**Form 4: Results and conclusion**

**1. Team No:** 11

**2. Project Title**: Investing and finding a DNA Cryptography layer for securing data in spark cluster.

**3. Experiment Environment:**

Execution Requirements:

Operating System : Linux(Ubuntu)

Latest version of VSCode 1.60.0.Apache Spark (Latest Version) and NodeJS (Version 18.8.1).

ExpressJS (version 4.18.2) library has been included to harness its capabilities for building a robust and responsive webserver.

Nodemailer (3.0.3) module for Node.js that is used for sending emails.

Parameter Formulas:

The current spark cluster security mechanism consumes

T(SC)=U[(6t)+x+y] +O(N)

The developed Spark Cluster security mechanism consumes

T(SAI)=U(5) +[O(N)+D]

**4. a Experiment 1:**

Metadata Security existing and proposed Mechanisms.

|  |
| --- |
| Number of times Updation Number of times Updation |
| Required(Existing) Required (Proposed) |
| User1 8 1 |
| User2 16 2 |
| User3 24 3 |

The above table is showing for 3 Spark salve nodes metadata information existing which is updating every 8 seconds, but the proposed security mechanism can update every 64 seconds for reducing the computational burdens.

**Findings:**

* Reduces update frequency to every 64 seconds.
* The proposed mechanisms demonstrate significant improvements in computational efficiency and metadata security.

**4. b Experiment 2:**

Security Configurations existing and proposed

**Findings:**

* Consolidates security into 1 configuration.
* Eliminates metadata security computations.

**4. c Experiment 3:**

User Authentication computation

The following table showing the 10 users wants login single node cluster and the required to authentication by using Kerberos before entering the cluster. Every time they request KDC for each session which is taking 10 computation per session, each users may request authentication KDC depending on their usability of cluster.

|  |
| --- |
| No.of sessions Total Number of Time Total |
| Authentications/ Computations Authenticated/ Computations |
| Day (Existing) Day(Proposed) |
| User1 5 50 2 8 |
| User2 10 100 3 12 |
| User3 8 80 4 16 |
| Total 23 230 9 36 |

Table shows the user sessions and total computations of existing and proposed authentication.

**5. Parameter comparison table**

|  |  |  |
| --- | --- | --- |
| Parameter | Previous methods | Proposed method |
| Metadata Security | Requires metadata updates every 8 seconds | Significantly reduces computational burdens. |
| Security Configurations | Involves 2 security configurations. | Consolidates security into 1 configuration. |
| User Authentication | Total computations for authentication reach 230 for 3 users. | Total computations for authentication are reduced by 84% for 3 users. |

**6. Final Conclusion Statements**

A Secure E-Authentication Layer (SEAL) as a secure layer which positioned above the Spark Cluster. This mechanism provides better authentication for the spark cluster by using limited computations and providing better user security from hackers. The main objective is to design layer to implement node-sensitive data hiding using DNA sequences and provide security to the user and its data from hackers.

**Signature Supervisor**