Facial Recognition using TrustZone

Shivam Shekhar
MS Computer Engineering
ss6960@columbia.edu

Ritwik Goel
MS Computer Engineering
ss6960@columbia.edu

ABSTRACT

This report presents the development and implementation of a secure facial recognition system leveraging ARM TrustZone technology. The project aimed to create a robust authentication system by integrating a mobile application with a Trusted Execution Environment (TEE) for enhanced security. The mobile application captures user images, performs liveness detection, and communicates with the TEE for facial recognition and authentication. Despite successful development of the mobile application and trusted application components, the project faced challenges in establishing communication between these components via the GlobalPlatform API, primarily due to limited documentation and resources. This report outlines the project's objectives, design, implementation, learnings, and future directions.

KEYWORDS

Facial Recognition, TrustZone, Trusted Execution Environment, GlobalPlatform API, Authentication, Hardware Security.

1 INTRODUCTION

In the contemporary digital era, the ubiquity of mobile devices has become a double-edged sword, offering unparalleled convenience while simultaneously presenting significant security vulnerabilities. As these devices increasingly become the repositories of sensitive personal and financial information, the imperative for robust security mechanisms has never been more critical. This project is situated within this context, aiming to harness the capabilities of ARM's TrustZone technology to forge a new frontier in secure authentication through the development of a sophisticated facial recognition system.

ARM's TrustZone technology represents a paradigm shift in the approach to mobile device security. By providing a hardware-based security extension, TrustZone facilitates the creation of a Trusted Execution Environment (TEE). This secure enclave is isolated from the normal operating environment of the device, thereby offering a sanctuary for sensitive operations and data. The TEE's impervious nature to the vulnerabilities that plague the normal operating environment makes it an ideal candidate for hosting secure authentication mechanisms.

The project's primary objective was to leverage this secure environment to develop a mobile application that not only captures user images but also verifies the liveness of these images to prevent spoofing attacks. This liveness detection is a critical component of the system, ensuring that the authentication process cannot be circumvented through the use of photographs or other replicas of the user's face. Upon successful liveness verification, the application securely transmits the data to the TEE, where the core of the facial recognition and authentication process takes place.

The facial recognition system developed as part of this project is not merely a technological exercise but a response to the growing demand for secure, convenient, and non-intrusive authentication methods. Traditional authentication mechanisms, such as passwords and PINs, are increasingly seen as cumbersome and vulnerable to a variety of attack vectors. Biometric authentication, with facial recognition at the forefront, offers a compelling alternative. By leveraging the unique physical characteristics of the user, facial recognition provides a level of security that is difficult to replicate or forge.

However, the integration of facial recognition technology with TrustZone's secure environment presents its own set of challenges and complexities. The project embarked on a journey to navigate these challenges, from the initial capture and processing of biometric data to the secure transmission of this data to the TEE and the subsequent authentication process. Each step of this journey required careful consideration of security implications, performance constraints, and user experience.

In conclusion, this project represents a significant step forward in the quest for secure mobile authentication. By combining the cutting-edge capabilities of ARM's TrustZone technology with advanced facial recognition algorithms, the project aims to set a new standard for security and convenience in mobile applications. As mobile devices continue to play an increasingly central role in our lives, the importance of such secure authentication mechanisms cannot be overstated. This project not only addresses the immediate need for improved security but also lays the groundwork for future innovations in the field of mobile authentication.

2 LITERATURE REVIEW

The literature review delves into the intricate landscape of facial recognition technologies, TrustZone architecture, and secure authentication mechanisms, uncovering the depth and breadth of research and development in these areas. This exploration is pivotal for understanding the current state of the art and identifying future directions for enhancing security and privacy in digital systems.

2.1 Facial Recognition Technologies

Facial recognition technologies have seen significant advancements in recent years, driven by improvements in machine learning algorithms, computational power, and data availability. Studies have focused on various aspects of facial recognition, including algorithmic development, accuracy improvements, and applications in security and authentication systems. For instance, deep learning-based approaches, such as Convolutional Neural Networks (CNNs), have dramatically enhanced the ability to accurately recognize faces under varying conditions, including different lighting, angles, and facial expressions [1]. These advancements have broadened the scope of facial recognition applications, extending beyond traditional security systems to include mobile device authentication, financial transactions, and even healthcare settings.

2.2 TrustZone Architecture

ARM's TrustZone technology offers a robust framework for establishing a Trusted Execution Environment (TEE), which is crucial for securing sensitive operations on mobile devices and embedded systems [2][3]. Research in this area has highlighted the architectural design of TrustZone, which partitions the system into secure and non-secure worlds, thereby providing a hardware-based isolation mechanism. This isolation is essential for protecting critical security functions from vulnerabilities in the non-secure world, such as the operating system and applications. Studies have also explored the implementation challenges and best practices for leveraging TrustZone to achieve a high level of security, emphasizing the importance of secure boot processes, secure storage, and secure communication channels within the TEE.

2.3 Integration Challenges and Solutions

Integrating mobile applications with TEEs, particularly through TrustZone, presents a set of challenges, primarily due to the complexity of establishing secure communication channels and managing data securely across different execution environments [4][5]. The literature has identified a lack of comprehensive documentation and examples as a significant barrier to effective integration. However, solutions have been proposed to address these challenges, including the development of standardized APIs, such as those provided by the GlobalPlatform, which facilitate secure interactions between mobile applications and the TEE [4]. Additionally, research has focused on designing secure protocols for data transmission and authentication processes that can operate efficiently within the constrained environment of the TEE, ensuring data integrity and confidentiality.

The literature review underscores the rapid advancements in facial recognition technologies and TrustZone architecture, alongside the persistent challenges in integrating mobile applications with TEEs. As the demand for secure authentication mechanisms continues to grow, the insights gained from these studies are invaluable for guiding future research and development efforts. By addressing the identified challenges and leveraging the potential of TrustZone and facial recognition technologies, it is possible to enhance the security and privacy of digital systems significantly.

3 ARCHITECTURE DESIGN

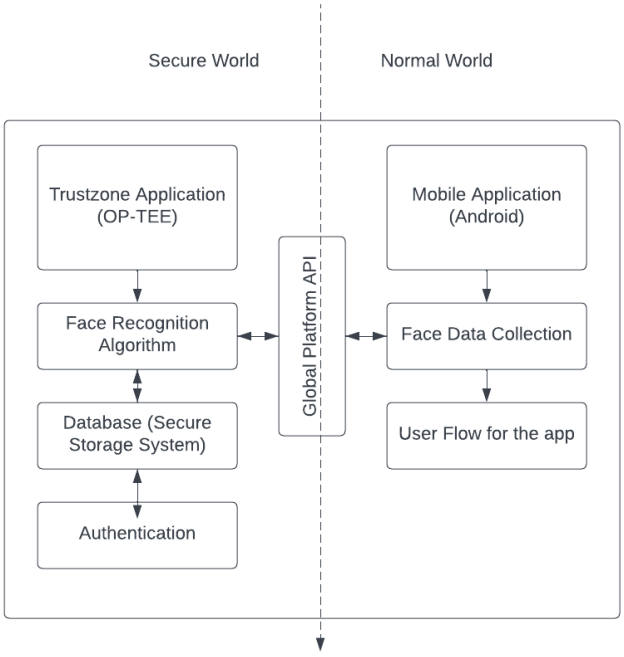

Fig. 1 Architecture Diagram of TZ Facial Recognition Application

The architecture shown of the Secure TrustZone Face Recognition system is meticulously designed to leverage the advanced security features of ARM's TrustZone technology, creating a robust and secure facial recognition system. This architecture is composed of two primary components: the mobile application and the trusted application within the Trusted Execution Environment (TEE). Each component plays a pivotal role in the system's overall functionality and security, working in tandem to provide a seamless and secure user experience.

3.1 Mobile Application

The mobile application serves as the user's gateway to the facial recognition system. It is designed with a user-friendly interface that guides the user through the process of capturing their image for authentication purposes. The application incorporates advanced liveness detection algorithms to ensure that the captured images are from a live person, thereby mitigating the risk of spoofing attacks through photographs or videos. This liveness detection is a critical security feature, as it forms the first line of defense against unauthorized access attempts.

Once the image is captured and liveness is verified, the mobile application prepares the data for secure transmission to the TEE. This involves encrypting the data to protect it against potential interception or tampering during transmission. The design of the mobile application emphasizes ease of use without compromising security, ensuring that users can authenticate themselves quickly and efficiently.

3.2 Trusted Application within the TEE

The trusted application resides within the secure zone of the TEE, isolated from the normal operating environment of the device. This isolation is crucial, as it protects the facial recognition and authentication processes from potential threats present in the non-secure environment. The trusted application is responsible for receiving the encrypted biometric data from the mobile application, decrypting it, and then processing it for facial recognition and authentication. The facial recognition algorithm implemented within the trusted application is carefully selected to balance security, performance, and resource constraints inherent to the TEE. The algorithm must be efficient enough to operate within the limited computational resources of the TEE while maintaining high accuracy in facial recognition to prevent false positives or negatives during authentication.

3.3 Secure Communication via GlobalPlatform API

A key aspect of the system architecture is the secure communication channel established between the mobile application and the trusted application within the TEE. This communication is facilitated by the GlobalPlatform API, which provides a standardized interface for interacting with the TEE. The use of the GlobalPlatform API ensures that data transmitted between the secure and non-secure environments is encrypted and protected against interception or tampering.

The GlobalPlatform API also simplifies the development process by providing a set of well-defined interfaces for message passing, data encryption, and secure session management. This allows the project team to focus on the core functionality of the facial recognition system without having to implement custom security protocols for communication between the mobile application and the TEE.

The architecture of the Secure TrustZone Face Recognition system is designed to leverage the strengths of ARM's TrustZone technology to provide a secure and efficient facial recognition system. By dividing the system into two primary components—the mobile application and the trusted application within the TEE—and establishing secure communication via the GlobalPlatform API, the architecture ensures the integrity and security of the biometric authentication process. This design not only protects against common security threats but also provides a seamless and user-friendly authentication experience.

4 IMPLEMENTATION

The implementation phase of the Secure TrustZone Face Recognition project was a multifaceted endeavor that required meticulous planning, coordination, and technical prowess. This phase was structured around a series of sequential and interdependent stages, each critical to the project's overall success. The primary objective was to develop a secure and efficient system capable of capturing biometric data through a mobile application, processing this data within a Trusted Execution Environment (TEE) using facial recognition algorithms, and securely authenticating the user. However, the integration of the mobile application with the TEE, facilitated by the GlobalPlatform API, presented significant challenges due to the scarcity of comprehensive documentation and practical examples.

4.1 Development of the Mobile Application

The initial stage involved the development of the mobile application, which serves as the user interface for capturing biometric data. This application was designed to guide users through the process of image capture while ensuring the liveness of the captured images to prevent spoofing attacks. The development team focused on creating a user-friendly interface that simplifies the authentication process without compromising security. The application was also engineered to encrypt the captured biometric data before transmission, ensuring its integrity and confidentiality.

4.2 Development of the Trusted Application within the TEE

Subsequently, attention shifted to the development of the trusted application within the TEE. This component is the heart of the facial recognition system, responsible for processing the encrypted biometric data received from the mobile application. Given the constrained environment of the TEE, the facial recognition algorithms had to be carefully selected and optimized for efficiency and performance. The development team explored various algorithms, ultimately choosing those that offered the best balance between accuracy and resource utilization. This optimization was crucial for ensuring that the facial recognition process could be executed swiftly and reliably within the TEE.

4.3 Integration Challenges

The integration of the mobile application with the trusted application within the TEE represented the project's most daunting challenge. The team planned to utilize the GlobalPlatform API for this purpose, expecting it to provide a secure and standardized interface for communication between the two components. However, the lack of detailed documentation and practical examples on how to effectively use the GlobalPlatform API for this specific use case hindered progress. The team encountered difficulties in establishing a secure communication channel, which was essential for transmitting encrypted biometric data from the mobile application to the TEE and ensuring the integrity of the authentication process.

4.4 Overcoming Integration Challenges

To address these integration challenges, the team undertook a comprehensive review of available resources, including the GlobalPlatform API documentation and related technical materials. Efforts were made to reach out to the developer community, seeking advice and examples from those who had successfully implemented similar integrations. Additionally, the team experimented with various approaches to secure communication, leveraging the limited examples available to prototype potential solutions. This iterative process of research, experimentation, and community engagement was critical for making incremental progress towards a viable integration strategy.

The implementation phase of the Secure TrustZone Face Recognition project was a testament to the complexities inherent in developing secure, efficient, and user-friendly authentication systems. Despite the challenges encountered, particularly in integrating the mobile application with the TEE, the team's dedication to overcoming these obstacles underscored their commitment to delivering

a robust facial recognition system. The lessons learned from navigating the integration challenges, especially the importance of accessible and detailed documentation, will undoubtedly inform future efforts in the field of secure authentication technologies.

5 SECURITY ANALYSIS

This section delves into the security analysis of the system, highlighting its strengths, potential vulnerabilities, and areas for future security enhancements.

5.1 Face Liveness Detection and Side Channel Attacks

The integration of face liveness detection in face recognition systems is crucial for preventing spoofing attacks where an attacker might use a photo, video, or a different replica of a genuine user's face to trick the system. However, these systems are not immune to side channel attacks. Side channel attacks exploit indirect information, such as power consumption patterns or execution timing, which can inadvertently leak sensitive data about the system's operations. In the context of face detection systems, particularly those utilizing TensorFlow, attackers could analyze these patterns to infer details about the model's architecture or the facial data being processed. To mitigate such attacks, implementing countermeasures like noise injection, algorithm randomization, or hardware-level protections is essential. These measures aim to mask or obfuscate the information leaked through these unintended channels, thereby safeguarding the system against potential exploits that could compromise user privacy and system integrity.

5.2 OpenCV Face Recognition Weaknesses

OpenCV offers versatile face recognition functionalities but has notable weaknesses, especially in handling variations in lighting, pose, and facial expressions. The accuracy of OpenCV's face recognition algorithms heavily depends on the quality and diversity of the training data. Biased or non-diverse training data can lead to poor generalization and potential biases in recognition results. Moreover, OpenCV might not be well-suited for real-time processing of large datasets or high-resolution images due to computational constraints. Addressing these weaknesses requires careful preprocessing of training data, parameter tuning, and possibly augmenting OpenCV with additional techniques to enhance its robustness and accuracy in diverse face recognition scenarios.

5.3 TrustZone Integration Considerations

Incorporating ARM's TrustZone technology into face recognition apps introduces several security considerations. TrustZone provides a secure enclave for protecting sensitive facial data and enhancing user authentication. However, developers must address secure enclave protection, communication integrity, user authentication, hardware vulnerabilities, and privacy preservation comprehensively. Proper isolation of the secure enclave, securing communication channels, mitigating hardware vulnerabilities, and adhering to privacy regulations are critical to ensure the application's security, reliability, and user trust.

5.4 Camera Module Utilization in Face Recognition

Utilizing the phone camera for face recognition, especially when integrated with TrustZone technology, presents vulnerabilities related to unauthorized camera access, data tampering, side-channel attacks, physical security risks, and privacy concerns. Ensuring robust security measures, including securing the camera interface, encrypting data, protecting against side-channel attacks, maintaining physical device security, and implementing privacy safeguards, is paramount. Regular security assessments are crucial for identifying and addressing potential vulnerabilities, thereby maintaining the confidentiality, integrity, and privacy of users' facial data and ensuring user trust in the face recognition app's security and reliability.

In conclusion, while face recognition technologies offer significant benefits for security and convenience, they also present various security challenges that must be addressed through comprehensive security measures and regular assessments. Ensuring the protection of sensitive data, user privacy, and system integrity is essential for maintaining user trust and the overall effectiveness of face recognition systems.

6 LEARNING

The Secure TrustZone Face Recognition project embarked on a journey that was as much about discovery and learning as it was about development and implementation. The project team, through its various stages, encountered numerous learning opportunities that spanned the technical intricacies of TrustZone technology and the nuanced challenges of project management. These learnings have not only enriched the team's understanding and skills but have also laid the foundation for future projects in similar domains.

6.1 Technical Learnings

One of the most significant areas of learning was the deep dive into ARM's TrustZone technology. The team explored the architecture of TrustZone, understanding how it enables the creation of a Trusted Execution Environment (TEE) that is isolated from the normal operating environment. This exploration included studying the mechanisms TrustZone provides for secure boot, secure storage, and secure execution of applications, which are critical for protecting sensitive operations and data.

The development of secure communication channels between the mobile application and the TEE was another area that provided substantial learning. The team grappled with the complexities of establishing these channels using the GlobalPlatform API, a process that was hindered by the lack of detailed documentation and practical examples. Through trial and error, research, and community engagement, the team gained insights into secure message passing, data encryption, and session management within the context of TrustZone.

Additionally, the project provided an opportunity to delve into the world of facial recognition algorithms. The team researched and evaluated various algorithms, considering factors such as accuracy, efficiency, and the constraints of running within the TEE. This

process involved not only theoretical study but also practical implementation and optimization of algorithms, offering a hands-on learning experience in algorithm selection and application.

6.2 Project Management Learnings

From a project management perspective, the project underscored the importance of resource availability. The team experienced firsthand the challenges posed by insufficient documentation and the lack of developer support, particularly in relation to the GlobalPlatform API. This situation highlighted the need for thorough planning, including contingency plans for overcoming information gaps and leveraging community resources.

The project also emphasized the value of clear communication and effective task distribution among team members. With a project of this complexity, ensuring that all team members were aligned on goals, tasks, and timelines was crucial for maintaining progress and addressing challenges promptly. The team learned the importance of regular updates and meetings, not only for tracking progress but also for brainstorming solutions to technical hurdles.

In conclusion, the Secure TrustZone Face Recognition project was a rich source of learning for the team, offering insights into both the technical and managerial aspects of developing a secure authentication system. The technical learnings about TrustZone technology, secure communication, and facial recognition algorithms have enhanced the team's capabilities in these areas. Simultaneously, the project management learnings about resource planning, communication, and teamwork have provided valuable lessons for future projects. These learnings, combined with the practical experience gained, position the team well for continued success in the field of secure system development.

7 FUTURE WORK

The future work for the Secure TrustZone Face Recognition project is outlined with a clear focus on addressing the integration challenges that have been a significant hurdle during the project's implementation phase. This section elaborates on the strategies and specific areas of development that the project team intends to pursue to enhance the system's functionality and reliability.

7.1 Overcoming Integration Challenges

The primary focus will be on resolving the integration issues between the mobile application and the Trusted Execution Environment (TEE). This involves a multi-faceted approach:

7.1.1 Extensive Research into Resources: The project team plans to conduct thorough research into existing documentation, tutorials, and case studies related to the GlobalPlatform API. This will include a deep dive into resources provided by GlobalPlatform as well as third-party content that may offer insights into similar integration challenges.

7.1.2 Engagement with the Developer Community: Recognizing the value of collective knowledge, the project team aims to actively engage with the developer community. This includes participating in forums, attending workshops, and possibly contributing to open-source projects. Such engagement will help in gathering practical insights and solutions that have been effective in similar scenarios.

7.1.3 Utilization of Simulation Tools: To better understand the integration challenges and test potential solutions, the project team will utilize simulation tools such as QEMU for ARM environments. This approach allows the team to emulate different scenarios and integration behaviors in a controlled setting.

7.2 Enhancing the Facial Recognition Algorithm

The Secure TrustZone Face Recognition project, as outlined in the report by Shivam Shekhar and Ritwik Goel, has made significant strides in leveraging ARM's TrustZone technology to create a sophisticated facial recognition system for mobile applications. A critical component of this system is the facial recognition algorithm, which plays a pivotal role in accurately identifying individuals and ensuring the security of the authentication process. The report mentions plans for future work focused on enhancing this algorithm to improve accuracy, efficiency, and user satisfaction. This section aims to expand on these plans by exploring potential strategies and technologies that could be employed to achieve these goals.

7.3 Algorithm Optimization

Optimizing the facial recognition algorithm involves refining its ability to process and analyze biometric data efficiently. One approach to optimization could involve the implementation of more advanced image processing techniques to enhance the quality of the captured images before they are analyzed. Techniques such as adaptive histogram equalization or noise reduction could improve the algorithm's ability to recognize faces under various lighting conditions and reduce the impact of environmental factors on the recognition process.

7.4 Incorporation of Advanced Machine Learning Techniques

The integration of advanced machine learning techniques, particularly deep learning models like Convolutional Neural Networks (CNNs), could significantly enhance the facial recognition capabilities of the system. Deep learning models are renowned for their ability to learn complex patterns and features from large datasets, making them highly effective for facial recognition tasks. Implementing lightweight versions of these models that are optimized for the constrained environment of the TEE could offer a balance between performance and resource utilization. Transfer learning, where a pre-trained model is fine-tuned with a specific dataset, could also be a viable strategy to improve the algorithm's accuracy without the need for extensive computational resources.

7.5 Real-time Performance Improvements

Improving the real-time performance of the facial recognition process is crucial for user satisfaction and the overall effectiveness of the system. This could involve optimizing the codebase for faster execution, possibly by employing more efficient data structures or algorithms that reduce computational complexity. Additionally, exploring parallel processing techniques or hardware acceleration options available within the TrustZone environment could further

reduce latency and enhance the responsiveness of the facial recognition process.

7.6 Testing with Diverse Datasets

To ensure the robustness and fairness of the facial recognition algorithm, it is essential to test it against diverse datasets that include a wide range of facial types, expressions, and environmental conditions. This testing can help identify any biases or weaknesses in the algorithm, allowing for targeted improvements. Incorporating datasets from different demographic groups and scenarios can also enhance the algorithm's ability to perform accurately in real-world applications.

7.7 Ethical Considerations and Privacy

As the facial recognition algorithm is enhanced, it is crucial to consider the ethical implications and privacy concerns associated with biometric authentication systems. Ensuring that the system adheres to privacy regulations and ethical guidelines is essential for maintaining user trust and safeguarding personal data. Implementing features such as explicit user consent, data anonymization, and secure data storage can help address these concerns.

The future work for the Secure TrustZone Face Recognition project is geared towards creating a more robust, efficient, and user-friendly system. By addressing the integration challenges and enhancing the facial recognition algorithm, the project aims to set a new standard in secure facial recognition technologies. These efforts will not only improve the current project but also contribute to the broader field of secure biometric authentication systems

8 CONCLUSION

The Secure TrustZone Face Recognition project embarked on an ambitious journey to harness ARM's TrustZone technology in creating a cutting-edge facial recognition system designed for enhanced security in mobile applications. Spearheaded by Shivam Shekhar and Ritwik Goel, the project meticulously outlined a comprehensive plan spanning several weeks, detailing tasks from literature review to final code review and testing. The project's repository served as a testament to the team's dedication and systematic approach towards achieving their goal.

8.1 Project Achievements

The project team successfully developed key components of the system, including the mobile application for capturing and processing biometric data, and the trusted application within the Trusted Execution Environment (TEE) for facial recognition and authentication. These achievements mark significant milestones in the project's lifecycle, showcasing the team's technical prowess and their ability to navigate the complexities of TrustZone technology and facial recognition algorithms.

8.2 Integration Challenges

Despite the successes, the project encountered substantial challenges in integrating the mobile application with the TEE, primarily due to the limited documentation available on the GlobalPlatform API. This gap in resources posed a significant hurdle, hindering the seamless communication necessary for the secure transmission of biometric data between the non-secure and secure environments. The team's efforts to overcome these challenges underscored the critical need for comprehensive documentation and developer support in the realm of secure mobile application development.

8.3 Valuable Learnings

The project provided the team with invaluable learnings, both from a technical and project management perspective. The exploration of TrustZone technology and the development of secure communication channels offered deep insights into the intricacies of creating secure systems within constrained environments. Moreover, the project management challenges highlighted the importance of resource availability, clear communication, and effective task distribution among team members. These learnings are not only pivotal for the team's future endeavors but also contribute to the broader community's understanding of developing secure authentication systems.

8.4 Laying the Foundation for Future Work

The Secure TrustZone Face Recognition project, despite the challenges encountered, has laid a solid foundation for future work in the field of secure authentication systems. The project's outcomes and learnings pave the way for further exploration and development, particularly in overcoming the integration challenges and enhancing the facial recognition algorithm for improved accuracy and efficiency. Future work will also focus on exploring alternative resources, engaging with the developer community, and potentially forming partnerships with academic institutions to gain deeper insights into the GlobalPlatform API and other related technologies.

In conclusion, the Secure TrustZone Face Recognition project represents a significant step forward in the quest for secure and efficient facial recognition systems. While the journey was met with challenges, the achievements, learnings, and the foundation laid for future work underscore the project's success and its contribution to the field of secure mobile authentication. The dedication and effort of Shivam Shekhar, Ritwik Goel, and the entire project team have not only advanced the technical capabilities in this domain but have also highlighted the critical areas for improvement and further research. As the project concludes, it leaves behind a legacy of innovation, perseverance, and a roadmap for future advancements in secure authentication technologies.

9 REFERENCES

- Advancements and Breakthroughs with FACE TRUST Part 2.
- ARM TrustZone: Secure Your Embedded Systems
- TrustZone for Cortex-A
- Demystifying Arm TrustZone: A Comprehensive Survey
- What is TrustZone?