# Chapter 3
# Artificial Intelligence–Supported Bio–Cryptography Protection

**K. Sriprasadh**

https://orcid.org/0000-0003-2494-6151
*SRM Institute of Science and Technology, India*

## ABSTRACT

*Cryptography is a technological term to protect a secret message or information. The practices of converting the normal text into unreadable form are called encryption. It is possible through key management. Artificial intelligence is a technology that supports all domain in decision making. Bio-inspired cryptography is bio-cryptography that can identify the human unique features and covert as a key and incorporate in the encryption process through artificial intelligence multiple bio-cryptographic keys that can be linked into a single key module with artificial intelligence decision-making support in the decryption part. Through decision-making support, exact and accurate authentication can be made possible.*

## 1. INTRODUCTION

Cryptography is normally is done as a practice in the form of converting normal text into encrypted text the through key. Key may be symmetric and asymmetric, In the process of cryptography key is involved in converting the data into inaccessible format with the support of key. In the bio cryptography similar process can be considered .Initially bio cryptography should be analysed to know the knowledge about the bio cryptography. Cryptographic ideology which involves the human unique features in identifying and authenticating a user for provisioning the service is can be coined as bio cryptography (Alroobaea et al., 2022).

Organizations needs of security in a better manner the multiple types of authentication can be provided based on the various aspects of credentials, those data can be duplicated in one or in another form, so that such data for security should be replaced with the data or credentials that are not matched or duplicated for authentication trials. As the cyber criminals act in precise manner to match the security data with the fake data to satisfy the authentication, bio inspired cryptographic system is recommended for data

protection. The told authenticating system works with unique features of human. It can be considered for authentication purpose for providing ultimate security for human data.

Authentication in many ways can be considered for security of data or for accessing a device. Authentication is based on the users the authentication can be varied for the company staff and authentication can be different for the end users. Different level of authentication can be considered for people to people based on the knowledge level. Those security should be in a standardize manner assuring total security for the device or a service.

To understand in the better manner end users cannot use multiple or two level authentication as technical or educated person does. But similar level security should be provided to their earning and belongings. For this reason Bio cryptography can provide a multi or similar protection. In this book chapter multiple unique human features are matched and mapped in a single verification term.That will provide them an authentication proven system.

Authentication model can considered in two ways they are

1. Based on the security model
2. Based on the User level of usage

Let's take a closer look at the many sorts of authentication techniques available:

*Figure 1. Different types of authentication*
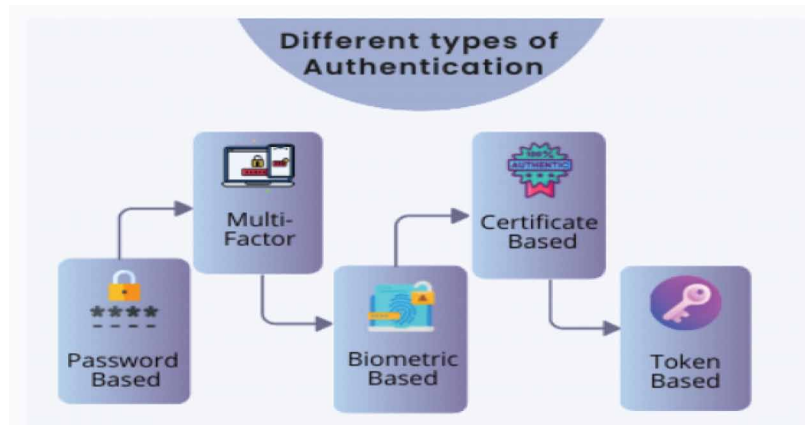


## 2. LITERATURE REVIEW

A literature review has been done on various biometrics factor for authenticating a user, based on users' own identical property that the user possesses to provide the security to the user and user data.

Through table 1, the following error correction ideology are studied, and show cased for the user as for the understanding from the table 1, keystroke-based bio-metric security and voice recognition, error correction is made through discretization it was referred from Monrose et al. (1999). Signature identification ideology is understood from Hao and Chan (2002). In this ideology, signature velocity forward features and backward features are understood in the form of graphical representation here error

## Related Content

Quantum Cryptography: Basic Principles and Methodology

Satish Rupraoji Billewar, Gaurav Vishnu Londheand Sunil Bahiru Ghane (2021). *Limitations and Future Applications of Quantum Cryptography (pp. 1-20).*

www.irma-international.org/chapter/quantum-cryptography/272362

Empowering Secure Communication With Specific Triangular Matrices: Practical Examples Unveiled Using Different Approximations

Özen Özer Özerand Nadir Subasi (2024). *Innovations in Modern Cryptography (pp. 270-291).*

www.irma-international.org/chapter/empowering-secure-communication-with-specific-triangular-matrices/354043

Cryptographic Voting Protocols

Kannan Balasubramanianand Jayanthi Mathanan (2018). *Algorithmic Strategies for Solving Complex Problems in Cryptography (pp. 124-133).*

www.irma-international.org/chapter/cryptographic-voting-protocols/188518

Secure Multi-Party Computation (SMPC) Protocols and Privacy

Mosiur Rahaman, Varsha Arya, Sheila Mae Orozcoand Princy Pappachan (2024). *Innovations in Modern Cryptography (pp. 190-214).*

www.irma-international.org/chapter/secure-multi-party-computation-smpc-protocols-and-privacy/354040

Post-Quantum Lattice-Based Cryptography: A Quantum-Resistant Cryptosystem

Aarti Dadheech (2021). *Limitations and Future Applications of Quantum Cryptography (pp. 102-123).*

www.irma-international.org/chapter/post-quantum-lattice-based-cryptography/272367