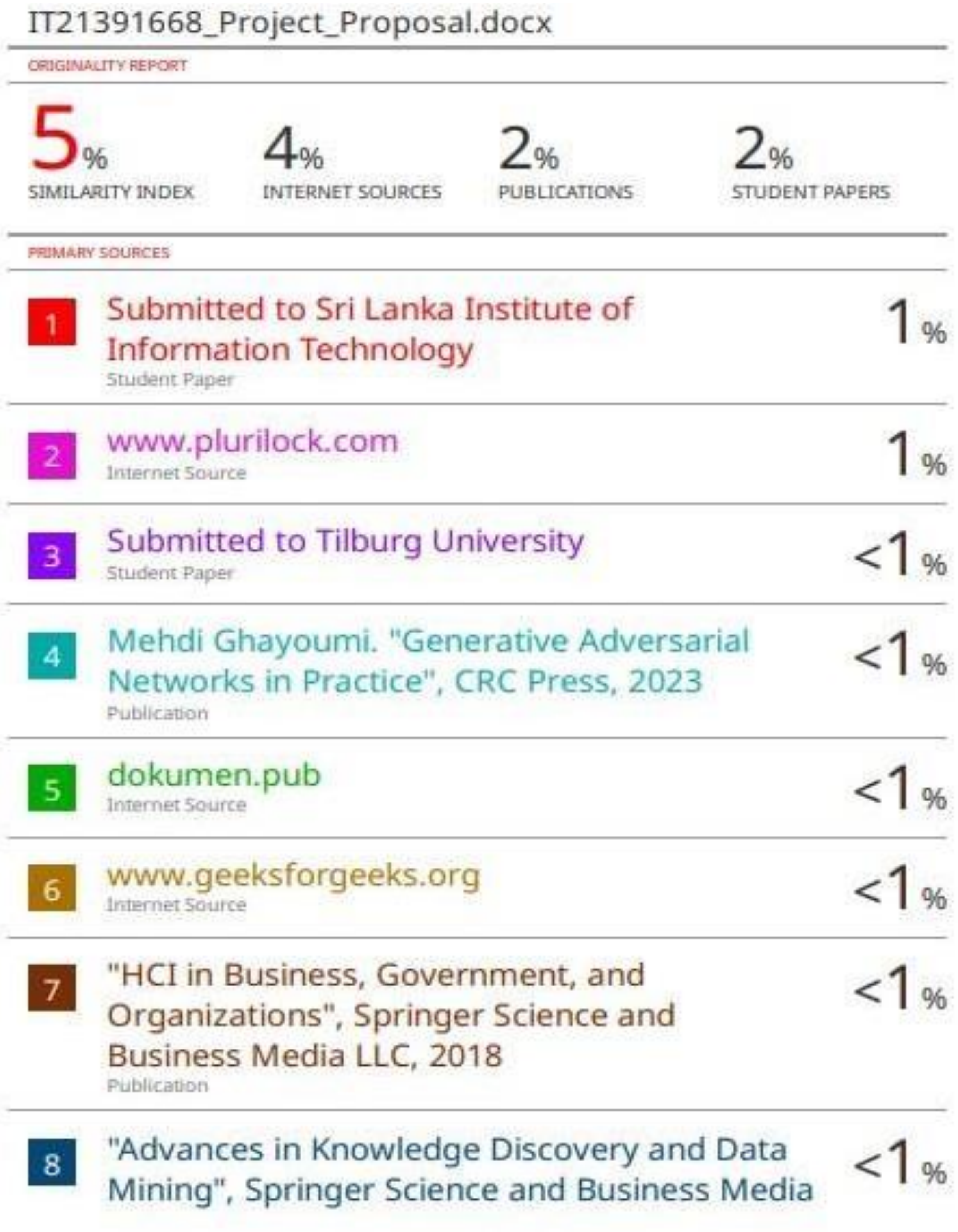
[5] W3SCHOOL, "NumPy Introduction," [Online]. Available: https://www.w3schools.com/python/numpy/numpy_intro.asp. [Accessed 12 08 2024].

[6] pandas, "pandas documentation," 10 04 2024. [Online]. Available: https://pandas.pydata.org/docs/. [Accessed 12 08 2024].

[7] A. Kececi, A. Yildirak, K. Ozyazici, G. Ayluctarhan, O. Agbulut and I. Zincir, "Implementation of machine learning algorithms for gait recognition," 08 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2215098619306214. [Accessed 10 08 2024].

[8] National Academies, "Biometric Recognition: Challenges and Opportunities," 2010. [Online]. Available: https://nap.nationalacademies.org/read/12720/chapter/2. [Accessed 10 08 2024].

12. Plagiarism Report



IT21391668_Project_Proposal.docx

ORIGINALITY REPORT

5%	4%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Sri Lanka Institute of Information Technology Student Paper	1%
2	www.plurilock.com Internet Source	1%
3	Submitted to Tilburg University Student Paper	<1%
4	Mehdi Ghayoumi. "Generative Adversarial Networks in Practice", CRC Press, 2023 Publication	<1%
5	dokumen.pub Internet Source	<1%
6	www.geeksforgeeks.org Internet Source	<1%
7	"HCI in Business, Government, and Organizations", Springer Science and Business Media LLC, 2018 Publication	<1%
8	"Advances in Knowledge Discovery and Data Mining", Springer Science and Business Media	<1%