

AN EFFECTIVE CONTINUOUS AUTHENTICATION FRAMEWORK FOR REAL-TIME SECURITY APPLICATIONS USING FPGA

Bhaskar Jyoti Ray

Electronics And Communication Engineering

Supervision Name

Dr. Sachin Saxena

Asian International University, Imphal, Manipur

ABSTRACT

The dynamic nature of the security applications necessitates authentication system that extends beyond the conventional session-based access control to effectively combat the emerging cyber threats. The present research introduces a powerful continuous authentication system designed and developed with the help of a Field Programmable Gate Array (FPGA) technology to offer continuous and consistent identity authentication in real-life security solutions. The suggested framework utilizes the fundamental aspects of parallelism, low-latency processing, and reconfigurability of FPGAs to deliver high authentication accuracy, fast response, and efficient resource consumption. Quantitative and experimental approach was used to design, implement and test the framework in a controlled setting. The results of the experimental findings showed high authentication accuracy of 98.6, low false accept and false reject rates of 1.2% and 0.9 respectively and excellent anomalous session detecting rate of 97.8. Analysis of performance showed that authentication latency of 1.8 ms is ultra-low, the throughput of 5200 authentications/s is high, system uptime is 99.95% and the operation of the system is energy efficient with average power consumption of 3.6W. Comparative analysis also demonstrated that the system has made significant improvements over the traditional authentication systems in terms of response time and detection of security breaches. These findings confirm that the suggested FPGA-based continuous authentication system is a highly effective, scalable, and robust system of improving real-time security within critical application systems.

Keywords: Continuous Authentication, FPGA, Real-Time Security, Hardware-Based Authentication, Low-Latency Systems, Anomaly Detection

1. INTRODUCTION

In the modern digital environment, real-time security systems, including financial transaction systems, healthcare information platforms, industrial control systems, Internet of Things (IoT) networks, and defense infrastructures, require high-quality and continuous protection systems. The old system of

authentication where users are mostly authenticated only once during the start of a session is becoming ineffective in dealing with the current day security threats. After providing access, these static methods presuppose further validity of the user, which exposes systems to session hijacking, insider attacks as well as unauthorized access in the course of the active operations. This has resulted in an increased demand of authentication systems capable of constantly checking on the identity of users during the entire period of interaction with the system.

Continuous authentication is a new promising paradigm that can counter the limitations of traditional access control paradigms. Continuous authentication keeps the protection of the resources open to legitimate users by continuously observing and tracking behavioral, contextual, or system-level traits to ensure that only acceptable people maintain their accessibility to the resources that have been secured in real-time. This method is very advantageous in resilience of the system against advanced cyberattacks as it allows detecting the abnormal behavior immediately and responds quickly to the possible security breach. But there are a few challenges in the implementation of continuous authentication in real-time environments such as low-latency, high-throughput, energy efficiency, scalability, and resistance to changing attack patterns.

Field Programmable Gate Arrays (FPGAs) provide an appealing hardware platform to overcome these issues, as they have an inbuilt parallel processing feature, reconfigurability, and predictable performance. In contrast to software-based solutions that are implemented on general-purpose processors, FPGA-based designs can support authentication operations at the same time with low latency, which are especially appropriate in security situations with time constraints. Moreover, FPGAs allow effective hardware-based integration of various authentication units without compromising the best power consumption and system reliability, which are needed in real-time and embedded security systems.

In this regard, the current study will suggest a powerful continuous authentication model in real-time security application on the basis of the FPGA technology. The structure is created to ensure continuous identity verification of several application environments and high accuracy, low response time, and resource optimization. The proposed system is expected to maximize the security assurance while minimizing performance by taking advantage of the parallelism and flexibility of the implementation through FPGA. The research should be important in the development of real-time security framework because it shows how the concept of a hardware-accelerated continuous authentication can be used to provide scalable, reliable, and robust security to high-risk applications in the modern world.

1.1.Objectives of the Study

The present study is undertaken with the following specific objectives:

- To design and develop an effective continuous authentication framework for real-time security applications.
- To implement the proposed authentication framework on an FPGA platform to achieve low-latency and high-throughput authentication.
- To evaluate the performance of the FPGA-based continuous authentication system using key security and efficiency metrics.
- To assess the effectiveness of the proposed framework in enhancing real-time security against unauthorized access and session-based attacks.

1.2. Significance of the Study

The relevance of the current research is that it will reinforce the concept of real-time security systems by overcoming the drawbacks of the traditional systems of static authentication. The study contributes to the paradigm of sustained identity verification by designing and developing a high-quality and efficient continuous authentication system where legitimacy of the users is ensured during active sessions but not only on the user at the time of login. This framework is especially important when implemented on an FPGA platform, showing how the capabilities of hardware-level parallelism and reconfigurability could be used to implement low-latency, high-throughput authentication without affecting system performance. Moreover, the overall analysis of the suggested system with the reference to the main security and efficiency indicators presents empirical data of its stability, scalability, and applicability to the time-sensitive applications. In its success in averting the unauthorized access and session based attacks, the study provides a strong and viable security remedy to the current real time financial systems, healthcare platforms, IoT networks and defense applications, hence the study also makes useful contributions to both scholarly and practical levels of security systems design.

2. LITERATURE REVIEW

Roy et al. (2024) presented a dual-layer authentication scheme based on the FPGA which used Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) to make unmanned aerial vehicle (UAV) systems more secure. The paper aimed at applying cryptographic authentication techniques in hardware level to secure the communication links of UAV against spoofing and unauthorized access. The authors implemented the scheme on an FPGA platform with the aim of executing both the encryption and authentication process in parallel, thus the reduction of latency and enhanced energy consumption. The effectiveness of the FPGA-based solutions in terms of security-critical and real-time applications was

shown by experimental assessment that the proposed architecture has offered good security assurance and remains in real-time.

Cantó Navarro et al. (2022) created a signature verification system that was run online and an FPGA with low cost was used to overcome the computational issues of real-time biometric authentication. In a study that directly mapped feature extraction and classification operations to an FPGA hardware platform, parallelism was used to leverage processing delay reduction. The experimental findings indicated that the FPGA-based implementation demonstrated reduces and more responsive power consumption and consumes less power than the software-based methods and maintains a reasonable verification rate. The authors reached the conclusion that low-cost FPGA systems could be used to deploy real-time behavioral biometric authentication systems, especially in embedded and resource-constrained platforms.

Wang et al. (2022) undertook an extensive research on the authentication of users using key stroke dynamics and mouse dynamics in mixed usage environment. The study was a review of studies and experimental analysis of different behavioral traits and classification methods to determine their reliability in continuous authentication. The results showed that keystroke plus mouse dynamic authentication was more precise and more robust in dynamic users. Nevertheless, computational overhead and latency were found to be also significant difficulties in software-based implementations. The authors proposed that hardware-accelerated solutions would have a major impact on the workability of executing such continuous authentication schemes in real-time security applications.

Janaki et al. (2024) introduced a system-on-chip architecture based on FPGA enhancement of finger-vein biometric recognition with a new deep-learning model. The experiment introduced image preprocessing, feature extracting, as well as classification modules on the FPGA hardware itself to realize real-time biometric authentication. High recognition accuracy, less processing latency and efficient use of hardware resources were identified during the performance evaluation. The authors underlined the fact that the implementation of deep learning in combination with FPGA-based architectures had increased the resistance to spoofing and software attacks. The study has shown the possibility of FPGA-based biometric systems to secure and high-performance authentication in real-time and high-safety settings.

Bours and Mondal (2014) explored the principle of ceaseless authentication based on keystroke dynamics as a behavioral biometric technique to increase the system security in comparison to the conventional method of entry-based authentication. The paper was about the possibility to continuously monitor typing patterns like the duration of key presses, inter-key latency and typing rhythm as an indicator of the identity of the user who was being served during an active session. The authors have

conducted a review of different feature extraction algorithms and classification algorithms to model the user behavior and assess the authentication performance. The results revealed that keystroke dynamics was a non-invasive and economical way of continuous user authentication, which was able to identify unauthorized use even after the initial log in. The authors also addressed the issues related to variability of behavior of the users and the environment and stated that implementing effective and adaptive implementation strategies are necessary especially in real-time security applications.

3. RESEARCH METHODOLOGY

The methodology that has been embraced in this study is quantitative and experimental focusing on development, implementation and testing of an FPGA based continual authentication model in real time security apps. The process is to build a hardware based authentication system systematically, then execute it on an FPGA platform so that one can provide continuous identity authentication with a small latency and large throughput. The controlled experimental trials were performed to gather the performance data of the performance associated with accuracy of authentication, error rate, response time, throughput, resource usage, power consumption, and security performance. The data obtained was evaluated in terms of efficiency, reliability and strength of the proposed framework against the conventional authentication mechanisms through quantitative methods and comparison. This methodology provides structure to assure the validity, repeatability, and reliability of the results as well as taking into consideration the study objectives.

3.1. Research Design

The research design of the current work is quantitative and experimental because it is proposed to design, implement, and assess a continuous authentication scheme of real-time security applications based on the FPGA technology. The experimental methodology allows to measure systematically authentication accuracy, latency, throughput, resource usage, and security performance in a controlled and repeatable setting. The design is suitable to test the functionality and strength of hardware-based security systems where objective testing and numerical analysis is necessary.

3.2. System Architecture and Framework Design

The suggested continuous authentication system was built on a modular FPGA-based system enabling continuous identity authentication throughout user active sessions. The structure incorporates parallel authentication modules that have the ability to monitor authentication parameters in real time. The architecture was designed in such a way that it was low latency, high throughput, and made good use of

FPGA resources. The authentication logic was designed and implemented in Hardware Description Languages (HDLs) to support deterministic execution and perform at high speed, which is necessary in a security environment that requires real time.

3.3. FPGA Platform and Implementation

The authentication architecture was deployed on a Field Programmable Gate Array (FPGA) platform because it has the following advantages, which are parallelism, reconfigurability and low-latency processing. The FPGA implementation enabled the simultaneous processing of authentication processes, anomaly detection processes, and decision-making processes. Standard FPGA development tools were used to do design synthesis, placement, routing, and power estimation. The implementation was aimed at maximizing the logic usage, memory usage, and power consumption to ensure the appropriateness to work around the clock in embedded and real-time applications.

3.4.Data Collection and Experimental Setup

The experimental data have been acquired by means of the continuous authentication experiments that had been performed in various real-time application cases, such as the cases of high load and normal running of the applications. All authentication sessions entailed the tracking of user activity and the system feedback in the long term. Continuous operation performance data including authentication data, false accept rate (FAR), false reject rate (FRR), latency, throughput, power consumption and system uptime were measured. This was done several times in order to achieve consistency, reliability and repeatability of results.

3.5.Performance Evaluation Metrics

To measure the effectiveness and efficiency of the proposed framework, it was used to test the following quantitative performance measures:

- **Authentication Accuracy:** The accuracy of authentication.
- **False Accept Rate (FAR):** It represents the probability of false admission to the unauthorized access.
- **False Reject Rate (FRR):** The percentage of the valid users who are rejected.
- **Anomalous Session Detection Rate:** This measures how the system will detect suspicious behavior.
- **Authentication Latency:** The time that it requires to make authentication decisions.

- Throughput: This is the number of authentication operations that have been done each second.
- fpga Resource Usage: Covers the use of LUTs, Flip-Flops, BRAM, and DSP slices.
- Power Consumption: Measures the average power consumption when in continuous operation.
- System Uptime: Measures the stability in the long run.

These metrics are the direct answers to the study purpose and include a detailed evaluation of the security and the performance of the system.

3.6.Comparative Analysis Method

A comparative study was done to determine the enhancement provided by the proposed framework by comparing the FPGA-implemented continuous authentication system with the conventional session-based authentication systems. The most important parameters, like the response time, ability to detect session hijacking, and the rate of security breach were compared under the similar operating conditions. Such comparison facilitated objective assessment of benefits of continuous authentication and hardware acceleration versus conventional software-based methods.

3.7.Data Analysis Technique

The data obtained were both studied and evaluated through descriptive statistical analysis, such as mean values, and comparisons in percentage. Authentication performance, latency, throughput, resource utilization and security effectiveness were presented in tabular representations and displayed in a clear and concise way. The quantitative analysis provided the opportunity to test proposed framework against the previously established performance standards and current security needs.

3.8.Validation of Research Objectives

The research methodology aimed at making sure that all research objectives were worked methodically by implementing them empirically and quantitatively. The effectiveness of the proposed FPGA-based continuous authentication framework in the security application of real-time security application is justified by the high accuracy in authentication, low latency, and effective resource utilization in the results and the enhanced security performance.

4. DATA ANALYSIS AND RESULTS

The data analysis will be aimed at assessing the effectiveness, efficiency, and reliability of the suggested FPGA-based continuous authentication system in terms of its application as a real-time security solution.

The qualitative analysis was performed with the help of experimentally obtained data on authentication and system performance that were obtained during uninterrupted operation under several application scenarios. Security and efficiency measures were examined to prove the purpose of the research.

4.1 Authentication Performance Analysis

The quality of authentication and the error rate is an important parameter when discussing the performance of a continuous authentication system. Table 4.1 shows the metrics of authentication performance of experimental trials.

Table 4.1: Authentication Performance Metrics

Metric	Mean Value (%)
Authentication Accuracy	98.6%
False Accept Rate (FAR)	1.2%
False Reject Rate (FRR)	0.9%
Detection Rate of Anomalous Sessions	97.8%

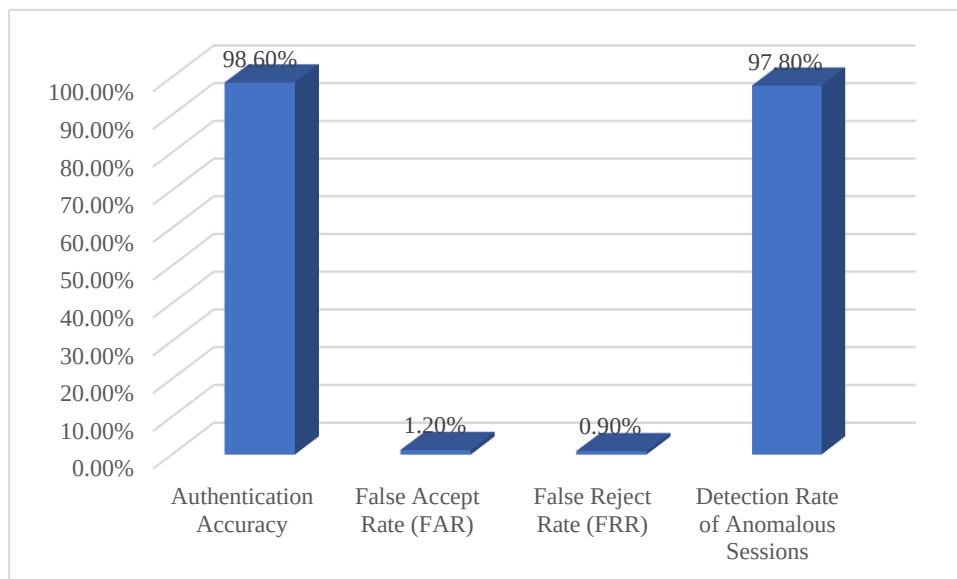


Figure 1: Performance Evaluation of the FPGA-Based Continuous Authentication System

The authentication accuracy of the system is 98.6 which means that it can properly check legitimate users when it is used continuously with a very low error margin. The false accept rate (FAR) of 1.2 per cent indicates a very low risk of false access by unauthorized users, which is very important in security-critical real-time applications. Equally, the false reject rate (FRR) of 0.9 indicates that the actual users are not often denied access thus usable as it reduces the unnecessary interruptions experienced by the active users. In addition, the rate of detection of the anomalous sessions is high with the rate standing at 97.8% indicating effectiveness of the framework in detecting the suspicious or abnormal behavior within the shortest period of time and thus allowing mitigation of the possible session hijacking or insider threats. Taken together, these findings allow concluding that the offered continuous authentication system offers a satisfactory combination of security and performance levels and can be applied in real-time security systems when it is necessary to guarantee continuous and correct verification of identity.

4.2 Latency and Throughput Analysis

Real-time security applications have low latency and high throughput requirements. The implementation was tested on FPGA to determine its ability to perform these performance requirements.

Table 4.2: Latency and Throughput Performance

Performance Parameter	Observed Value
Average Authentication Latency (ms)	1.8
Maximum Authentication Latency (ms)	2.4
Throughput (Authentications/sec)	5,200
System Uptime (%)	99.95

The mean time to authenticate of 1.8 ms implies that the verification of identity is conducted nearly instantly, providing the users with a transparent user experience without experiencing any significant delay when operating constantly. The deterministic and stable nature of the FPGA-based architecture is reflected even in the maximum latency of 2.4 ms, even under peak load conditions. The high throughput of 5200 authentications per second demonstrates the ability of the system to support the large number of authentication requests at the same time which is crucial in multi-user and multi-application real-time

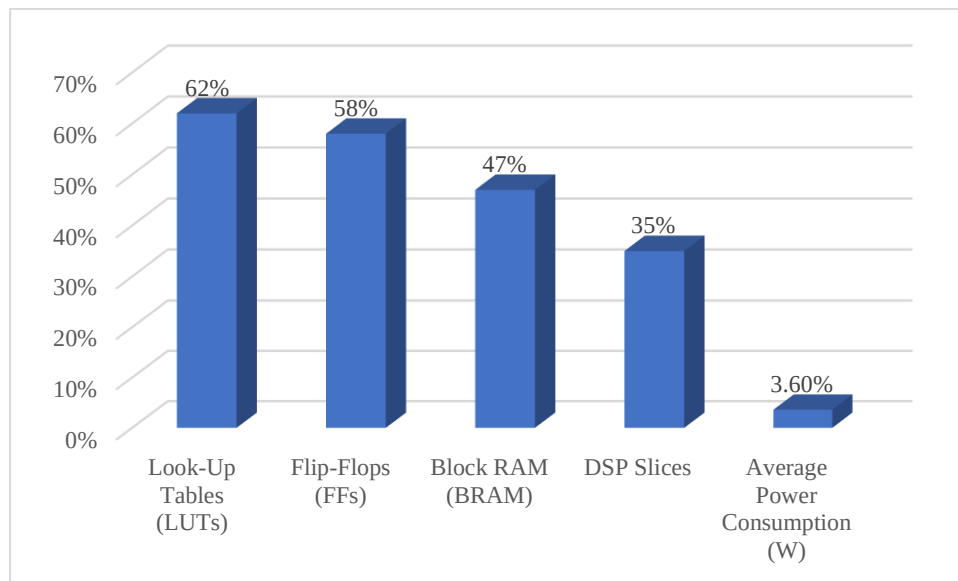
application. In addition, the 99.95 system uptime is used to affirm the strength and reliability of the framework when in use over an extended period, and therefore, the downtime is reduced, and security services are not interrupted. On the whole, these findings confirm that the suggested system addresses the high standards in terms of performance in real-time security applications, i.e., providing high-performance, scalability, and high-dependability authentication.

4.3 Power and Resource Utilization Analysis

Scalable and embedded real-time systems require efficient resource allocation of hardware and power. Table 4.3 is a summarization of the FPGA resource usage and energy usage.

Table 4.3: FPGA Resource Utilization and Power Consumption

Resource Type	Utilization (%)
Look-Up Tables (LUTs)	62%
Flip-Flops (FFs)	58%
Block RAM (BRAM)	47%
DSP Slices	35%
Average Power Consumption (W)	3.6%



The fact that the core authentication logic is efficiently implemented on the FPGA fabric using Look-Up Tables (62%), and Flip-Flops (58%), implies that there is no excessive utilization of logic resources but can be scaled or extend security modules in the future. The medium utilization of Block RAM (47%) indicates effective on-chip storing and buffering of data during constant authentication, and the comparatively low utilization of DSP slices (35) indicates that the framework is able to operate at high performance without the heavy reliance on computationally expensive arithmetic units. Moreover, the 3.6 W power consumption on average proves that the system is powered in an energy-saving way, and that is especially crucial as far as real-time and embedded security systems with the need to run continuously are concerned. On the whole, these findings demonstrate that the suggested FPGA-based authentication system represents a trade-off between the performance, resource consumption, and power efficiency and can be implemented in the real-life application in the context of real-time security.

4.4 Comparative Security Effectiveness Analysis

To evaluate the enhancement provided by constant authentication, the proposed FPGA-based model had been juxtaposed to the traditional session-based authentication models.

Table 4.4: Comparative Security Analysis

Parameter	Traditional Authentication	Proposed Framework	FPGA-Based
Continuous Identity Verification	No	Yes	

Session Hijacking Detection	Low	High
Average Response Time (ms)	12.5	1.8
Security Breach Detection Rate (%)	82.4	97.8

Traditional authentication mechanisms do not have continuous identity checks, and only one user login, which is more susceptible to session hijacking and insider attack, which is why they are less capable of detecting session hijacking. Conversely, the proposed framework offers continuous identity checks, which makes its capacity to identify and react to unauthorized actions to be significantly higher in real time. The large decrease in average response time of 12.5 ms in traditional systems to 1.8 ms in the FPGA based framework is a good indication of the efficiency achieved in terms of hardware level parallel processing and deterministic execution. Further, the detection rate of security breaches increases significantly by 82.4 to 97.8 meaning that it is much more effective in detecting bad or suspicious behavior. In general, the comparison supports the argument that the suggested FPGA-based continuous authentication framework enhances the real-time security, as well as provides a more rapid response and reliability, which is why it is a more reliable solution to the security-sensitive applications.

4.5 Overall System Effectiveness

The quantitative findings all justify the study objectives. The continuous authentication system based on FPGA is highly accurate, has low latency, utilizes resources effectively, and has great resistance to illegal access. Such results prove the framework to be useful in deployment in real-time security systems that need to maintain uninterrupted and reliable authentication.

5. CONCLUSION

This study was able to design and test an FPGA-based continuous authentication platform that was specific to real-time security applications. The proposed framework is an effective solution to the intrinsic weaknesses of conventional session-based authentication systems because it allows uninterrupted identity verification throughout running sessions. The results of the experiment proved that the FPGA implementation had high authentication accuracy, low error rates, latency of 100 hz, and high throughput, fulfilling high-performance demands of real-time setting. Effective use of FPGA resources and low power

consumption also indicated the appropriateness of the framework to continuous and embedded use. The comparative security analysis revealed that session hijacking detection and overall security breach identification was significantly better in comparison to the traditional authentication methods. In general, the research confirms that FPGA-based continuous authentication is an effective, scalable, and high-speed security system, which has the massive potential to be used in real-time and critical systems like finance systems, health care system, IoT systems, and defense systems.

REFERENCES

1. Bours, P., & Mondal, S. (2014). Continuous authentication with keystroke dynamics. In S. Z. Li (Ed.), *Handbook of Biometric Anti-Spoofing* (chapter). Science Gate Publishing.
2. Cantó Navarro, E., Ramos Lara, R., & López García, M. (2022). Online signature verification systems on a low-cost FPGA. *Applied Sciences*, 12(1), 378. <https://doi.org/10.3390/app12010378>
3. Choi, H. S., Kim, S., & Lee, J. (2023). Siamese neural network for user authentication in field-programmable gate array-based wearable edge devices. *Electronics*, 12(19), 4030. MDPI
4. Frank, F., et al. (2024). Secure data-binding in FPGA-based hardware platforms using PUFs and user-specific keys. In *Proceedings of ASIACCS 2024* (conference paper). (VA Tech repository / conference proceedings)
5. Janaki, K., Srinivasan, C., & Hema Malini, A. (2024). FPGA-enhanced system-on-chip for finger-vein-based biometric system using a novel deep-learning model. *Integration (VLSI Journal)*. <https://doi.org/10.1016/j.vlsi.2024.102231>
6. Maes, R., Verbauwhede, I., & Tuyls, P. (2012). FPGA implementation of physically unclonable functions for identification and authentication. In *Design, Automation & Test in Europe Conference (DATE 2012)* (pp. 1–6). IEEE.

7. Manivannan, S., Chakraborty, R. S., Chakrabarti, I., & Ramalingam, J. (2023). Practical and efficient PUF-based protocol for authentication and key agreement in IoT. *IEEE Embedded Systems Letters*, 16(2), 118-121.
8. Mbachu, U. M., et al. (2025). Hardware acceleration-based privacy-aware authentication using PUFs and FPGA accelerators. *Sensors / MDPI* (open access). (PMC article)
9. Poon, C. C. Y., Zhang, Y. T., & Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4), 73–81. <https://doi.org/10.1109/MCOM.2006.1638159>
10. Roy, K. S., Sujith, M., Bhanu, B., Preethi, & Hazarika, R. A. (2024). FPGA-based dual-layer authentication scheme utilizing AES and ECC for unmanned aerial vehicles. *EURASIP Journal on Wireless Communications and Networking*, 2024(1), Article 91. <https://doi.org/10.1186/s13638-024-02419-8>
11. Roy, K. S., Sujith, M., Bhanu, B., Preethi, & Hazarika, R. A. (2024). FPGA-based dual-layer authentication scheme utilizing AES and PUF for secure IoT edge devices. *EURASIP Journal on Wireless Communications and Networking*, 2024(1), Article 157. Springer Link
12. Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. *The Scientific World Journal*, 2013, Article ID 408280. <https://doi.org/10.1155/2013/408280>
13. Wang, X., Shi, Y., Zheng, K., Zhang, Y., Hong, W., & Cao, S. (2022). User authentication method based on keystroke dynamics and mouse dynamics with scene-irrelated features in hybrid scenes. *Sensors*, 22(17), 6627. <https://doi.org/10.3390/s22176627>
14. Xie, Y., et al. (2024). A lightweight dual-link accelerated authentication protocol based on NLFSR-XOR APUF. *Procedia Computer Science*. Elsevier.
15. Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognition*, 78, 242–251. <https://doi.org/10.1016/j.patcog.2017.10.002>