EasyChair Preprint

№ 11637

Advancing System Security: Biometrics, Cryptography and Authorization Protocols

Arun Shah

December 28, 2023

Advancing System Security: Biometrics, Cryptography and Authorization Protocols

Arun Shah

arun.shahie@gmail.com

Abstract: This article investigates the convergence of biometric authentication and authorization systems, looking at how they might be used to strengthen security measures across several domains. It examines how these technologies work together and clarifies how they might be used together to improve access control, strengthen identity verification, and reduce security threats. By means of an extensive examination of this combination, the research highlights the crucial function of biometrics in transforming authentication and authorization frameworks.

1. Introduction

The authentication and authorization nexus are where the security and seamless user experience imperatives meet in today's digitally connected world. A revolutionary era has begun with the development of biometric technologies, which provide unmatched accuracy in confirming personal identities through innate physiological or behavioral characteristics. Authorization controls access to resources or functionalities within a system, whereas authentication verifies a user's identity. Combining biometric authentication and authorization systems offers an alluring opportunity that promises enhanced security, reduced vulnerabilities, and simplified access control procedures. To alter the landscape of secure access protocols across many sectors, this article explores the fusion of these technologies.

Further, human-technology interactions have decreased during the past thirty years, but technological connections have increased. Differentiating genuine people is now more crucial than ever. For precise person identification, several industries, including forensics, border control, security access, and contemporary systems like smartphone locks, e-commerce, and e-governance, mostly rely on fingerprint-based technology [2]. Using fingerprints for identification works better than other biometrics like iris scans, voice recognition, or facial traits since they are assumed to be both constant and distinctive [5].

Because fingerprint-based identification systems are more affordable and inherently reliable than other biometric techniques, they have become more and more popular. Fingerprints are a very useful tool for identifying people in a variety of settings, from security checkpoints to contemporary digital platforms, because of their consistency and distinctiveness [3]. In contrast to

conventional password systems that are vulnerable to loss or human error, biometric authentication offers a safe and nearly unchangeable method of verification. With this technology, user experiences are streamlined, and security measures are strengthened since it provides a reliable and easy way to verify an individual's identification. Furthermore, fingerprint-based authentication is less expensive and more reliable. In contrast to passwords, which are vulnerable to theft, loss, or forgetfulness, biometrics provide a different approach to personal authentication by utilizing biological characteristics that never change. Unlike passwords, they can never be lost or forgotten, and they are difficult to duplicate [1].

As the gatekeeper of digital security, an authentication system verifies the identity of users trying to access data or systems. Its main purpose is to verify the authenticity of a person's identification using different techniques, like multifactor authentication, biometrics, tokens, and passwords. These systems prevent unwanted access by verifying users, making sure that only authorized individuals or organizations have access to private data or services. Systems for authentication are essential for safeguarding digital infrastructures, thwarting threats, and maintaining the integrity of data and systems. Such data integrity is essential for many small businesses [10,11].

Current development of biometric authentication techniques and the fortification of security frameworks have been the two main topics of recent authentication publications. Recent developments in biometrics—facial recognition, fingerprint scanning, and behavioral biometrics, in particular—have drawn attention for their potential to improve security while facilitating easier user authentication. Furthermore, the implementation of the Zero Trust framework is also an important topic which focus on strict access limits and ongoing verification to avert possible security breaches. Many difficulties exist in development of authentication systems for decentralized systems and securely implementing cryptographic methods in distributed networks to securely maintain identities. Multi-factor authentication (MFA) systems, which incorporate several aspects like biometrics, geolocation, and behavioral analytics, improves security.

2. Biometric Combined Protocols

In the field of AFIS (Automated Fingerprint Identification Systems), several approaches have proposed [4]. The best methods for user verification, from matching specific image segments to fine-grained alignment, comparison, and localization [4]. The core elements of fingerprint biometrics are the same for all of these different approaches: fingerprint collection, then pre-processing to remove duplication and prepare the sample for further steps. The process of feature extraction entails identifying pores, minutiae, and other unique fingerprint characteristics. To ascertain whether the user fits the

enrolled data, a similarity percentage is obtained by comparing these attributes with the previously computed template from the enrollment step. Any of these levels of success indicates that the implementation in a smart card setting is viable.

3. Biometric with Cryptographic Protocols

Combining biometric authentication and cryptography creates a strong security paradigm that makes use of both technologies' advantages. Biometric template protection is one important application. An individual's biometric data is represented by these templates, and cryptography is essential to their security. These templates are encrypted before being stored, so even if they are accessed, someone without the necessary decryption key cannot read them. By addressing worries about the possible disclosure of private biometric data, this method strengthens the biometric systems' overall security stance.

Furthermore, the creation of cryptographic keys based on biometric data is made possible by cryptographic procedures. Using biometric features, such fingerprints or iris scans, as a base, unique keys are created. These keys therefore make the encryption and decryption operations easier because they are generated from the intrinsic uniqueness of biometric features. This fusion increases the security and integrity of sensitive data and operations by directly integrating biometric data into cryptographic operations. This guarantees that only people with validated biometric credentials can access encrypted information or carry out cryptographic operations. Earlier issues and challenges in biometric protocols and their survey collections are available in [7,6] respectively.

4. Biometric with Authorization Protocols

By incorporating cryptographic approaches, authorization protocols can be improved and fortified, enhancing the security of access control mechanisms. Using cryptographic techniques to administer and enforce access control policies is one of the main approaches. Cryptographic techniques can be used to encrypt access control lists or policies, guaranteeing that only authorized parties have the decryption keys necessary to view or alter these documents. By doing this, harmful actors are prevented from making unauthorized changes or gains access, preserving the integrity of the authorization framework. Role based access control [8], usage control authorization models [13] and their implementation are discussed in [9,10,14].

Cryptographic mechanisms can also be incorporated into credentials or authorization tokens. Tokens that are cryptographically secure can store data about a user's responsibilities or access rights. These tokens can have their integrity and authenticity confirmed by the system by adding digital

signatures or encrypting them. This procedure ensures that only legitimate and authorized users can access resources or carry out particular tasks within the system, preventing tampering or forgery of access credentials. By combining cryptography and authorization protocols, the access control infrastructure is strengthened against unwanted attempts to acquire access and user credentials are guaranteed to be dependable.

5. Conclusion

The integration of biometric authentication, cryptographic techniques, and strong authorization mechanisms represents a significant advancement in strengthened security for modern systems. Through the use of cutting-edge cryptographic algorithms, this combination not only increases the accuracy of identity verification using biometric markers but also guarantees the integrity and security of critical data. Combining this with strict permission procedures creates a complex security layer that effectively protects access control systems. The interplay of biometrics, cryptography, and authorization protocols represents a holistic strategy for strengthening digital ecosystems, cultivating a paradigm where identity verification, data security, and access control work in unison to build robust and reliable systems.

References:

1. Venakatesan, N., and M. Rathan Kumar. "Finger print authentication for improved Cloud Security." In *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS*), pp. 434-439. IEEE, 2016.

2. Zhang, David D. "Personal Authentication." In *Automated Biometrics*, pp. 269-288. Springer, Boston, MA, 2000.

3. Jain, Anil K., Sharath Pankanti, Salil Prabhakar, and Arun Ross. "Recent advances in fingerprint verification." In *International conference on audio-and video-based biometric person authentication*, pp. 182-190. Springer, Berlin, Heidelberg, 2001.

4. Sanchez-Reillo, Raul, C. Sanchez-Avila, and L. Mengibar-Pozo. "Microprocessor smart cards with fingerprint user authentication." In *Proceedings. 36th Annual 2002 International Carnahan Conference on Security Technology*, pp. 46-49. IEEE, 2002.

5. Cucinotta, Tommaso, Riccardo Brigo, and Marco Di Natale. "Hybrid fingerprint matching on programmable smart cards." In *International Conference on Trust, Privacy and Security in Digital Business,* pp. 232-241. Springer, Berlin, Heidelberg, 2004.

6. Christian Rathgeb and Andreas Uhl, “A survey on biometric cryptosystems and cancelable biometrics”, *EURASIP Journal on Information Security*, volume 2011, Article number: 3, 2011.

7. U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, Biometric cryptosystems: issues and challenges, Proceedings of the IEEE, Volume: 92, Issue: 6, Page(s): 948 - 960, June 2004.

8. P.V. Rajkumar and Ravi Sandhu, “Poster: Security Enhanced Administrative Role Based Access Control Models”, *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1802-1804, Vienna, Austria, October 24-28, 2016.

9. P.V.Rajkumar, S.K.Ghosh, and P.Dasgupta, "An end to end correctness verification approach for application specific usage control", *Proceedings of IEEE International Conference on Industrial and Information Systems (ICIIS*), pp. 1-6, December 28-31, 2009.

10. P.V.Rajkumar, S.K. Ghosh, and P. Dasgupta, “Concurrent usage control implementation verification using the spin model checker”, *Proceedings of Recent Trends in Network Security and Applications: Third International Conference*, pp. 214-223, July 23-25, 2010.

11. K.Raghavan, M.Desai, and P.V. Rajkumar, “Multi-step Operations Strategic Framework for Ransomware Protection”, *SAM Advanced Management Journal*, Volume 85, Edition 4, 2020.

12. K.Raghavan, M.S. Desai, and P.V. Rajkumar, “Managing cybersecurity and ecommerce risks in small businesses”, Journal of management science and business intelligence, 2 (1), 9-15, 2017.

13. P.V. Rajkumar and R. Sandhu, “Safety Decidability for Pre-Authorization Usage Control with Identifier Attribute Domains”, *IEEE Transactions on Dependable and Secure Computing*, 17 (3), 465 – 478, 2020.

14. P.V. Rajkumar, S.K.Ghosh, and P.Dasgupta, “Application specific usage control implementation verification”, *International Journal of Network Security and Its Applications*, 1 (3), 116-128, 2009.