Với khả năng chống tấn công tuyệt vời Argon2 được ứng dụng rộng rãi trong thực tế, đặc biệt là ứng dụng trong việc bảo vệ mật khẩu

1/Quản lý mật khẩu

Khi lưu trữ mật khẩu, vấn đề cần quan tâm bậc nhất là việc mật khẩu không thể bị tìm ra bằng 1 cách thức tấn công nào. Argon2 với khả năng bảo mật thuộc loại tốt nhất hiện nay hoàn toàn đáp ứng được yêu cầu này. Trong thực tế ta hoàn toàn có thể tự sử dụng argon2 để băm và lưu trữ mật khẩu phục vụ cho mục đích cá nhân hoặc tổ chức. Ta có thể dễ dàng bắt gặp các hệ thống quản lý mật khẩu đang sử dụng Argon2 như LastPass và KeePass

+ LastPass là 1 trình quản lý mật khẩu trực tuyến phổ biến nhất được tích hợp trong đa số trình duyệt hiện nay

+ KeePass là trình quản lý mật khẩu hỗ trợ chủ yếu cho Window, phục vụ cho việc lưu trữ và quản lý mật khẩu

2/Bảo vệ dữ liệu

Mặc dù thời gian băm và xác thực khá chậm so với các hàm băm hoặc các thuật toán mã hóa khác, Argon vẫn được sử dụng để bảo vệ những dữ liệu quan trọng nhằm chống lại các cuộc tấn công đánh cắp dữ liệu trên máy chủ hoặc các máy cá nhân. Việc băm dữ liệu bằng Argon2 có thể nói là bảo đảm an toàn gần như tuyệt đối, việc đọc hay ghi dữ liệu được mã hóa bằng Argon2 (được cấu hình chính xác) là chưa được ghi nhận.

3/Xác thực

Đôi khi Argon2 còn được sử dụng như hỗ trợ cho việc xác thực người dùng. Thông tin của người dùng trong hệ thống được lưu lại và băm bằng Argon2. Việc này làm giảm tối đa tấn công chiếm quyền điều khiển ngăn chặn hacker truy cập vào hệ thống khi chưa được cấp phép. Một số giao thức bảo mật đang sử dụng Argon2 có thể kể đến như OAuth và OpenID Connect

4/Blockchain

Công nghệ chuỗi khối Blockchain không còn quá xa lạ với chúng ta trong thời điểm hiện tại. Argon2 được sử dụng để mã hóa khối trong Blockchain đảm bảo tính toàn vẹn của hệ thống chống tấn công sửa đổi ở mức độ cao. Tiêu biểu có thể kể đến trong dự án Moreno hoặc ít phổ biến hơn là Wownero và Koto. Do tính năng khó bị tấn công, có thể trong tương lai sẽ có nhiều dự án Blockchain sử dụng Argon2 để mã hóa các khối