Native language encryption for secure storage of User credentials in Database

Final Year Project

BY

HIRESH R 310620106044

EASWARI ENGINEERING COLLEGE

OUTLINE

- Objectives
- Introduction
- Literature Survey
- Existing Methodology
- Proposed Methodology
- Results and Discussion
- Publications
- References

OBJECTIVES

- Implement Tamil Language Hashing
- Cultural Integration
- Security Enhancement

INTRODUCTION

The project methodology takes a meticulous approach, outlining the step-by-step implementation of Tamil language hashing. This encompasses the design and development of the hashing algorithm itself, its seamless integration into a secure password management system, and a rigorous evaluation of its performance and robustness under various conditions. The emphasis on system architecture ensures that the native language encryption is seamlessly woven into the fabric of secure credential storage, aligning with cultural nuances and relevance.

LITERATURE SURVEY

S.NO	JOURNAL DETAILS	TECHNIQUES USED	INFERENCE
1.	"A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," by J. H. Cheon and J. Kim, in IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1052-1063, May 2015, doi: 10.1109/ TIFS.2015.2398359.	PKE-SHE Integration, Homomorphic Decryption Optimization, private-key SHE to public-key SHE	Hybrid Efficiency, Decryption Optimization, database encryption and cloud computing
2.	"Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps" by Barreto, Libert, McCullagh, and Quisquater. It was standardized in IEEE 1363.3 and in ISO/IEC 14888-3:2015.	Bilinear Pairings, Innovative Identity-Based Signature, pairing calculations and verification algorithms, Framework Evaluation	Cryptographic tool that combines confidentiality, authentication, and non-repudiation, efficiency gained through bilinear mappings over elliptic curves.

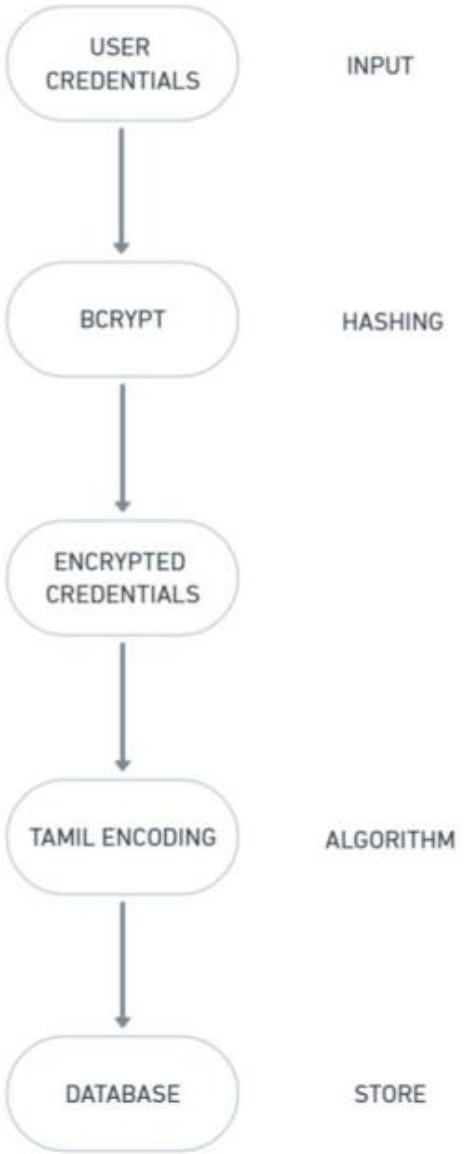
LITERATURE SURVEY

S.NO	JOURNAL DETAILS	TECHNIQUES USED	INFERENCE
3.	"Implementation of cryptographic algorithm for secured communication in tamil language using python program." By M. Vivek Prabu, R. Karthika; AIP Conf. Proc. 24 May 2023; 2718 (1): 050002.	Symmetric encryption algorithms such as AES or DES, management system to generate, store, and exchange encryption,	Sensitive information shared in Tamil can be protected from eavesdropping and unauthorized access
4.	"Secure storage of user credentials and attributes in federation of clouds." By Luciano Barreto, Leomar Scheunemann, Joni Fraga, and Frank Siqueira. 2017. In Proceedings of the Symposium on Applied Computing (SAC '17). Association for Computing Machinery, New York, NY, USA, 364–369	Secret Sharing, Distributed Databases, employs OpenID Connect , Prototype Implementation.	Address security concerns in cloud federations by securely storing user information using secret sharing techniques, uses of Identity Providers (IdPs) for authentication.

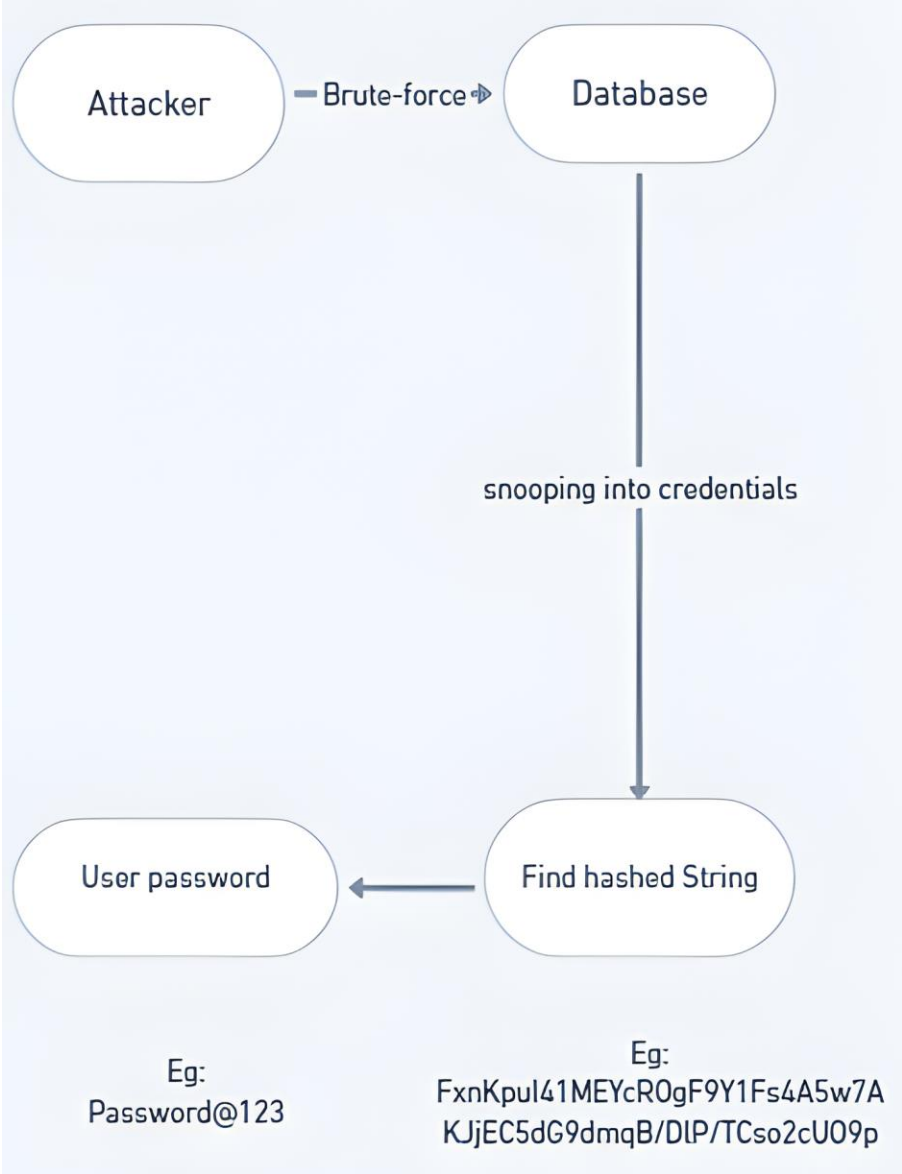
LITERATURE SURVEY

S.NO	JOURNAL DETAILS	TECHNIQUES USED	INFERENCE
5.	Y. Yasumura, H. Imabayashi and H. Yamana, "Attribute-based proxy re-encryption method for revocation in cloud storage: Reduction of communication cost at re-encryption," *2018 IEEE 3rd International* Shanghai, China, 2018, pp. 312-318, doi: 10.1109/ICBDA.2018.8367699.	Attribute-based Encryption (ABE), Combining ABE with a symmetric encryption scheme, Proxy Re-encryption, Symmetric Encryption Scheme.	Re-encryption of data, resulting in significant communication costs and computational burdens, ABE and Syalim's encryption scheme reduces communication costs between the data owner cloud storage.
6.	K. Honda, J. Lee, H. Kim, M. Cho and M. -C. Lee, "Enhanced security computational double random phase encryption by using additional random function," 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2021, pp. 155-159, doi: 10.1109/ICTC52510.2021.9621077.	Double Random Phase Encoding (DRPE), Computational Encryption, Additional Random Function	Enhanced Security, Resistance to Attacks, obust against cryptanalysis techniques, organizations can ensure robust protection for their critical information assets.

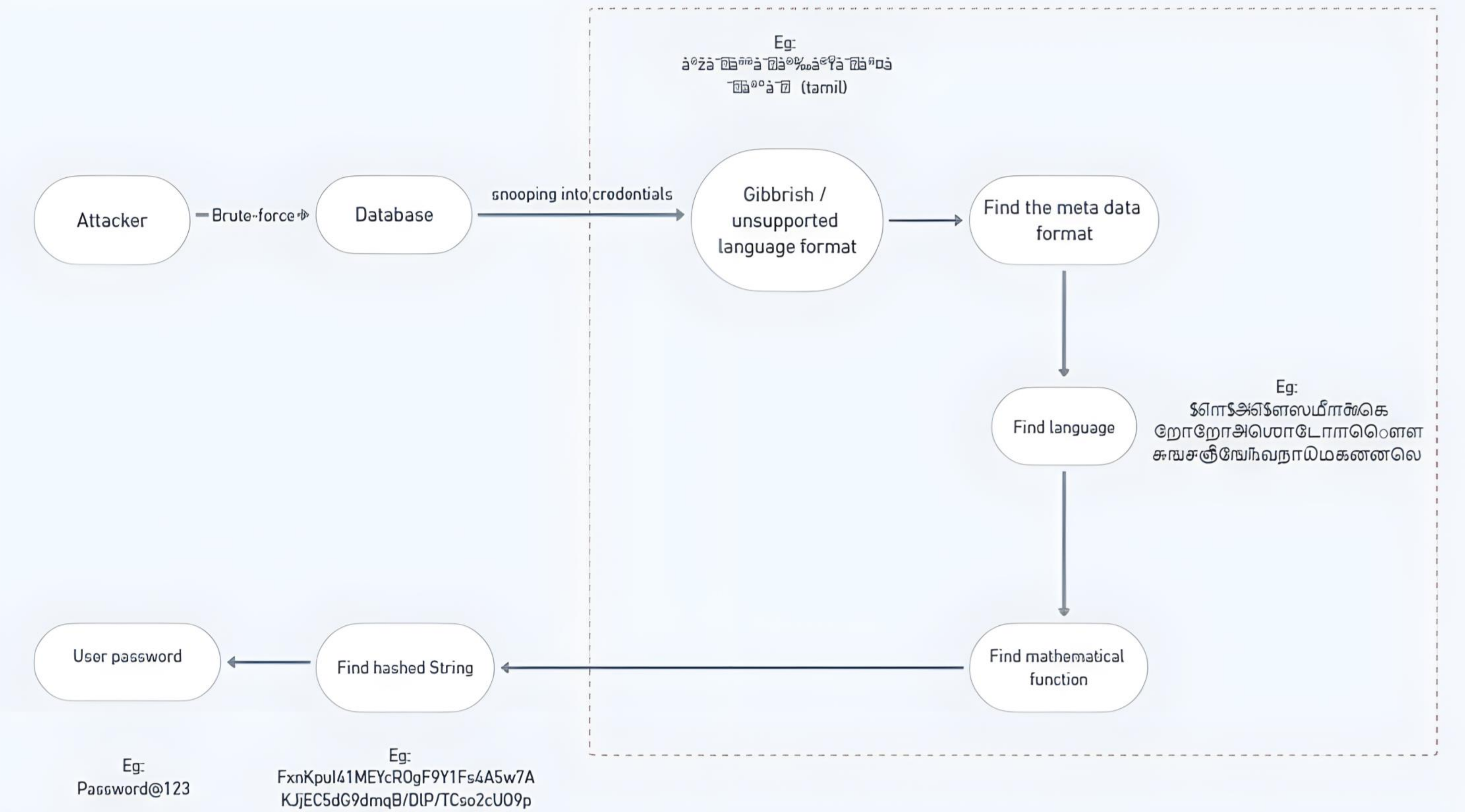
BLOCK DIAGRAM



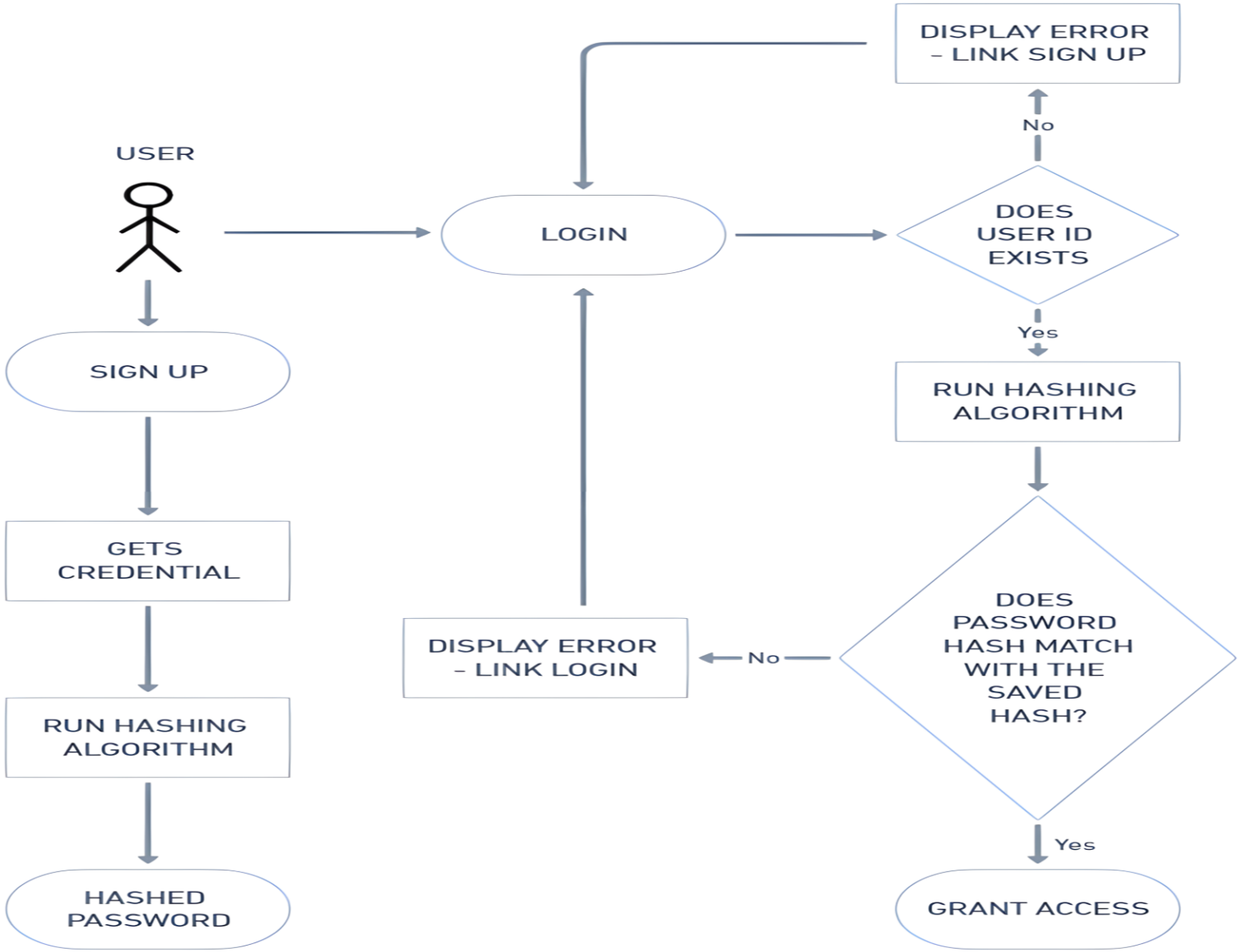
EXISTING SYSTEM



PROPOSED SYSTEM



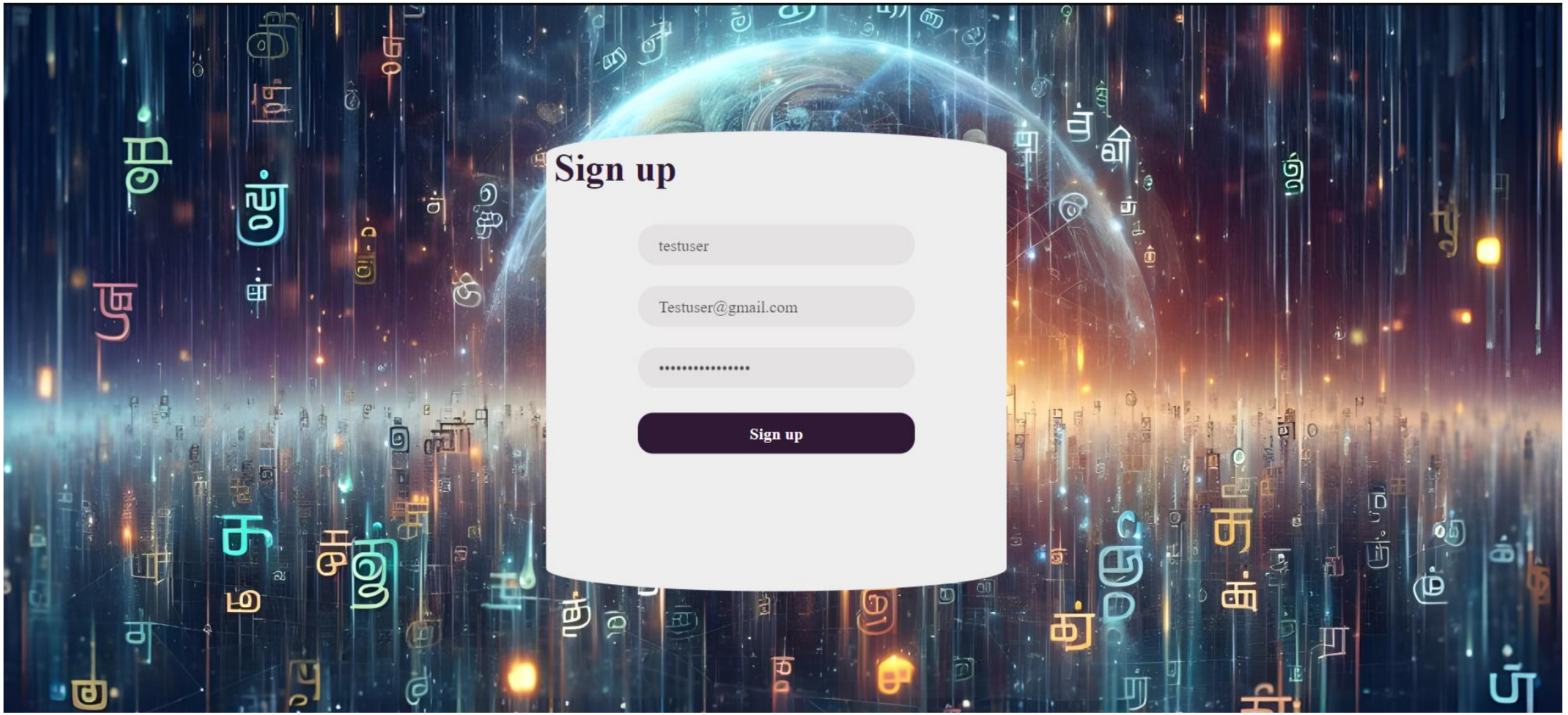
WORKING


USER
SIGN UP
GETS CREDENTIAL
RUN HASHING ALGORITHM
HASHED PASSWORD
LOGIN
DISPLAY ERROR – LINK LOGIN
No
DOES PASSWORD HASH MATCH WITH THE SAVED HASH?
Yes
GRANT ACCESS
RUN HASHING ALGORITHM
Yes
DOES USER ID EXISTS
No
DISPLAY ERROR – LINK SIGN UP

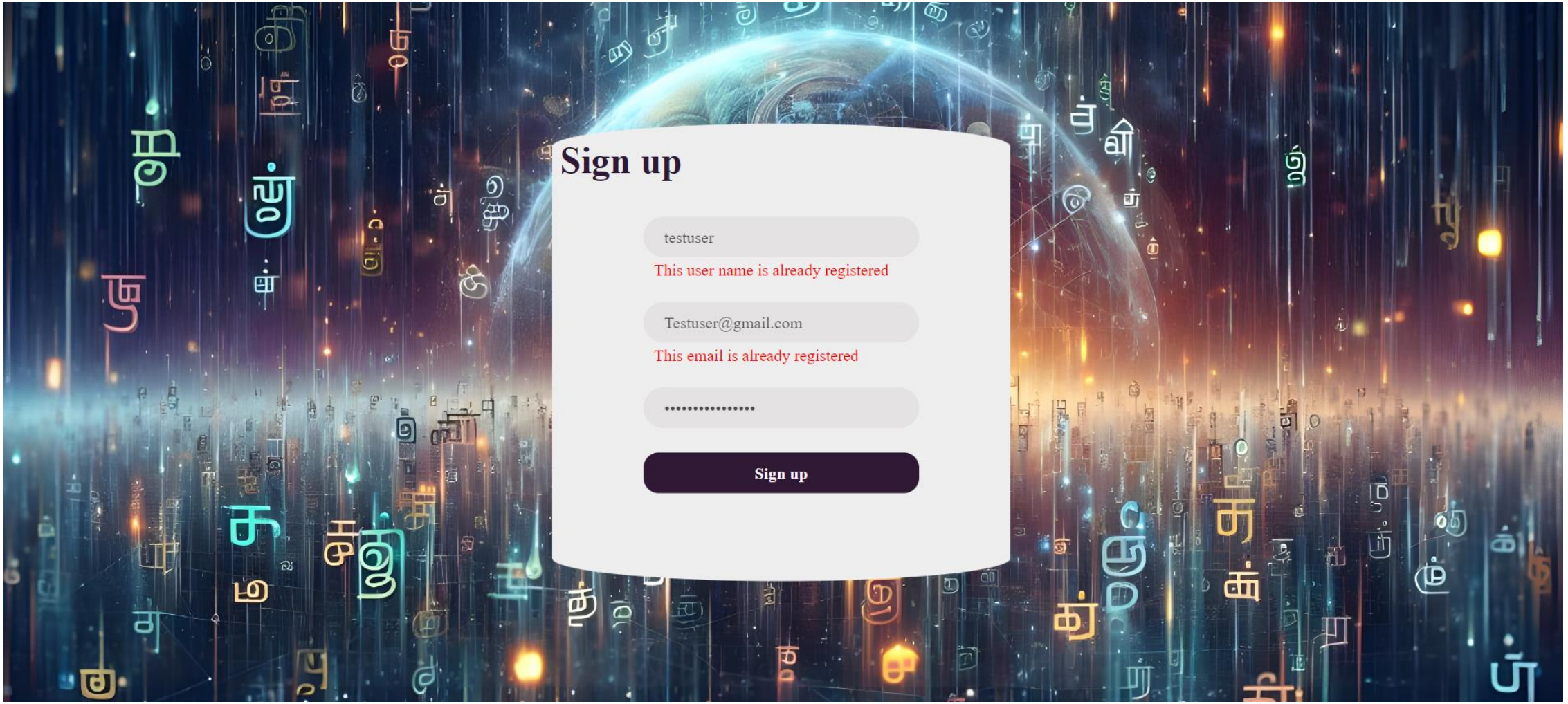
RESULTS

Initial Sign up page ➔

Enter the details ➔

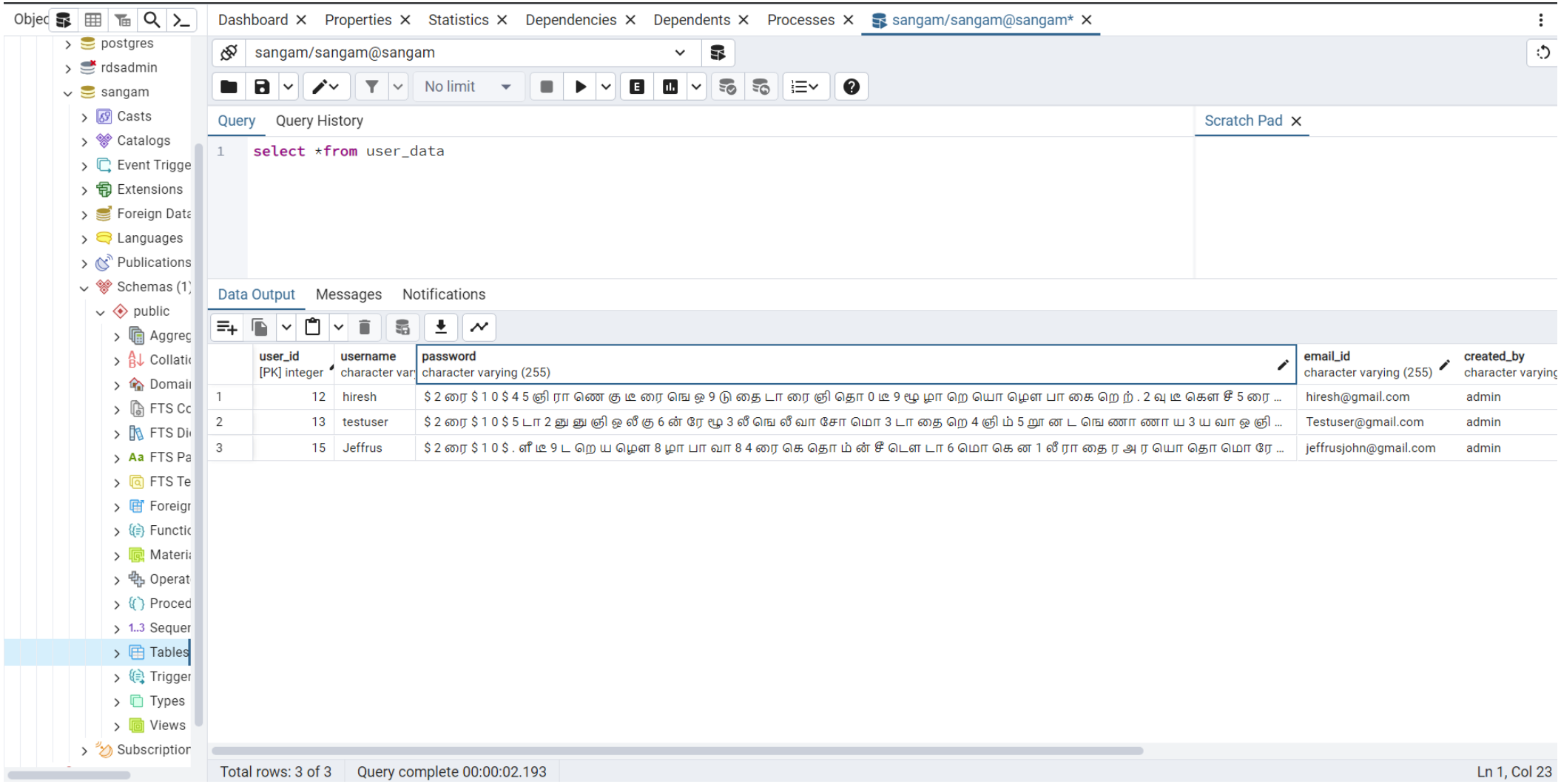


User created successfully ➔



RESULTS

In the AWS postgresql Database ➔

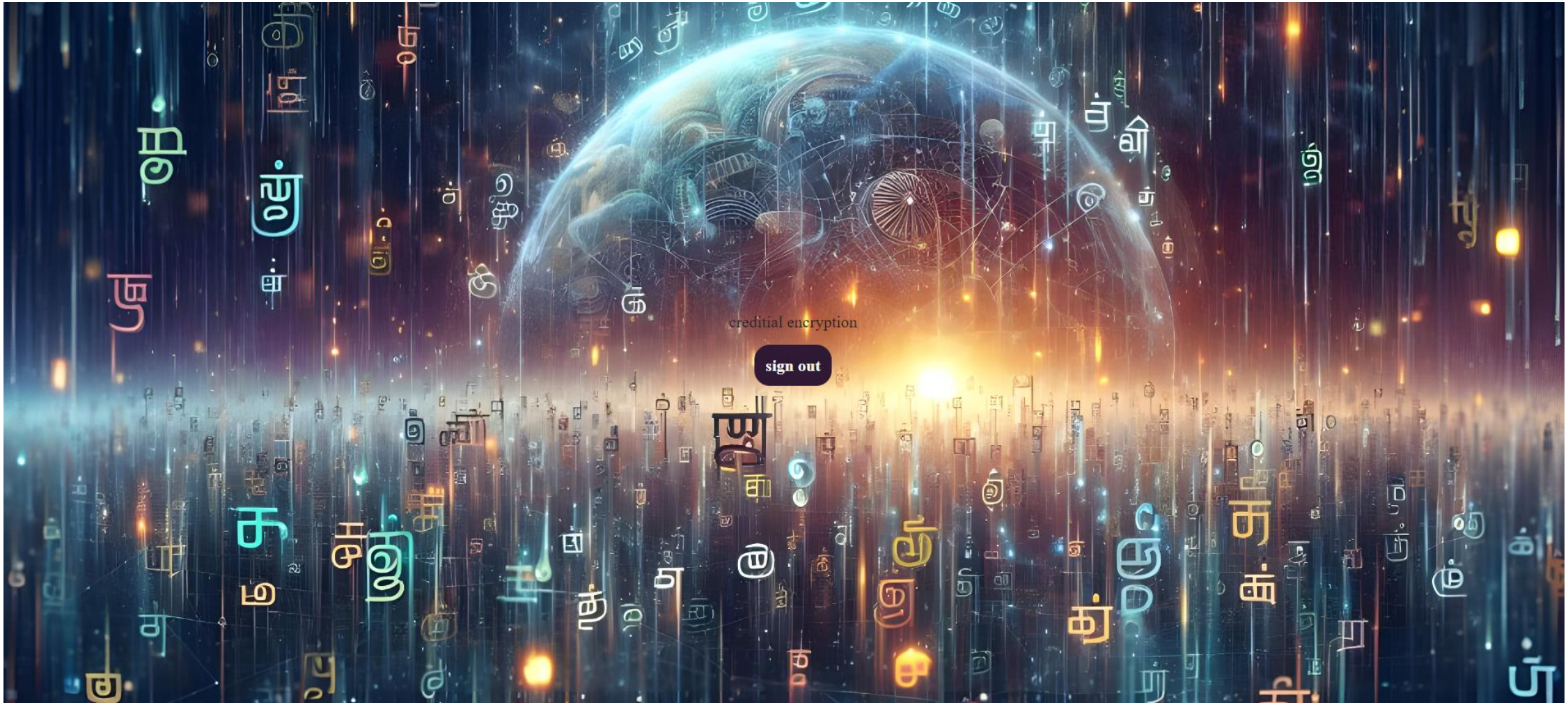


TESTING

Sign in ➔

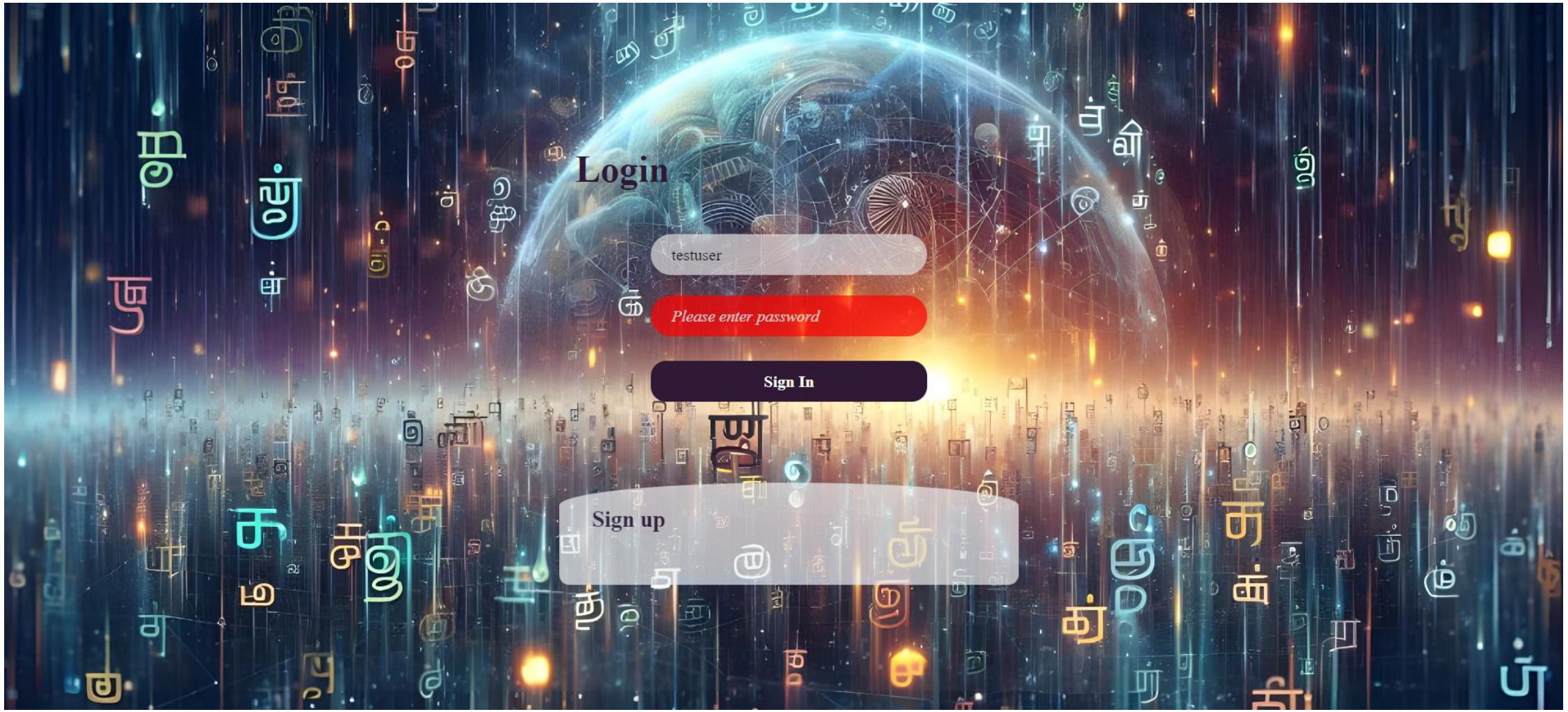
TESTING

Successful login when correct Credentials are given ➔



TESTING

When wrong credentials are given ➔



FUTURE DISCUSSION

- **Secure communication**

The algorithm could be used to develop secure communication protocols for Indian businesses, organizations, and individuals. This could help to protect sensitive information from being intercepted by attackers.

- **Data protection**

The algorithm could be used to protect sensitive data such as government records, financial transactions, and personal information. This could help to prevent data breaches and identity theft.

- **Anonymous communication**

The algorithm could be used to develop anonymous communication protocols for Indian users. This could help to protect users from online surveillance and tracking.

- **E-voting**

The algorithm could be used to develop secure and anonymous e-voting systems for Indian elections. This could help to improve the integrity and fairness of elections.

CONCLUSION

The proposed Tamil encryption has the potential to be a valuable tool for Indian users. The algorithm is accessible, secure, and efficient, and it can be tailored to the specific needs of Indian users. Additionally, the algorithm can help to promote the use of Tamil in the digital world.

I believe that the development and deployment of the proposed “Native language encryption for secure storage of user credentials in database” is a worthwhile endeavor. The potential benefits of the algorithm are significant, and the challenges can be overcome. I hope that more people will join me in supporting the development of this important technology

PUBLICATIONS

CONFERENCE:

ICDCS2024 - 573
ACCAI-2024 ACCAI-24-17-5375

JOURNELS:

VJST – Result Pending
IJRESM-0102 - Awaiting Payment
Cyber Security and applications - Result Pending

REFERENCES

[1] "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," by J. H. Cheon and J. Kim, in IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1052-1063, May 2015, doi: 10.1109/ TIFS.2015.2398359.

[2] "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps" by Barreto, Libert, McCullagh, and Quisquater. It was standardized in IEEE 1363.3 and in ISO/IEC 14888-3:2015.

[3] “Modeling and simulation of a Tamil language encoder for advanced encryption technologies”, By S Suthaharan, Volume 4, Issue 7,2023,100740,ISSN 2666-3899.

[4] "Tamilian cryptography: An efficient hybrid symmertric key encryption algorithm" by R Geetha, T Padmavathy, T Thilagam and A Lallithasree, Wireless Personal Communications, pp. 1-16, 2019.

[5] “Password-based Encryption Approach for Securing Sensitive Data.” By Mustacoglu, Ahmet & Fox, Geoffrey & Catak, Ferhat Ozgur. (2020). Security and Privacy. 3. 10.1002/spy2.121.

REFERENCES

[6] “Secure storage of user credentials and attributes in federation of clouds.” By Luciano Barreto, Leomar Scheunemann, Joni Fraga, and Frank Siqueira. 2017. In Proceedings of the Symposium on Applied Computing (SAC '17). Association for Computing Machinery, New York, NY, USA, 364–369.

[7] “Cryptography for tamil language.” By Prabu MV, Keerthana N, Karthika R. InAIP Conference Proceedings 2023 May 24 (Vol. 2718, No. 1). AIP Publishing.

[8] "Research on Cross-Domain Authentication Scheme for V2G Networks Based on SM9 Signature Cryptography Algorithm and Consortium Blockchain Technology." by Deng, J., Jiao, L., Zhang, L., Ren, Y. (2023). In: Barolli, L. (eds) Advances in Intelligent Networking and Collaborative Systems. INCoS 2023.

[9] “Implementation of cryptographic algorithm for secured communication in tamil language using python program.” By M. Vivek Prabu, R. Karthika; AIP Conf. Proc. 24 May 2023; 2718 (1): 050002.

[10] “Multilanguage Based SMS Encryption Techniques.” By Rajendiran, M., Syed Ibrahim, B., Pratheesh, R., Nelson Kennnedy Babu, C. (2013). In: Kumar M., A., R., S., Kumar, T. (eds) Proceedings of International Conference on Advances in Computing. Advances in Intelligent Systems and Computing, vol 174. Springer, New Delhi.


Thank
you!