Privacy Preserving Biometric Authentication

E. Bertino\textsuperscript{1}, S.J. Elliott\textsuperscript{2}, A.Bhargav-Spantzel\textsuperscript{1}, A.C.Squicciarini\textsuperscript{1}, S. K. Modi\textsuperscript{2}
\textsuperscript{1}CERIAS, \textsuperscript{2}Department of Industrial Technology. Purdue University

Introduction:

• One approach to the problem of reducing the threat of identity theft is the widespread adoption of systems using biometrics authentication.
• Improper storage and use of identification credentials raises several security and privacy risks.
• The goal is to provide a privacy preserving methodology for strong biometric authentication in federated identity management systems.

Advantages:

• Privacy Preserving Multifactor Authentication \textsuperscript{[1]}: multifactor authentication is essential for secure authentication mechanisms. The identity management framework is used to provide proofs of multiple strong identifiers for a given user.

• Interoperability: Our scheme provides an interoperable, usable, secure, and inexpensive to use biometric authentication in a federation.

• User Control: The raw biometric never leaves the client machine therefore providing complete control to its owner.

Primary Tools Used:

• Secure Sketches: Fuzzy key storage mechanism which allows to recover a secret key $w$ from a faulty reading $w'$ of $w$.

• Zero Knowledge Proof: Interactive method allowing one party to prove to another that a statement is true, without revealing anything other than the veracity of the statement.

Authentication Phases:

• Registration: The integer commitment corresponding to the recorded biometric template is sent to the registrar.

• Authentication: The recover module reproduces the originally stored biometric template which is used by the ZKP module to form the correct proofs for authentication.

Reference: