Power System Technology
ISSN:1000-3673

Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

Predicting the Fastest, Safest Restoration Path Post-Breach Using ML

Gaurang Deshpande

Software Developer, IBM, USA

Email: gaurangdeshpande89@gmail.com

Abstract: The study is analysing the role of Machine Learning in predicting the fastest and safest path in the context of post-breaches. The study is applying explanatory design and using qualitative and quantitative data to derive the results. The results reveal how ML is effective in identifying the patterns within the system and user behaviours. The ML is ensuring the quick discerning of the vulnerable areas of the network requiring isolation. The prediction of the fastest and most secure path is possible on account of ML. The companies have been recommended to use ML with a Decision-Tree algorithm and multi-training method for gaining accurate outcomes.

Keywords: Machine Learning in recovery, post-breach, restoration path post-breach, ML in restoration, ML in recovery strategy.

I. INTRODUCTION

A. Background of the study

The breaches within a network are a stark reality necessitating effective restoration paths. The post-breach recovery is required when a specific breach or leak is identified. The fastest and safest path can ensure that the model continues to function handling the regular queries posed by the system [1]. The impacts of the leaked model are being significantly reduced using the safe, restoration path. Machine Learning is able to identify the fastest and safest pathways to restoration. The ML is enhancing the process by automating vital actions such as isolating the compromised system. The study is examining how the ML models can enable the fastest and safest restoration path in the context of an incidence occurring. The possible restoration paths post-breach will ensure that the system continues to process queries without any fear.

B. Overview

The number of data breaches has exploded in the current times with companies gathering more data [3]. The recovery strategies are vital in enhancing customer satisfaction in the context of a data breach taking place. The safest and fastest restoration path can induce the necessary compensation and remorse that can ascertain consumer satisfaction [3]. The organisation response strategy to post-breach incidents is crucial for attaining customer satisfaction [4]. Machine Learning has a crucial role to play in such instances disabling any kind of malicious IPs or identifying any type of patching vulnerabilities. The tracking of patches that are more vulnerable leads to effective decisions [5]. The post-breach situation can deeply benefit from the integration of ML models that are able to categorise vulnerabilities and isolate the areas affected.

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

C. Aims and Objectives

The study is attempting to accomplish the following objectives in its execution: 1) To identify the complexities encountered by the organisation in a post-breach situation 2) To critically analyse the role of ML in empowering the safest and fastest restoration path in the post-breach situation 3) To discern the vital enhancements required in ML applications for improving the recovery path in a post-breach situation.

D. Problem Statement

The restoration path is instrumental in enhancing the recovery within a post-breach situation [6]. There is immediate recovery needed in a post-breach situation such that the reputation of an organisation remains intact. There are multiple forms of recovery needed in a system including process recovery, regulatory recovery, employee recovery and customer recovery [6]. The restoration path can ascertain the speedy recovery ensuring the systems continue to operate smoothly. There is reduced investigation regarding the use of ML in post-breach situations identifying faster and safer paths of restoration. The use of ML in recovery through the identification of the safest and fastest restoration path can benefit organisations suffering from post-breach incidents.

E. Scope and Significance

The scope of the study is to identify the post-breach complexities and difficulties that organisations struggle to manage. The study endeavouring to analyse and establish the role of Machine Learning in identifying the fastest and safest restoration path expediting the recovery in post-breach situation. The study is identifying the additions or improvements in ML that can empower its recovery process defining the safest route. The recovery-based design strategy is relying on the rapid estimation of the situation [7]. The study is significant since it will improve the recovery-based process in post-breach defining the role of ML. Organisations can ensure speedy recovery applying the ML functionalities applying the knowledge gained.

II. LITERATURE REVIEW

A. Complexities and challenges of post-breach recovery

There are immense complexities associated with post-breach recovery within a system. The technical challenges are faced in ensuring that all the systems have been restored to their previous states. The identification and removal of any remaining threat in a system is one of the critical complexities. The recovering of lost data and simultaneously verifying its integrity is one of the challenges in the post-breach context. There are 5% reductions in stock prices in response to a potent data breach encountered by a system [8]. The data breaches have resulted in 4.35 $ billion in losses in 2022 [8].

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

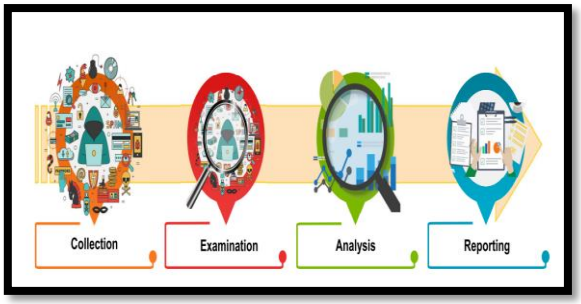

Figure 1: Steps after data breaches(Source: [8])

The data breach incidents are investigated by collecting, examining, analysing and reporting data [8] [***Refer to Figure 1***]. The data breach losses are immense requiring quick data recovery after the incident. There are systematic steps needed post-breach to ensure fast recovery. Detailed data scanning is essential for uncovering the data that has been compromised. The containing of the data breach can prevent the data losses facilitated by blocking malicious traffic and disabling the affected accounts. The data breaches require a rigorous examination of the other categories of data involved in the records leaked and the potent threats they are posing to the current system [9]. The post-breach situation is filled with difficulties and complexities that require an in-time and yet safe recovery path.

B. The role of ML in discerning the safest and fastest restoration path

Machine Learning is crucial in identifying the paths that can benefit the recovery process. Business continuity is possible when integrating ML models in the breach recovery procedure. The ML is impactful in analysing huge volumes of data and interpreting the vulnerability patterns present within them. The areas affected and their isolation can be identified by ML leading to a more robust system. The ML is effective in identifying vulnerable code fragments [10]. The application of ML in post-breach incidents can ensure quick recovery discerning the vulnerabilities within the system. Further, the ML has capacities to classify a specific domain name as malicious or benign [11]. Hence, the blocking of malicious IP addresses can be attained with ML being integrated across the various post-breach incidents encountered. The ML is also able to analyse user behaviours and detect the underlying anomalies within the system. The ML can detect anomalies with 80% accuracy and the post breach situation can ensure quick recovery [12]. The careless or malicious behaviour with the potential for spreading of the breach can be discerned with the application of ML models.

C. Integration in ML applications to enhance recovery

The ML while enhancing root cause analysis, isolation and blocking of malicious IP addresses are prone to critical errors. There are possibilities of generalisation errors with ML models failing to accurately identify the vital patterns [13]. The ML with generalisation errors in post-breach context can fail to identify the causes, areas of attacks and containments needed for restoring the system to their previous state. The multi-level training of the ML algorithms making use of deep learning can refine the model and reduce the possibilities of generalisation errors [13]. The ML models can often fail to interpret human behaviour successfully [14]. The interpretation of human behaviours in post-breach context is vital for identifying any malicious

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

or careless tendencies. The choice of interpretable models and algorithms that help in identifying the key features can lead to more accurate ML outcomes. The decision trees can empower ML models to interpret stronger and more effective results [15]. Companies facing data breaches can benefit through the decision tree used in ML to learn patterns from datasets.

III. METHODOLOGY

A. Research Design

The research is using explanatory research design to comprehend the role of ML in defining the secure and fastest route for post-breach recovery. The explanatory design is taking into account the phenomenon and the relation of the determinants to it [16]. The research striving to understand the ML model functionalities and features leading to improved recovery is strengthened by applying the explanatory design. The explanatory design is elaborating how the features of ML are being impactful in identifying the patterns in post-breach situation. The restoration path being benefitted by the aspects of ML discerning the anomalies and blocking affected areas. The effectiveness of ML is being derived through the explanatory design applying its outcomes within the post-breach context.

B. Data Collection

The data collection in the study is making use of both qualitative and quantitative categories. The chart, graphs and statistical inferences within the secondary data are being collected for the quantitative data. The quantitative data is facilitating learning of the exact attributes of ML that are effective in defining restoration paths. The qualitative data for the research is being assimilated from existing journal articles, industry reports and books. The qualitative data is lending knowledge on the post-breach complexities and how they need to be addressed to ensure business continuity. The collection of both types of data is aiding in accomplishing a comprehensive understanding of the phenomenon.

C. Case Studies Examples

Case Study I: HSBC

HSBC has faced numerous breaches indicating the need for resilient post-breach recovery. Thus, it can be noted how HSBC continued to function in a disrupted manner with the breaches affecting SME lending and inaccurate information regarding the fees. The impacts of the breach lasted for almost 5 years indicating the need for a resilient recovery of the system [18]. The breaches have disrupted regular operations, compromising the confidentiality of customers' data.

Case Study II: Facebook

Facebook has encountered multiple data breaches exposing the critical vulnerabilities within the system. The company had faced extreme data breaching incidents with 530 million users' data being publicly released [19]. The lack of proper security measures resulted in the data being leaked and shared over the system. There had been no immediate steps for identifying the areas of attacks and separating them. The integration of effective ML models could have ensured positive results for the company.

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

D. Evaluation Metrics

The evaluation metrics compare values leading to accurate results for the data collected [17]. Accuracy and precision are the key evaluation metrics that are being used for the current study. The correctness of ML in identifying areas of attacks and the vulnerability patches is being examined to understand its relevance. The accuracy measuring the acuteness of ML identification is establishing its impacts in post-breach incidents. The precision is another crucial metric checking the degree to which the ML is being effective in post-breach control. The safest and fastest path ensured through the automation and isolation possible through ML is being derived. The metrics are being used for assessing the applications of ML in examining data patterns and extracting key insights.

IV. RESULTS

A. Data Presentation

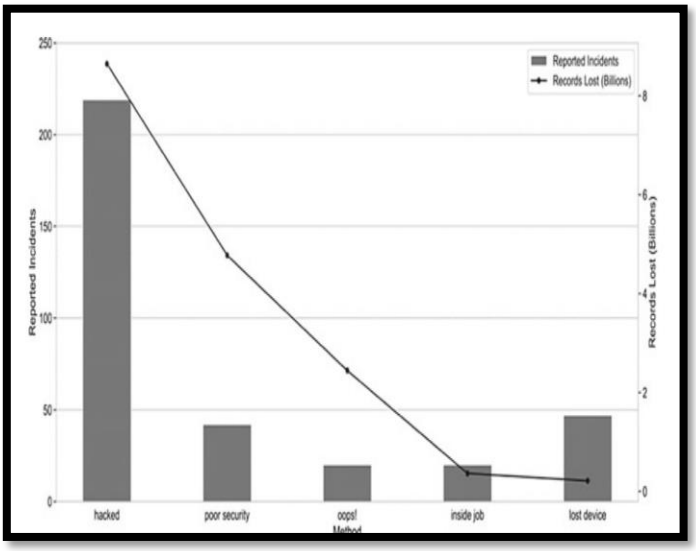

Figure 2: The reasons identified for data breach in the system

(Source: [12])

There are various reasons for the data breach incident within a system. The hacked incident represents 53% of the data breaches taking place and 29% represents the issues of poor security [12]. There are human factors involved in the breaches taking place. The ML model identifying the reasons and the core areas affected can suggest the immediate actions needed. The categorisation of the root causes through ML can empower any organisation to identify the critical areas of vulnerability. The recovery process is easier with the integration of ML.

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

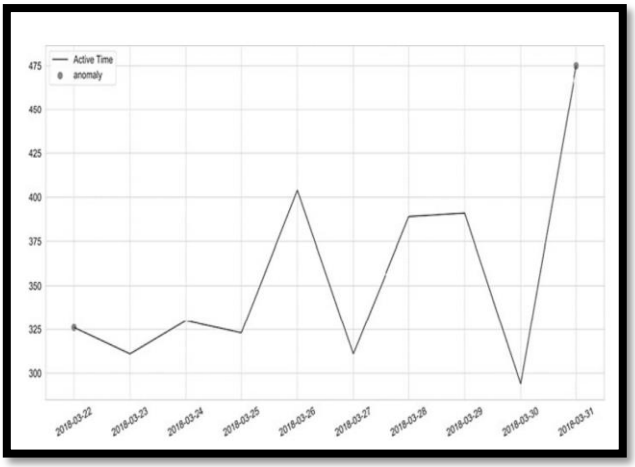

Figure 3: The identification of anomalies

(Source: [12])

The ML model is impactful in identifying the anomalies within the system. The user behaviour characterisation is being achieved with the ML model showing an accuracy of 0.8169 [12]. The ML model can identify the anomalies in user behaviour that can be responsible for the breaches taking place. The model aids in identifying root causes that are vital for ensuring a safe and fast restoration path for the business. The user behaviours can be rectified preventing the spread of the breaches over the network.

B. Findings

The ML model's validity in being able to derive root causes and identifying anomalies is being inferred [12]. The analysis pinpoints the capacities of ML in defining safe and fastest restoration in the post-breach situation. The categorisation of the reasons behind the attack can determine the areas affected. The isolation of such areas can be easier through the insights received. The safest route to restoration is possible with the verification of the factors responsible for the breach. Further, it can be noted how ML models are effective in discerning the anomalies in human behaviour. The recovery to the former state is possible through the rectification of such behaviours that can trigger massive breaches within the system. The ML has a critical role to play in terms of the discrepancies and classification attained by applying its features. The safest and fastest path to recovery is possible through the vital know-how derived through ML model.

C. Case Study Results

Case Study	***Strategy***	***Impact***	***Outcome***
HSBC	Data breaches on customer data base [18]	Data breaches affecting SME lending products and inaccurate	HSBC facing disrupted operations with the data breaches

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

		information regarding fees [18]	
Facebook	Data breaches exposing confidential user data [19]	Loss of reputation impacts customers' privacy [19]	Facebook continuing to struggle with safe and fast paths

Table 1: Case Study Outcomes

(Source: self-created)

The above analysis of case studies reveals how both Facebook and HSBC have faced data breaching incidents. The lack of ML for identifying potent reasons behind the breach continues to affect the systems' outcomes.

D. Comparative Analysis

Source	***Aim***	***Findings***	***Gaps***
[1]	The post-breach recovery methods capable of robust defences [1]	The examination of previous leaked models able to perform well against adaptive attacks [1]	The lack of analysis of the features of models that can identify fresh modes of attacks in the system
[4]	Identification of response strategies to the breaches in the system [4]	The risks to reputation faced on account of the attacks in the system [4]	Reduced examination of the response strategies needed by organisations in the technical domain
[5]	The identification of factors triggering vulnerability within the system [5]	The vulnerable version and patch information aiding the recovery models [5]	The lack of case studies on how the ML models can benefit vulnerability identification
[6]	The data breach recovery areas that need immediate focus [6]	The four areas of recovery including process and regulatory recovery needed after the data breach [6]	The lack of focus on how the recovery strategies should be shaped

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

[7]	The use of ML for optimisation framework empowering the recovery-based design [7]	The efficacy of a recovery-based design strongly benefitted from the ML models [7]	Limited discussion of diverse cases making use of ML
[11]	The use of ML for accurate discerning of malicious factors [11]	The malicious domain detection attained within the network applying Machine Learning [11]	The reduced exploring of the features of ML is vital for recovering

Table 2: Comparative Analysis

(Source: self-created)

The comparative analysis of the various findings gathered from the study has been done in the table. The findings reveal how ML is playing an instrumental role in improving the organisation's response strategies to data breaches taking place. The ML can identify vulnerabilities and malicious factors within the system facilitating faster recovery from attacks.

V. DISCUSSION

A. Interpretation of Results

The results reveal how there are critical complexities in the post-breach context. There are technical issues faced regarding the removing of remaining threats and maintaining the integrity of the remaining data [8]. There is an immediate need for identifying the data and areas that have been attacked to prevent the breach from spreading. There are process and regulatory recoveries needed in the post-breach situation requiring the detection of patterns. The study reveals how ML is positively affecting the efficacy of recovery strategies. The fastest and safest paths to restoration can be obtained applying the features of ML. The ML identifies the vulnerabilities within the system and anomalies in user behaviours triggering the breach [12]. Such learning is essential for constructing the safest and quickest path back to the restoration. The use of decision trees within ML can reduce the complexities of generalisation [15]. The analysis is revealing the need for multi-level training in ML models.

B. Practical Implications

There are practical implications for organisations making use of ML to define the fastest and most seamless path for restoration. The use of ML using multi-level training can be helpful in identifying the areas needing isolation in the post-breach situation [14]. The vulnerable patches within the system that need to be rigorously protected after the attack will be identified. Companies facing data breaches can construct robust models of recovery with the integration of ML. The ML can identify the critical patterns within the system leading to improved results.

C. Challenges and Limitations

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

There are inherent limitations associated with the integration of ML models within the system. The ML Models are prone to generalisation errors failing to identify any new anomalies within the system. The ML models can fail to interpret the data appropriately creating a scope of erroneous results. The use of decision trees can empower the outcomes with the testing and assessment of various situations [15]. The use of ML will ensure that companies are able to quickly recover from breaches and prevent their permeation across the system. The safest and fastest path is accomplished with the use of ML models integrated with decision-tree algorithms.

D. Recommendations

The companies are facing incidents of data breaches, consistently affecting their reputation. The use of ML models can aid in identifying the key factors that are responsible for the breaches. The companies should make use of ML models to examine the system prior and post to the breach takes place. The companies should make use of multi-level training of the ML models to attain accurate and precise results [14]. The employees should be trained on the expected user behaviours that can tangibly reduce the chances of an attack taking place. The employees should be trained on the uses of the ML model and their application in the breaches taking place.

VI. CONCLUSION AND FUTURE WORK

The study is analysing the use of the ML model for the fastest and safest recovery path in case of data breaches occurring. The analysis reveals how the ML model is increasing the efficacy of recovery strategies with the isolation of affected systems and blocking malicious IP addresses identified. The anomalies in user behaviour triggering the attack are being extracted as well. The ML model is hence being impactful in driving the necessary improvements for organisations affected by data breaches. Future work should focus on how the ML models should be implemented in the existing systems to enable fast recovery.

VII. REFERENCE LIST

[1] Shan, S., Ding, W., Wenger, E., Zheng, H. and Zhao, B.Y., 2022, November. Post-breach recovery: Protection against white-box adversarial examples for leaked dnn models. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2611-2625).

[2] Zhang, X., Yadollahi, M.M., Dadkhah, S., Isah, H., Le, D.P. and Ghorbani, A.A., 2022. Data breach: analysis, countermeasures and challenges. *International Journal of Information and Computer Security*, *19*(3-4), pp.402-442.

[3] Greve, M., Masuch, K. and Trang, S., 2020. The More, the Better? Compensation and Remorse as Data Breach Recovery Actions-An Experimental Scenario-based Investigation. In *Wirtschaftsinformatik (Zentrale Tracks)* (pp. 1278-1293).

[4] Ou, C.X., Zhang, X., Angelopoulos, S., Davison, R.M. and Janse, N., 2022. Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. *International Journal of Information Management*, *65*, p.102498.

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

[5] Xu, C., Chen, B., Lu, C., Huang, K., Peng, X. and Liu, Y., 2022, November. Tracking patches for open source software vulnerabilities. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 860-871).

[6] Mohammed, Z., 2022. Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People*, *2*(1), pp.41-59.

[7] Issa, O., Silva-Lopez, R., Baker, J.W. and Burton, H.V., 2023. Machine-learning-based optimization framework to support recovery-based design. *Earthquake Engineering & Structural Dynamics*, *52*(11), pp.3256-3280.

[8] Hakim, A. R., Ramli, K., Gunawan, T. S., and Windarta, S. 2023. A novel digital forensic framework for data breach investigation. *IEEE Access*, *11*, 42644-42659.

[9] Neto, N.N., Madnick, S., Paula, A.M.G.D. and Borges, N.M., 2021. Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)*, *13*(1), pp.1-33.

[10] Bilgin, Z., Ersoy, M.A., Soykan, E.U., Tomur, E., Çomak, P. and Karaçay, L., 2020. Vulnerability prediction from source code using machine learning. *IEEE Access*, *8*, pp.150672-150684.

[11] Palaniappan, G., Sangeetha, S., Rajendran, B., Goyal, S. and Bindhumadhava, B.S., 2020. Malicious domain detection using machine learning on domain name features, host-based features and web-based features. *Procedia Computer Science*, *171*, pp.654-661.

[12] Palacios, R. and Morales-Rocha, V., 2021. A proposal for data breach detection in organizations based on user behavior. *Computational Intelligence for Business Analytics*, pp.283-300.

[13] Lye, K.O., Mishra, S. and Molinaro, R., 2021. A multi-level procedure for enhancing accuracy of machine learning algorithms. *European Journal of Applied Mathematics*, *32*(3), pp.436-469.

[14] Krishnan, M., 2020. Against interpretability: a critical examination of the interpretability problem in machine learning. *Philosophy & Technology*, *33*(3), pp.487-502.

[15] Sarailidis, G., Wagener, T. and Pianosi, F., 2023. Integrating scientific knowledge into machine learning using interactive decision trees. *Computers & Geosciences*, *170*, p.105248.

[16] Bentouhami, H., Casas, L. and Weyler, J., 2021. Reporting of "Theoretical Design" in explanatory research: a critical appraisal of research on early life exposure to antibiotics and the occurrence of asthma. *Clinical Epidemiology*, pp.755-767.

[17] Vujović, Ž., 2021. Classification model evaluation metrics. *International Journal of Advanced Computer Science and Applications*, *12*(6), pp.599-606.

Power System Technology
ISSN:1000-3673
Received: 16-11-2025 Revised: 05-12-2025 Accepted: 05-01-2026

[18] OpenBankingExpo.com, 2023, *HSBC being 'closely' monitored by CMA after Open Banking breaches*, Available at : https://www.openbankingexpo.com/news/hsbc-being-closely-monitored-by-cma-after-open-banking-breaches/ [Accessed on : 3rd May, 2024]

[19] FirewallTimes.com, 2023, *Facebook Data Breaches: Full Timeline Through 2023*, Available at: https://firewalltimes.com/facebook-data-breach-timeline/ [Accessed on: 5th June, 2024]

[19] Goli, S. R. (2025). Towards Converged MLOps and SRE: Adaptive AI-Driven Reliability Strategies in Cloud Environments. Available at SSRN 5741602.

[21] Devapathni Yugandhar, M. B., Goli, A. K. R., Goli, S. R., & Chawla, N. (2025, August). Comprehensive Analysis of Challenges in Deploying AI Models in FinTech. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS).

[22] Chintale, P., & Gupta, G. (2025). Security and Privacy Issues in AI-Blockchain Enabled Digital Twin–Based Smart Grid. In AI and Blockchain in Smart Grids (pp. 127-141). Auerbach Publications.

[23] Goli, S. R., Deshpande, G., Konda, R., & Goli, A. K. R. (2025, August). Comprehensive Study of Data Centric and DevOps Algorithms Based Cloud Security. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-5). IEEE.