ARSAGON: An Integrated Approach Combining Symmetric, Asymmetric, and Hashing Algorithms for Multi-Factor Authentication (MFA)

Authors:

[1,2]Mursalim, [1]Yulaikha Maratullatifah, [1]Nevin Shera Adji

[1]University of Sugeng Hartono, [2]Universitas Gadjah Mada

Outline

- Introduction
- Methods
- Experiment
- Result and Discussion
- Conclusion
- Acknowledgement

Introduction

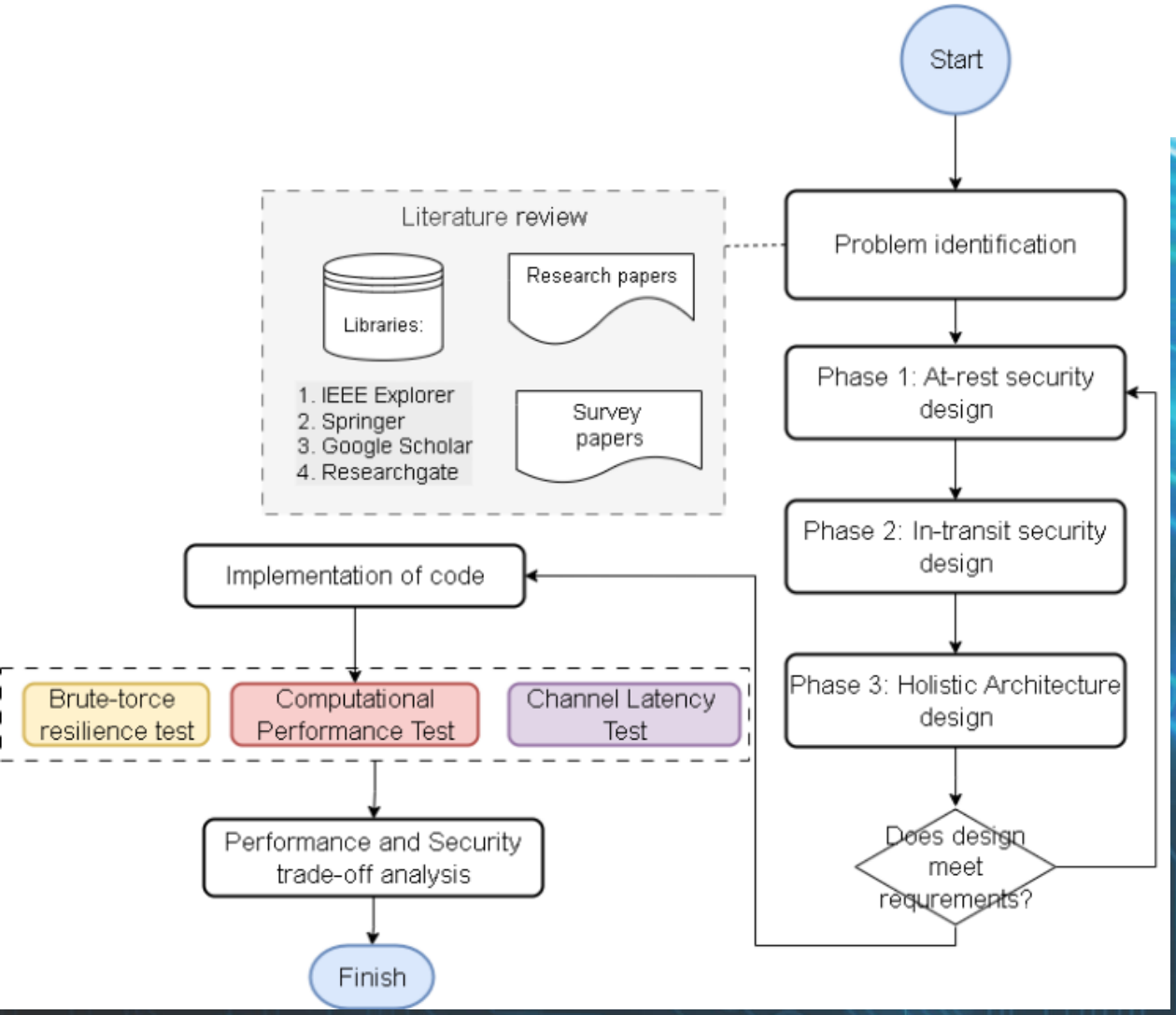
The Inadequacy of Single-Layer Defense & The Need for a Holistic Architecture

Why a single defense is less effective?

Limitations of single Authentication?

ARSAGON: Holistic Architecture

Methods

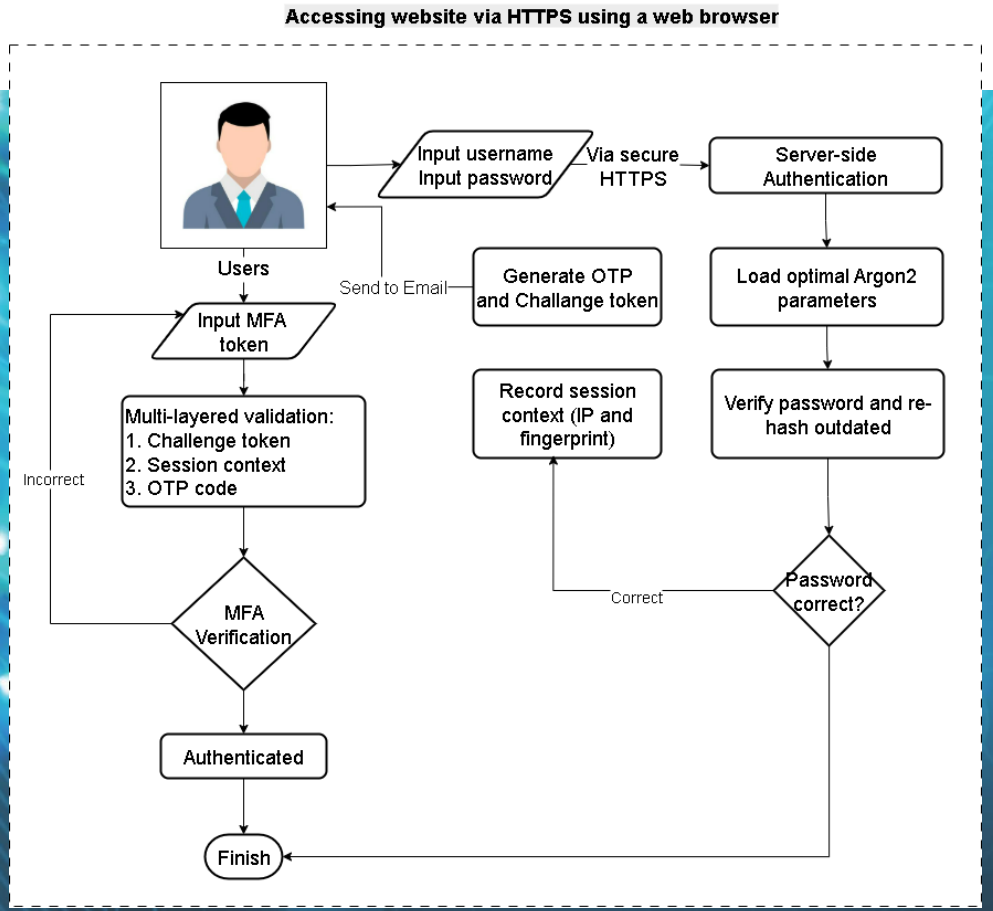


1. Architecture design
2. Implementation and testing
3. Analysis of result

Methods

The proposed methods is divided into 3 sequential phases:

1. Primary Authentication & Adaptive Hashing
2. MFA Challenge Phase
3. Multi-Layered Validation Phase



Experiment

Algorithm: ARSAGON

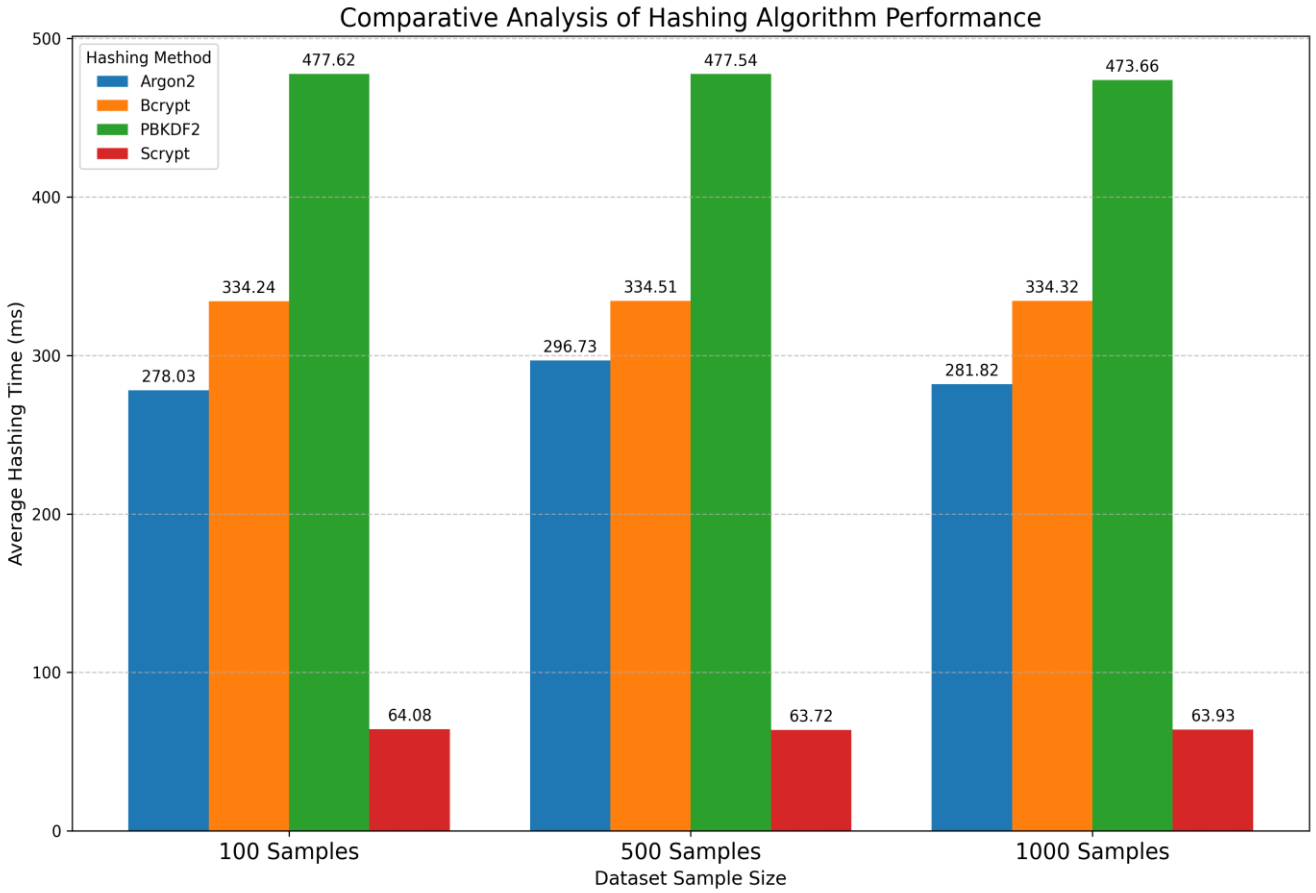
Input: Auth (user, pass), mfa_acc (OTP, chal_t)
Output: Authenticated success or failure

```
1:  Function LoginUser(Auth)
2:      User ← Auth(Auth.user, auth.pass)
3:      IF user != 0 Then
4:          UpdateHash(user, auth.pass)
5:          Chal_data ← GenMFAChal(user, req.cont)
6:          SendOPT(user.email, chal_data.otp)
7:          Return ReqMFAVer(chal_data.chal_t)
8:      Else:
9:          Return AuthFail
10: End IF
11: End Function
12: Function AuthMFA(mfa_acc)
13: Is_valid ← VerifyMultiMFA(mfa_acc, sess.chal_data)
14: IF is_valid != 0 Then
15:          User ← GetUserFromSess()
16:          LoginUser(user)
17:          ClearMFASessData()
18:          Return AuthSuccess
19: Else:
20:          Return AuthFail
21: End IF
22: End function
```

- The ARSAGON method is implemented through 2 primary functions that separate the authentication flow into distinct phases:

1. Function LoginUser(Auth)
2. Function AuthMFA(mfa_acc)

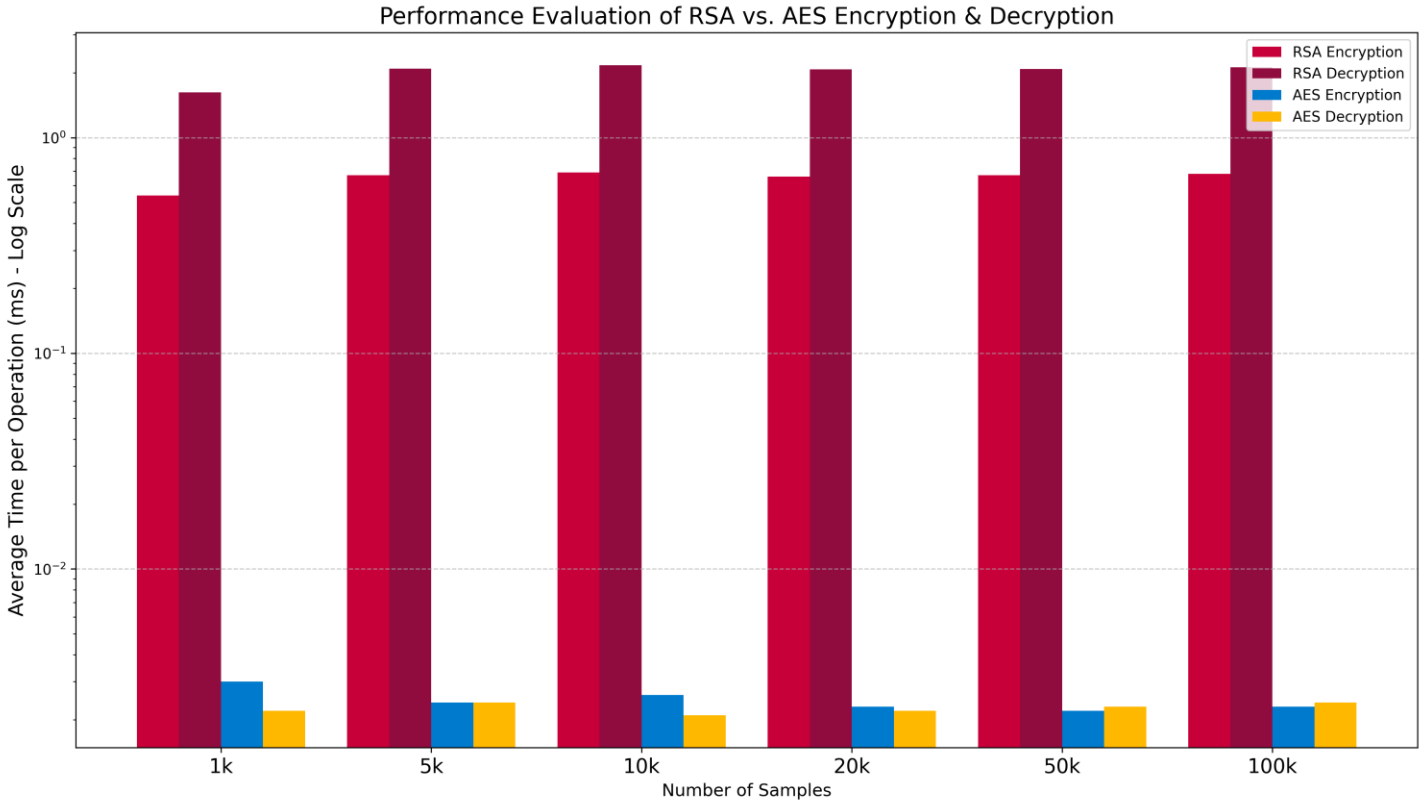
Result



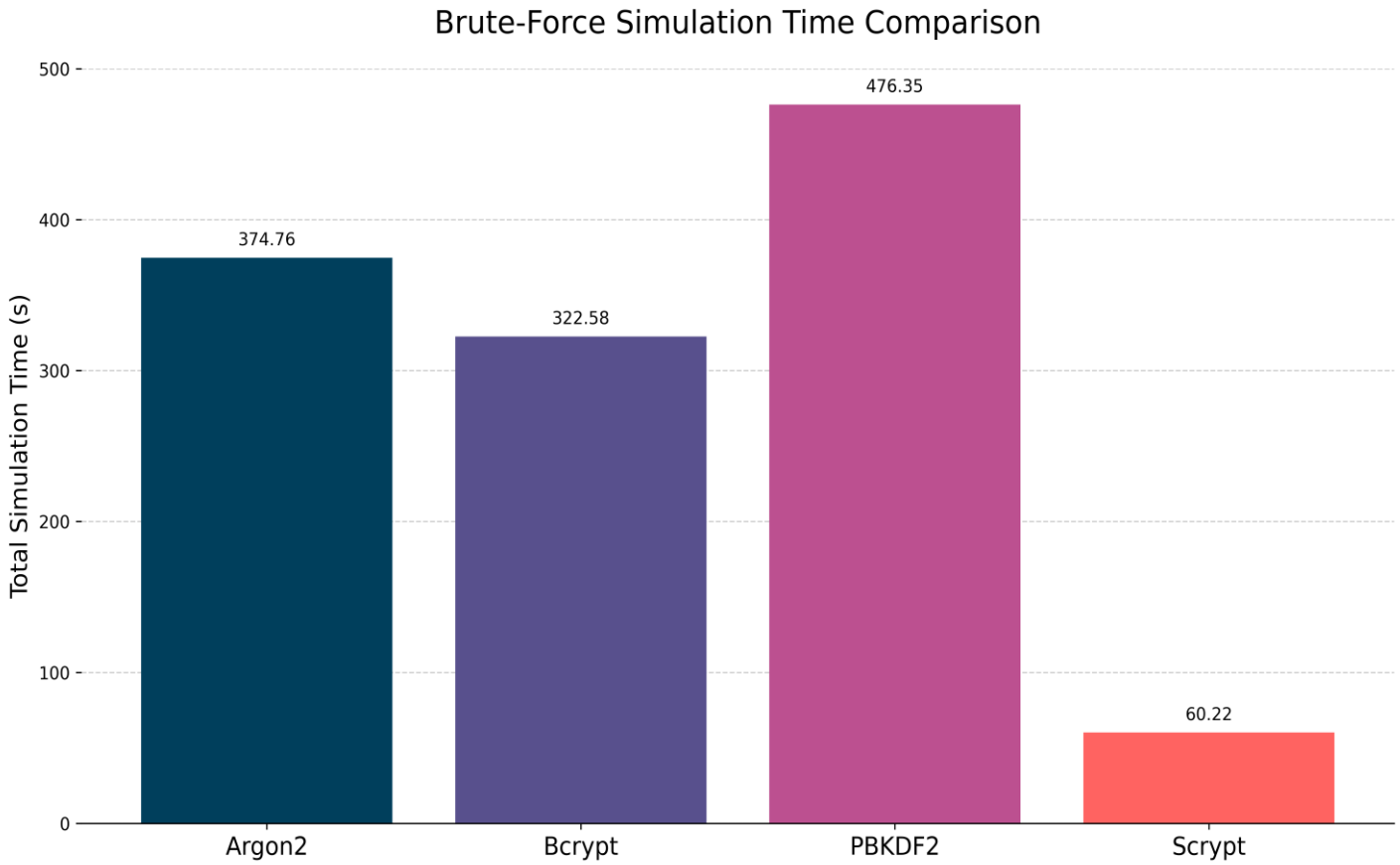
- The methods provide good result, Argon2 still remain stable and consitenacy approximately 200 above.
- ARSAGON, which main core is Argon2 obtain 278,03 (100 samples), 296,73 (500 samples) and 281,82 (1000 samples).
- Those result are significantly more computationally expensive than Scrypt.

Result

- Results: In-Transit Component Performanced text

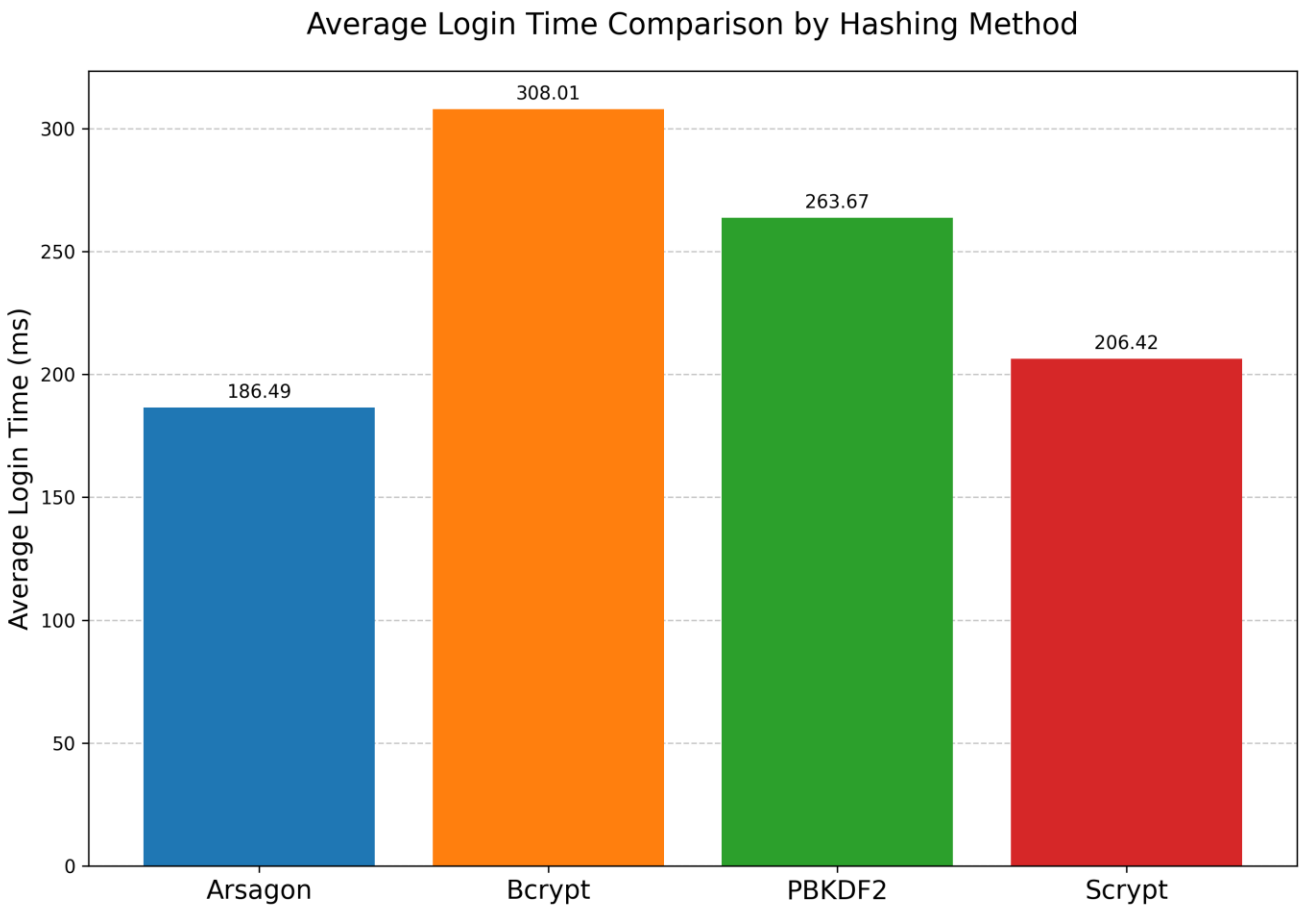


Result



- Brute-Force Simulation Time Comparison
- based on the empirical results, ARSAGON recorded a time of 374,76 s, which outperforms both Scrypt and Bcrypt methods.
- The result demonstrated that ARSAGON and PBKDF2 require significant computational resource to successfully attack from an attacker

Result



- End-to-End Authentication Latency involved four algorithm such as Arsagon (Argon2), Bcrypt, PBKDF2, dan Scrypt
- ARSAGON, achivied the lowest average login time at 186,49 ms
- Bcrypt and PBKDF2 were slower, with total login times of 308.01 ms dan 263.67 ms.

Result

Context	:	'IP': '127.0.0.1', user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64 … Chrome/138.0.0.0 Safari/53.7.36
Challenge token	:	Z0WytIv0u5Lj…0G8NA
Content-Type	:	Text/plain; charset="utf-8"
MIME-Version	:	1.0
Content-Transfer Encoding	:	7bit
Subject	:	Verification code
From	:	noreplay@arsagon.com
To	:	Mursalim.dsc@gmail.com
Date	:	Mon, 21 Jul 2025
Message-ID	:	<175308878032.11256….
Verification code	:	653790

Result

Challenge stored in session	**:**	**Z0WytIv0u5LjU0kWrKJcN2c…NAAwPfz0**
Challenge sent to browser	:	Z0WytIv0u5LjU0kWrKJcN2c…NAAwPfz0
Context stored in session	:	'IP': '127.0.0.1', user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64 … Chrome/138.0.0.0 Safari/53.7.36
Context on browser	:	'IP': '127.0.0.1', user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64 … Chrome/138.0.0.0 Safari/53.7.36
LOGIN	:	SUCCESS
Username	:	Mursalim
Password Hash	:	Argon2$argon2id$v=19$m=131072,t=5, p=8$SktXYNWsSU1MsPhv1Kgi5mgKrcAq/z6dLKDNqC5tdTxbcFc

Discussion

- This work successfully designed and validated ARSAGON, a holistic security architecture featuring an adaptive Argon2 for at-rest security.
- The Architecture provide a defense-int-depth approach by integrating robust at-rest security with industry standard TLS/HTTPS protocol for in-transit protection.
- The empirical determined optimal parameters for Argon2 were a time cost of 5, a memory cost of 131072 KiB and parallelism degree of 4.
- Brute-force simulations demonstrated that ARSAGON imposes a significantly higher computational cost on attackers, outperforming both Bcypt and Scrypt.
- End-to-end latency testing revealed a low average login time of 186,49 ms, confirming the system's practical efficiency without compromising user experience.

Conclusion

Contributionof the research

Proposed ARSAGON, a holistic security architecture that integrates:

- **Adaptive Argon2 for robust at-rest security**
- **Advanced MFA (OTP, Challenge token, context) for enhanced, phishing-aware security Standard HTTPS/TLS for in-transit protection**

Empirically demonstrated that ARSAGON archicteture provides:

- **Superior brute-force resilience compared to Bcrypt and Scrypt**
- **An efficient end –to end login latency of 186,49 ms, ensuring a positive user experience**

Limitation & Future Work

- The study did not include a formal ablation study to quantify the spesific security contribution of each individual MFA component
- Future work will focus on:
- Conductiong the aformenetioned ablation study
- Exploring the integration of Post-Quantum Cryptograpy (PQC) to ensure long-term resilience against future threats.

THANK YOU

Any Question?

Contact please : Mursalim
Email: mursalim.dsc@gmail.com |
mursalim.dsc@sugenghartono.ac.id

Q&A | Additional Presentation