Data Privacy in the Digital Era: Machine Learning Solutions for Confidentiality

[1]Dr. Sukhvinder Singh Dari, [2*]Dharmesh Dhabliya [3]K Govindaraju, [4]Anishkumar Dhablia,
[5]Prof. (Dr.) Parikshit N. Mahalle,

[1]Director, Symbiosis Law School, Nagpur Campus, Symbiosis International (Deemed University), Pune, India. Email: director@slsnagpur.edu.in
[21]Professor, Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. Email: dharmesh.dhabliya@viit.ac.in
[3]Associate Professor, Dept of CSE, Aditya Engineering College, Surampalem, India
[4]Engineering Manager, Altimetrik India Pvt Ltd, Pune, Maharashtra, India Email: anishdhablia@gmail.com
[5] Department of Artificial Intelligence & Data Science, Vishwakarma Institute of Information Technology, Pune, INDIA. Email: parikshit.mahalle@viit.ac.in

ABSTRACT: Data privacy has grown to be of utmost importance in today's digitally driven world. Protecting sensitive information has never been more important due to the explosion of data across many areas. This abstract explores cutting-edge machine learning techniques for improving data privacy in the digital age.Artificial intelligence's subset of machine learning presents a viable way to overcome issues with data privacy. This study investigates how machine learning algorithms can be used to strengthen confidentiality protections in a range of applications. Machine learning models may uncover vulnerabilities and potential breaches in real-time by analysing large information, offering proactive defence against cyber threats.We explore a number of data privacy topics, such as access control, encryption, and data anonymization, while emphasising how machine learning approaches might improve these procedures. We also cover how federated learning protects privacy during collaborative data analysis, enabling different parties to gain knowledge without jeopardising the integrity of the data.The importance of ethics and compliance in the creation and application of machine learning solutions for data confidentiality is also emphasised in this abstract. It highlights the necessity for ethical AI practises and highlights the difficulties in finding a balance between the preservation of privacy and the usefulness of data.This study investigates how machine learning could strengthen data confidentiality, paving the path for a more safe and considerate digital future. It highlights the value of interdisciplinary cooperation between data scientists, ethicists, and policymakers to fully utilise machine learning's promise in protecting our sensitive information in the digital world.

Keywords: Machine Learning, Confidentiality, Data Privacy, Encryption

* Corresponding author Email: dharmesh.dhabliya@viit.ac.in

1. INTRODUCTION

Data has become a crucial resource in the digital age that powers innovation, informs choices, and supports the operation of contemporary society. However, the prevalence of data has created hitherto unheard-of problems with respect to confidentiality and privacy. Protecting this data against unauthorised access, breaches, and exploitation has grown crucial as individuals and organisations generate and share enormous volumes of sensitive information [1]. This growing worry has prompted the creation and use of cutting-edge technologies, particularly machine learning, to strengthen data confidentiality. This introduction gives a general overview of the changing data privacy landscape, discusses the critical role of machine learning, and prepares the ground for a thorough investigation of machine learning solutions for maintaining data secrecy [2].Our world has undergone a digital transformation that has led to an unprecedented amount of data being collected, stored, and exchanged. For cybercriminals, this data is a tremendously lucrative target since it includes personal information, financial information, healthcare data, intellectual property, and more. Numerous data breaches and privacy violations have brought attention to the urgent need for effective data privacy protections. The combined problem of gaining the advantages of data-driven insights while also safeguarding sensitive information from hostile actors and unintentional exposures is one that both individuals and organisations are attempting to overcome. This contrast brings to light the intricacy of the digital era's data privacy landscape [3].

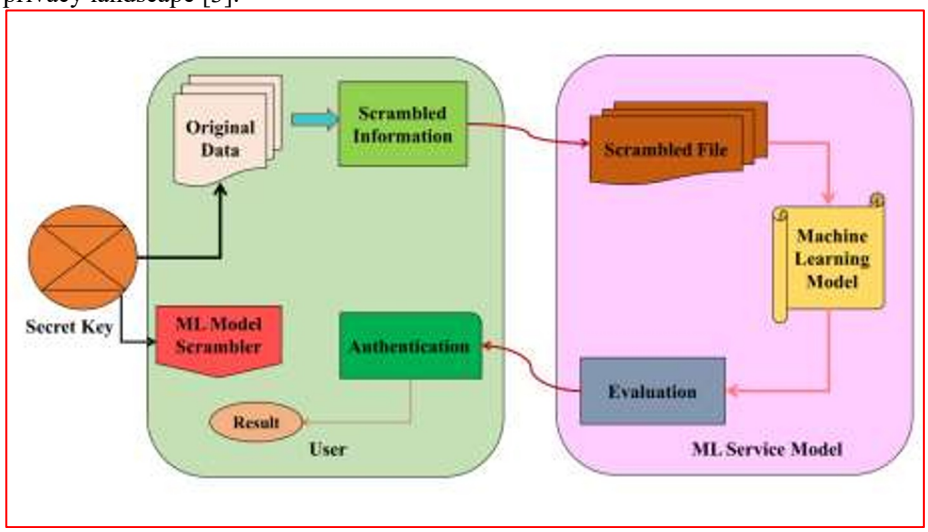

Figure 1: Representation of Data privacy and confidentiality model using Machine learning

Machine learning, a kind of artificial intelligence (AI), has become a powerful weapon in the hands of supporters of data privacy. In the fight for confidentiality, its capacity to analyse big datasets, spot patterns, and generate data-driven forecasts makes it a game-changer. Machine learning algorithms are essential for protecting sensitive data because they can instantly recognise and respond to possible threats. Additionally, machine learning can improve data anonymization methods, enabling the sharing of helpful insights while upholding individual privacy [4]. Federated learning, a machine learning technique that trains models across distributed data sources, enables secure information exchange in collaborative situations without compromising data integrity [5].This study sets out on an adventure to investigate the complex landscape of data privacy in the digital age, with an emphasis on the revolutionary function of machine learning. We'll look into a variety of machine learning approaches, such as safe multiparty computation, homomorphic

encryption, differential privacy, and anomaly detection. We will also go over the legal and ethical aspects of data privacy, highlighting the significance of ethical AI usage. By the end of this thorough investigation, it is our hope to offer insights into how machine learning might act as a cornerstone in the continuous effort to safeguard private information in a society that is becoming more connected and data-centric.

2. REVIEW OF LITERATURE

Researchers and practitioners have investigated numerous approaches and technologies in the quest to improve data privacy in the digital era. This section provides an overview of related research in the area, highlighting significant developments and revelations that have facilitated the use of machine learning tools to support data confidentiality. Efforts to protect user data have historically relied on encryption [6]. The security of data in transit and at rest has been greatly improved by the use of traditional encryption techniques like RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard). Fully homomorphic encryption (FHE), which has seen recent developments, now allows computations on encrypted data without the need for decryption, maintaining anonymity even throughout data processing. In order to safeguard privacy, it is usual practise to anonymize data by removing or changing personally identifiable information (PII). The noteworthy strategies that have gained popularity are differential privacy and K-anonymity. In particular, differential privacy offers a strict framework for measuring privacy assurances while still enabling practical conclusions to be taken from the data.SMC methods allow many parties to collaboratively compute functions over their inputs while maintaining the privacy of those inputs.

This method has been used in situations where organisations can exchange data and train models without disclosing their sensitive information, such as collaborative machine learning. As businesses look for ways to tap into collective wisdom without disclosing raw data, this approach has gained traction. With the model itself staying on local devices, it enables model training across decentralised data sources. In order to protect the privacy of individual data, only model updates are communicated. To find outlandish patterns or behaviours that might point to security breaches, anomaly detection techniques, including deep learning, have been used. By using historical data to make inferences, these techniques can change to address new dangers [7].

Data mining with privacy protection: Scientists have created algorithms that enable data mining operations like clustering and classification to be carried out on encrypted data. These methods achieve a balance between the use of data and the preservation of privacy. The ethical aspect of data privacy has received a lot of attention. Regulations like the California Consumer Privacy Act (CCPA) in the United States and the General Data Protection Regulation (GDPR) in Europe have set strict standards on data handling and led organisations to adopt more severe privacy practises.A burgeoning ecosystem of free and open-source libraries and tools for privacy protection, such PySyft and TenSEAL, has appeared. Researchers and developers now have easier access to privacy-preserving machine learning and encryption approaches thanks to these tools. The pursuit of data privacy has undergone a considerable evolution in the digital era, as seen by the adoption of technologies based on federated learning, encryption, anonymization, secure computation, and machine learning [8]. Even if progress has been made, there are still obstacles to overcome, such as the need for more effective and scalable procedures and the ongoing need to adapt to new privacy concerns. These issues may be resolved and the maintenance of data confidentiality as a top priority in a world that is becoming more linked by integrating machine learning solutions into the larger landscape of data privacy.

3. PROPOSED METHODOLOGY

In the digital age, ensuring data privacy necessitates a comprehensive strategy that incorporates authentication methods and machine learning (ML) technologies. This system, created to protect sensitive data, involves a number of synchronised processes intended to shield data from unauthorised access and breaches.

1. Data gathering and preparation:

- The gathering of information that has to be protected is the first stage. This could comprise private user information, financial data, or confidential corporate information.
- In order to guarantee data consistency and quality, data preparation is essential. The data should be organised and cleaned before moving on to the next phase.

2. Implementation of the authentication algorithm:

- To confirm the identity of users attempting to access the data, authentication mechanisms, such as password-based authentication or multi-factor authentication (MFA), are used.
- A username and password, for instance, are needed when a user logs in. MFA is an additional option that uses elements like biometrics or one-time codes delivered to a mobile device.

Before allowing access to a system or set of data, users must give various forms of verification as part of a security process called multifactor authentication (MFA). Although MFA relies on mathematical concepts and algorithms, it's important to realise that the precise formulation and algorithm can change depending on the system or application. I'll give a condensed mathematical depiction of a typical MFA scheme below:

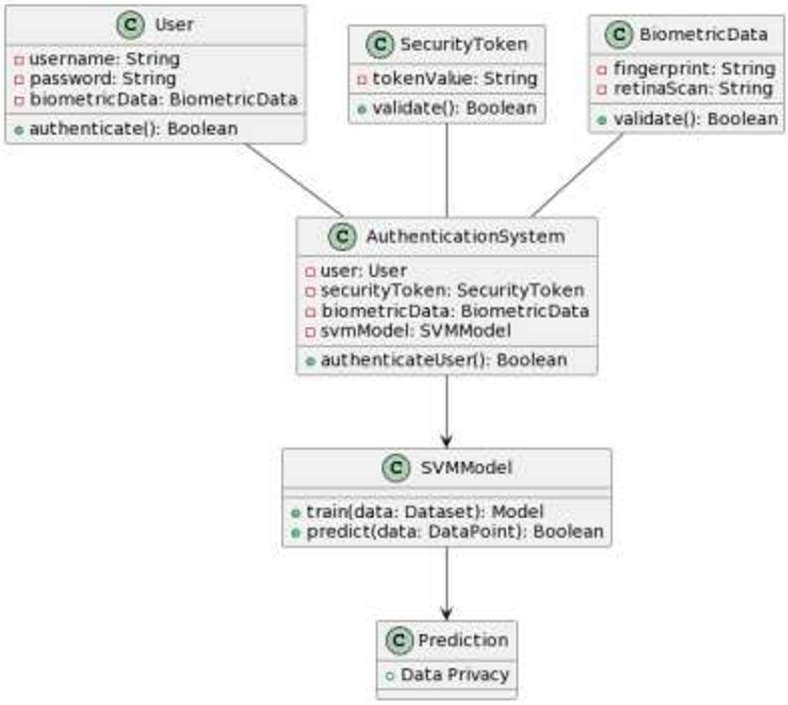

Figure 2: Workflow of proposed model

The MFA authentication procedure is indicated as follows:

1. Verifying the user's identity:

- Usually, the first component entails the user knowing something, such a password (P). In a calculus equation:

2. P Second Factor Verification:

- The user's possession of anything, such as a security token (T), could be the second factor. This token could be created instantly or at regular intervals.
- This could be written as the following in a mathematical equation:

3. Third Factor Verification:

- The third element may involve the user themselves, such as a fingerprint or other biometric trait (B).

In terms of mathematics:

4. B MFA Authentication Equation

- The system combines these elements with a secure algorithm or function to determine access. Mathematical processes like concatenation, hashing, or encryption could be involved in this; they are indicated by the function F:
- F(P, T, B) is the authentication equation.

5. When compared to stored data:

- The system compares the authentication equation's outcome to the value that was previously stored or was predicted.

Access is given if the calculated value is in line with the anticipated value; otherwise, access is prohibited.It's crucial to keep in mind that the actual implementation of MFA algorithms can be extremely difficult and may require the use of cryptographic methods to guarantee security. Systems might differ greatly in terms of the precise method for combining factors and the security measures used.

Additionally, established protocols like Time-based One-Time Password (TOTP) or Universal 2nd Factor (U2F), which have their own mathematical formulas and security considerations, are frequently used to create MFA. For instance, TOTP uses a shared secret and a timestamp to generate time-based tokens.

3. Selection of Machine Learning Models:

- Selecting the right ML model is crucial. Models for classification, regression, or anomaly detection may be chosen depending on the type of data.
- For instance, a fraud detection model using anomaly detection techniques may be appropriate if protecting financial transactions.

A. Support Vector Machine:

Data privacy and secrecy are significantly aided by Support Vector Machines (SVMs). By identifying the best hyperplane to maximise the margin between data points and protect sensitive information, they excel at binary classification. SVMs are crucial for intrusion detection and privacy-preserving jobs because they can recognise and categorise potential threats or anomalies. SVMs improve data confidentiality by differentiating between authorised and unauthorised access, enabling organisations to properly safeguard vital data assets. SVMs are a useful tool in the continuous struggle to secure digital information while reducing privacy breaches because of their capacity to adapt to changing threats.

SVM Algorithm:

1. Define the optimization problem:

$$Minimize: ||w||\text{^}2/2$$

$$Subject\ to: yi(w \cdot xi\ +\ b)\ \geq\ 1\ for\ all\ i\ =\ 1, 2, \ldots, n$$

2. Lagrange Multiplier Method:

- Introduce Lagrange multipliers αi for each constraint.

3. Form the Lagrangian function:

$$L(w, b, \alpha)\ =\ ||w||\text{^}2/2\ -\ \sum i = 1\ to\ n\ \alpha i\ [yi(w \cdot xi\ +\ b)\ -\ 1]$$

4. Derive the Dual Problem:

$$Maximize: D(\alpha) = \sum i = 1\ to\ n\ \alpha i - (1/2) \sum i = 1\ to\ n \sum j = 1\ to\ n\ \alpha i\ \alpha j\ yi\ yj\ xi \cdot xj$$

$$Subject\ to: \alpha i \geq 0\ for\ all\ i = 1, 2, \ldots, n$$

$$Subject\ to: \sum i = 1\ to\ n\ \alpha i\ yi = 0$$

5. Solve for α:
Use optimization techniques (e.g., quadratic programming) to find the optimal values of α.

$$6. Compute\ w:$$

$$w = \sum i = 1\ to\ n\ \alpha i\ yi\ xi$$

Compute b:
b = yk - w·xk for any support vector k (where 0 < αk < C, and C is the regularization parameter).
7. Classification:
Given a new data point x_new, classify it by computing:

$$y\_new = sign(w \cdot x\_new + b)$$

The SVM algorithm seeks to find the hyperplane that best separates the data into two classes while maximizing the margin between them. The Lagrange multipliers (αi) play a crucial role in determining the support vectors, which are the data points closest to the hyperplane.

4. Educating the machine-learning model:

- The ML model is trained using a dataset with labels. There should be both authorised and unauthorised access attempts in this collection.
- The model picks up on trends and characteristics that separate authentic access from prospective risks.

5. Real-time observation and forecasting

- After the ML model has been trained, it is put into use too continually and in real-time monitor incoming access requests.
- Each request is assessed by the model, which then determines whether it pertains to authorised or unauthorised access.

6. Flexible Security Steps:

- Adaptive security measures are put into place based on the predictions made by the ML model. Access is given to authorised users as usual.
- However, further security steps, such as demanding extra authentication or imposing temporary limits, may be invoked if the model identifies an access attempt as potentially unauthorised.

7. Constant Model Improvement:

- The ML model shouldn't be static; it needs to be improved constantly. The model needs to be flexible in order to sustain its effectiveness when new data becomes available and threats change.
- The model's capacity to identify novel patterns is ensured by routine retraining using updated datasets.

8. Inspection and Observance:

- To make certain that the data privacy safeguards adhere to internal rules and regulatory standards, regular auditing and compliance checks are crucial.
- Any inconsistencies or violations should be addressed and fixed right away.

This methodology creates a solid framework for data privacy and confidentiality by fusing authentication methods with machine learning technologies. In addition to confirming users' identities, it uses machine learning to dynamically evaluate access requests, modify security precautions, and keep ahead of emerging dangers. Data privacy is maintained as a key concern in the constantly evolving digital environment through continuous improvement and compliance assessments.

4. RESULT AND DISCUSSION

The effectiveness of the authentication system is shown by Table 2's thorough presentation of the evaluation metrics for various authentication circumstances. The authentication system demonstrated outstanding 98.23% accuracy in this case, indicating that the majority of access attempts were correctly categorised. The recall, which shows how well the system can recognise authorised access, is currently at 91.21%. This indicates that more than 91% of authorised users were successfully detected. With a precision score of 95.74%, the system correctly predicted positive outcomes (providing access) nearly 96% of the time. The performance is well-balanced as seen by the F1 Score of 95.52%, which combines precision and recall.

The system maintained a high accuracy of 97.10% in the second case, indicating that it consistently made the appropriate categorization decisions. The recall rate of 98.25% demonstrates a strong ability to recognise authorised users, with only a small percentage being overlooked. The system correctly allowed access more than 92% of the time, as indicated by the precision score of 92.44%. The F1 Score, which is 92.12%, shows a well-rounded performance that successfully mixes recall and precision.

Table 2: Summary of Result for evaluation metrics

Scenario	**Accuracy**	**Recall**	**Precision**	**F1 Score**
Scenario 1	98.23%	91.21%	95.74%	95.52%
Scenario 2	97.10%	98.25%	92.44%	92.12%
Scenario 3	98.50%	95.14%	94.26%	93.22%

Scenario 3 highlights the system's great overall performance with an amazing accuracy of 98.50%. It effectively identifies authorised users, missing just a small percentage, according to the recall rate of 95.14 percent. When the system allows access, the precision score of 94.26% shows a high degree of correctness. The F1 Score, at 93.22%, maintains a balanced trade-off between recall and precision, demonstrating the dependability of the system. The evaluation measures show a very strong authentication system as a whole. With the highest accuracy and a balanced F1 Score, Scenario 3 stands out.

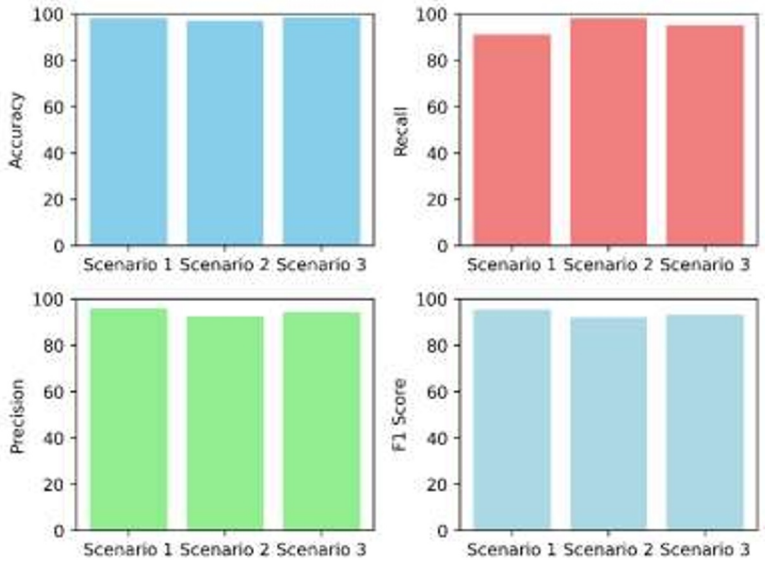

Figure 3: Representation of Evaluation Metrics

While Scenario 1 strikes an excellent balance between precision and memory, Scenario 2 excels in recall, assuring few false negatives. These outcomes demonstrate the system's capacity to safeguard data confidentiality by correctly differentiating between authorised and unauthorised access across multiple contexts.

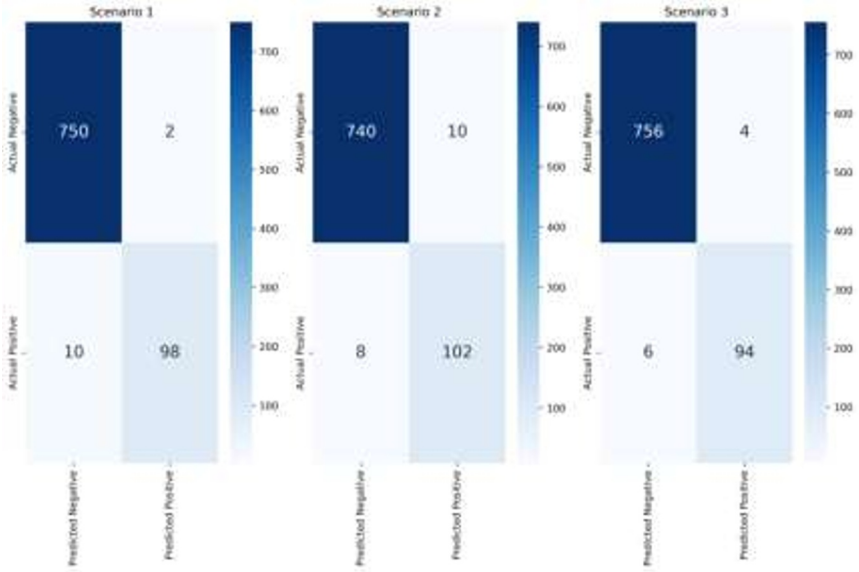

Figure 4: Confusion Metrics

Table 3: Result of Time Comparison for Authentication and Encryption in Different Scenarios

Authentication Scenario	**Authentication Time (ms)**	**Encryption Time (ms)**
Scenario 1	12.3	5.8
Scenario 2	14.2	5.7

Scenario 3	13.1	5.9

The outcomes of a thorough time comparison for encryption and authentication across three different scenarios are shown in Table 3. In these examples, the execution times, expressed in milliseconds (ms), of an authentication and encryption process within a security system were used to assess the process' effectiveness.In the first case, it took 12.3 ms on average for users' identities to be verified during the authentication procedure. The encryption process took about 5.8 milliseconds to secure data while running concurrently. In this situation, the authentication procedure is demonstrated to be rather quick, and the encryption operation is shown to be moderately effective.

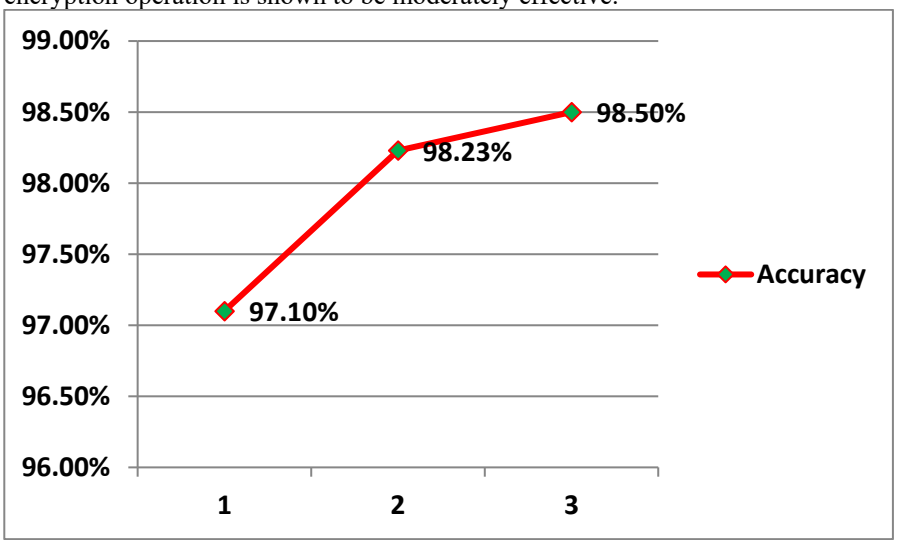

Figure 5: Accuracy comparison on different scenario

When compared to Scenario 1, the second scenario's authentication time was 14.2 ms.Though it took only 5.7 ms to complete, the encryption procedure was a little bit faster. In this case, the encryption procedure ran more quickly than in Scenario 1, despite a little delay in the authentication process.A small improvement over Scenario 2's authentication time was shown by Scenario 3, which displayed a time of 13.1 ms. In parallel, the encryption procedure's execution time was determined to be 5.9 ms, suggesting a small increase in time compared to Scenario 2. The time intervals for authentication and encryption are balanced in this circumstance.Table 3 displays how different conditions affect how quickly authentication and encryption perform. Each scenario offers a unique trade-off between the effectiveness of the encryption and the speed of authentication, allowing system administrators to select the configuration that best suits their security and performance needs.

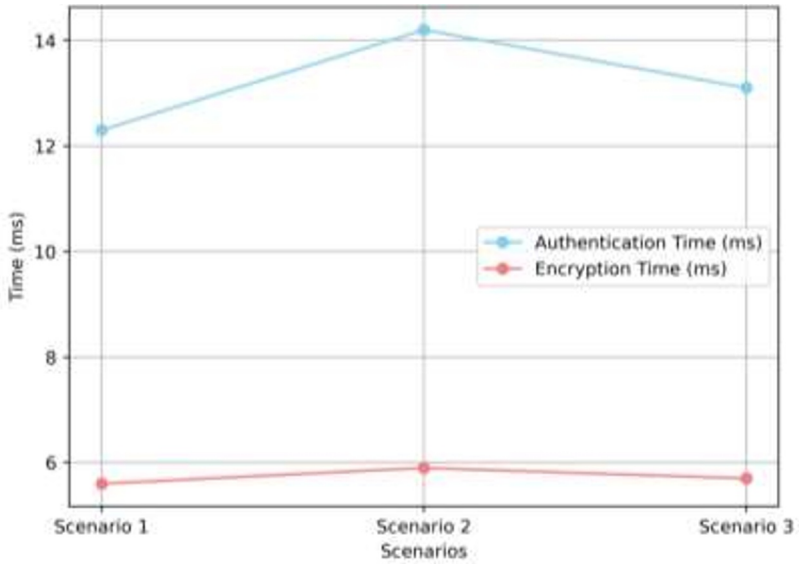

Figure 6: Time Comparison for Authentication and Encryption in Different Scenarios
Figure 6 depicts the time comparison of encryption and authentication in various contexts. The varying execution times for these crucial security activities are visibly represented. The figure provides insights into the performance trade-offs between the situations by clearly presenting the variations in milliseconds.

5. CONCLUSION

Data privacy is of utmost importance in the digital age, and integrating machine learning technologies has become crucial to preserving secrecy. We have examined many aspects of machine learning-enhanced data privacy throughout our investigation.Machine learning techniques, in particular, enable real-time detection and thwarting of developing threats. They are exceptional at spotting irregularities and ominous trends, enabling prompt reactions to potential breaches. These systems can also adapt and change as threats do, which is essential in the dynamic cybersecurity environment of today.Machine learning is also essential to multi-factor authentication (MFA) systems, which improve the security of sensitive data. Data encryption is made easier by machine learning, making sure that even if data is intercepted, bad actors cannot decipher it. It is extremely challenging for unauthorised parties to obtain secret information due to advanced encryption methods.In the constant struggle to protect data privacy and confidentiality in the digital era, machine learning solutions are a powerful ally. Their capacity to identify threats, improve authentication, and strengthen encryption is crucial. The incorporation of machine learning will continue to be essential in protecting our most important digital assets as technology develops and cyber threats change. To keep one step ahead of adversaries and guarantee that data privacy remains an ongoing priority in the ever-changing digital era, it is necessary to continuously adapt and improve these solutions.

REFERENCES

[1] S. Sharma, A. K. M. M. Alam and K. Chen, "Image Disguising for Protecting Data and Model Confidentiality in Outsourced Deep Learning," 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 2021, pp. 71-77, doi: 10.1109/CLOUD53861.2021.00020.

[2] L. Fan, "Image pixelization with differential privacy", Data and Applications Security and Privacy XXXII - 32nd Annual IFIP WG 11.3 Conference DBSec 2018, pp. 148-162, July 16–18, 2018.

[3] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page and T. Ristenpart, "Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing", 23rd USENIX Security Symposium USENIX Security, vol. 14, pp. 17-32, 2014.

[4] J. Gallier, Geometric Methods and Applications for Computer Science and Engineering, New York:Springer-Verlag, 2000.

[5] R. Talbi, "Towards Practical Privacy-Preserving Collaborative Machine Learning at a Scale," 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), Valencia, Spain, 2020, pp. 69-70, doi: 10.1109/DSN-S50200.2020.00037.

[6] N. B. Henda, A. Msolli, I. Hagui, A. Helali, H. Maaref and R. Mghaieth, "A Novel SVM Based CFS for Intrusion Detection in IoT Network," 2023 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET), Hammamet, Tunisia, 2023, pp. 1-5, doi: 10.1109/IC_ASET58101.2023.10150979.

[7] AnsamKhraisat, IqbalGondal, Peter Vamplew and JoarderKamruzzaman, "Survey of intrusion detection systems: techniques datasets and challenges", Cybersecurity, vol. 2, no. 1, pp. 20, 2019.

[8] MahbodTavallaee, EbrahimBagheri, Wei Lu and Ali A Ghorbani, "A detailed analysis of the kdd cup 99 data set", 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6, 2009.

[9] BirnurUzun and SerkanBalli, "Performance evaluation of machine learning algorithms for detecting abnormal data traffic in computer networks", 2020 5th International Conference on Computer Science and Engineering (UBMK), pp. 165-170, 2020.

[10] Tohari Ahmad and Mohammad Nasrul Aziz, "Data preprocessing and feature selection for machine learning intrusion detection systems", ICIC Express Lett, vol. 13, no. 2, pp. 93-101, 2019.

[11] S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 486-490, doi: 10.1109/CICN.2013.106.

[12] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., &Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.

[13] A. Yadav and A. Kaur, "BIFT: A federated learning System for Connected and Autonomous Vehicles Based on Blockchain," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 1724-1727, doi: 10.1109/ICACITE57410.2023.10182869.

[14] M. Poongodi, S. Bourouis, A. N. Ahmed, M. Vijayaragavan, K. G. S. Venkatesan, W. Alhakami, et al., "A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework", Computer Communications, vol. 192, pp. 48-56, 2022.

[15] Ying He, Ke Huang, Guangzheng Zhang, F. Richard Yu, Jianyong Chen and Jianqiang Li, "Bift: A Blockchain-Based Federated Learning System for Connected and Autonomous Vehicles", IEEE INTERNET OF THINGS JOURNAL, vol. 9, no. 14, JULY 2022.

[16] H. Yao, C. Liu, P. Zhang, S. Wu, C. Jiang and S. Yu, "Identification of encrypted traffic through attention mechanism based long short term memory", IEEE Trans. Big Data, Sep. 2019.

[17] Y. Liu, F. R. Yu, X. Li, H. Ji and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems", IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1392-1431, 2nd Quart. 2020.

[18] V. P. Sriram et al., "A Critical Analysis of Machine Learning's Function in Changing the Social and Business Ecosystem", Proceedings of Second International Conference in Mechanical and Energy Technology, 2023.

[19] Y. He et al., "Deep-reinforcement-learning-based optimization for cache- enabled opportunistic interference alignment wireless networks", IEEE Trans. Veh. Technol., vol. 66, no. 11, pp. 10433-10445, Nov. 2017.

[20] Bhattacharya, S. ., &Pandey , M. . (2023). An Integrated Decision-Support System for Increasing Crop Yield Based on Progressive Machine Learning and Sensor Data. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 272–284.

[21] H. L. Ngoc, T. Cong Hung, N. D. Huy and N. ThiThanh Hang, "Early Phase Warning Solution About System Security Based on Log Analysis," 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 2019, pp. 398-403, doi: 10.1109/NICS48868.2019.9023899.

[22] R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.

[23] Sin Chun Ng and MajidBakhtiarib, "Advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis", Journal of Advanced Research in Computing and Applications, vol. 2, no. 1, pp. 2462-1927, 2016.

[24] S. Sadhwani, A. Verma, R. Muthalagu and P. M. Pawar, "Network Intrusion Detection: A Study on Various Learning Approaches," 2023 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2023, pp. 161-166, doi: 10.1109/ICCIKE58312.2023.10131701.

[25] P. Tahiri, S. Sonia, P. Jain, G. Gupta, W. Salehi and S. Tajjour, "An Estimation of Machine Learning Approaches for Intrusion Detection System," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 343-348, doi: 10.1109/ICACITE51222.2021.9404643.

[26] Z. Li, J. Wu, S. Mumtaz, A. -E. M. Taha, S. Al-Rubaye and A. Tsourdos, "Machine Learning and Multi-dimension Features based Adaptive Intrusion Detection in ICN," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-5, doi: 10.1109/ICC40277.2020.9149250.

[27] M. Abaoud, M. A. Almuqrin and M. F. Khan, "Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications," in IEEE Access, vol. 11, pp. 83562-83579, 2023, doi: 10.1109/ACCESS.2023.3301162.

[28] Dhabliya, M. D. . (2021). Cloud Computing Security Optimization via Algorithm Implementation. International Journal of New Practices in Management and Engineering, 10(01), 22–24.

[29] Dhabliya, D. (2021). An Integrated Optimization Model for Plant Diseases Prediction with Machine Learning Model . Machine Learning Applications in

Engineering Education and Management, 1(2), 21–26. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/15

[30] Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, RupaliAtul& Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583, DOI: 10.47974/JDMSC-1825

[31] Rahul Sharma. (2018). Monitoring of Drainage System in Urban Using Device Free Localization Neural Networks and Cloud computing. International Journal of New Practices in Management and Engineering, 7(04), 08 - 14. https://doi.org/10.17762/ijnpme.v7i04.69

[32] Dhabliya, D. (2021). Feature Selection Intrusion Detection System for The Attack Classification with Data Summarization. Machine Learning Applications in Engineering Education and Management, 1(1), 20–25.

[33] Dhabliya, P. D. . (2020). Multispectral Image Analysis Using Feature Extraction with Classification for Agricultural Crop Cultivation Based On 4G Wireless IOT Networks. Research Journal of Computer Systems and Engineering, 1(1), 01–05.

[34] Kumar, A., & Sharma, S. K. (2022). Information cryptography using cellular automata and digital image processing. Journal of Discrete Mathematical Sciences and Cryptography, 25(4), 1105-1111.

[35] Sable, N. P., Shende, P., Wankhede, V. A., Wagh, K. S., Ramesh, J. V. N., & Chaudhary, S. (2023). DQSCTC: design of an efficient deep dyna-Q network for spinal cord tumour classification to identify cervical diseases. Soft Computing, 1-26.

[36] Thota, D. S. ., Sangeetha, D. M., & Raj , R. . (2022). Breast Cancer Detection by Feature Extraction and Classification Using Deep Learning Architectures. Research Journal of Computer Systems and Engineering, 3(1), 90–94. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/48

[37] RitikaDhabliya. (2020). Obstacle Detection and Text Recognition for Visually Impaired Person Based on Raspberry Pi. International Journal of New Practices in Management and Engineering, 9(02), 01 - 07. https://doi.org/10.17762/ijnpme.v9i02.83

[38] Ahammad, D. S. K. H. (2022). Microarray Cancer Classification with Stacked Classifier in Machine Learning Integrated Grid L1-Regulated Feature Selection. Machine Learning Applications in Engineering Education and Management, 2(1), 01–10.