International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(8s) 2026 pp. 1086-1098
https://doi.org/10.70917/ijcisim-2026-3413
Article

Dynamic Trust Boundary Frame Work for Enterprise Data Leakage Prevention

Nagarathinam A[1], T. Prabhu[2], Jeevalatha R[3]

[1]Department of Computer Science, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India.
Email: nagarathinam2161@gmail.com
[2]Department of Computer Applications, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, India.
Email: Prabhu.cse@drmgrdu.ac.in
[3]Department of Chemistry, Panimalar Engineering College, Chennai, Tamil Nadu, India.
Email: jeevalathar@gmail.com

Abstract: With the growing trend of cloud systems, remote work places, and enterprise network connections, enterprise data leakage is an emerging cybersecurity problem. Conventional Data Leakage Prevention (DLP) solutions are typically rigid and based on trust assumptions and pre-established security policies, which fall short when facing the changing landscape of insider threats and unusual user behavior. This study presents a Dynamic Trust Boundary Framework (DTBF) for enterprise data leakage prevention leveraging the CERT Insider Threat Dataset, to overcome these limitations. The proposed architecture combines data pre-processing, behavioral profiling, anomaly detection, computation of dynamic trust, risk estimation and adaptive access control. 25,000 activity records were analyzed during the preprocessing, which resulted in a total of 1520 duplicate records, 1100 missing records and 850 inconsistent records. The most influential security indicators are revealed to be login frequency (0.92), file access activity (0.88) and email behavior (0.81) by feature importance analysis. The anomaly detection module detected high risk events with scores of 95 and 98 respectively, and the dynamic trust scores ranged from 0.61 to 0.83 based on the user behaviour. The experimental results showed that the detection rate of DTBF was 98.5%, the classification accuracy was 98.2%, which is better than DLP, Zero Trust, Random Forest, SVM, and KNN. This research has proven that DTBF is an effective, adaptive, and scalable solution to prevent data leakages proactively in enterprise.

Keywords: Data leakage prevention, dynamic trust boundary, cognitive security analytics, predictive cybersecurity, leak localisation, insider threat detection, adaptive access governance, enterprise security.

1. Introduction

There can be damaging effects from data leak incidents including; financial loss, reputational harm, regulatory fines, loss of intellectual property, and disruption of business operations; as reported by [4]. Most (DLP) solutions tend to be static security policies, role-based access controls, and static trust assumptions; despite providing a base level of protection, they cannot handle the dynamic threat scenarios presented by insider threats, compromised credentials, privilege escalation attacks, "advanced persistent threats (APTs)", and unauthorized data movement across multiple, heterogeneous enterprise environments [6]. With the increased use of hybrid clouds and decentralized workforces, perimeter based security models are becoming less effective; adaptive and contextually aware security models will become essential [7]. The new innovations in “Zero Trust Architecture (ZTA)” models adopt the philosophy of “never trust, always verify”; through the continuous authentication and authorization for users, devices, and applications. However, there are still a lot of current zero trust implementations that utilize static trust scores and only analyze very narrow contextual elements that generates longer threat response timelines and result in the inability to adequately respond to the continuously shifting security landscape [8]. In addition, the evolving nature of the trust between enterprise ecosystems is based on multiple factors, such as user/device status, access, network availability, data classification (or sensitivity) and the history of security events surrounding an incident [9]. This makes it less ideal to use static trust boundaries to determine what may be considered as anomalous activity indicative of data loss [10] and therefore not trustworthy.

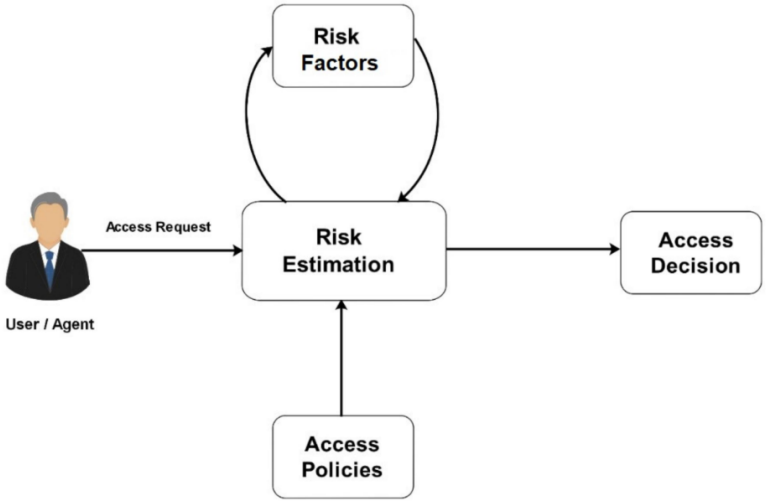

Figure 1: Risk-Based Access Control Framework [11]

To address these limitations, this research proposes an Enterprise Data Leakage Prevention Dynamic Trust Boundary Framework (DTBF). The proposed framework is based on the continuous monitoring of the trust levels associated with a given request, by applying an array of multidimensional contextual parameters, and uses real-time risk assessment to adjust access privileges dynamically (12). As mentioned previously, the DTBF will provide multiple levels of trust, which will include behavioral analytics, adaptive trust scores, risk-aware access controls, and ongoing monitoring mechanisms, which allows for flexible trust boundaries depending on how users behave in relation to their environment (13). The DTBF will proactively detect any suspicious activities; provide greater resistance against unauthorized access to data; and improve the overall organization's resilience to any type of threat, both internally and externally [14].

This paper proposes a Dynamic Trust Boundary Framework (DTBF) that leverages Al to assess real-time trustworthiness levels based on dynamic criteria, allowing for improved anticipatory protection methods as opposed to traditional non-AI or static methods, commonly used with electronic data protection solutions such as Data Loss Prevention (DLP) products. DTBF will augment traditional methodologies by utilizing increased context-based decision-making approaches in providing the ability to assess risk-changing conditions in real time while maintaining data integrity; ensure appropriate authorization; improve protection (i.e., use secure methods to access enterprise information); establish policy management based on user identity (i.e., role-based access control (RBAC)); generate a risk profile for monitoring and analysis of data lost (e.g., e-commerce, credit card) via a trust score; and create a dynamic access control policy. Furthermore, DTBF incorporates mechanisms/intrusions such as cyber threats, malware, and natural disasters into an organization's existing information system security program:

- To develop a Dynamic Trust Boundary Framework for continuous assessment of trust levels within enterprise environments.
- To design a context-aware trust scoring mechanism that incorporates user behavior, device status, network conditions, and data sensitivity attributes.
- To implement adaptive access control and policy enforcement strategies for mitigating enterprise data leakage risks.
- To evaluate the effectiveness of the proposed framework in detecting anomalous activities and reducing unauthorized data exposure.

2. Related Work

Addressing the challenges of enterprise data leakage and zero trust security has become the focus of recent research, with a focus on adaptive trust management, risk-aware access control, and privacy-preserving architectures. Dacayana et al. (2026) [17] emphasized the need for proactive incident response and effective communication, noting that structured approaches to incident response and transparent communication were found to significantly enhance the restoration of stakeholder trust following a breach. Asheshemi et al. (2026) [18] presented a Blockchain-Based Zero Trust Framework for cloud environments that shows the accuracy of the breach detection achieved is above 95% and the reduction in incident response time is 40%. Likewise, Pigola et al. (2026) [19] have highlighted that trust

management is a strategic organizational asset and that cultural alignment and financial preparedness are the most influential for successful adoption of Zero Trust. In 2009, Khan et al. (2009) [21] proposed Complex Linear Diophantine Fuzzy Relations for Data Loss Prevention (DLP) that enhanced the effectivity of cybersecurity decision making by around 18%. To minimize the attack surface in an MCP environment, Narajala et al. 2026 [21] proposed an enterprise-grade security framework, which provides better governance mechanisms. Sun et al. (2026) [22] presented a privacy-preserving blockchain-based architecture with 21 transactions per second (tps) and an average latency of 3 seconds, with an entropy of zero-knowledge proof (ZKP) of 7.65 bits/byte. In addition, Shonubi et al. (2025) [23] showed how AI-powered anomaly detection and continuous risk scoring can greatly improve federated Zero Trust deployments.

There have been recent innovations that have investigated adaptive security models in enterprise and cloud environment. Park et al. (2025) [24] combined Multi-Level Security and Zero Trust concepts to enhance the capability of anomalous behavior detection, achieving almost 32% higher accuracy than conventional access control approaches. Xu et al. (2025) [25] conducted a survey of 136 Zero Trust studies, finding that 98% of them were not validated in the real world, which indicates the need for adaptive and AI-informed trust mechanisms. Kalejaiye et al. (2025) [26] used federated learning and privacy-preserving methods to enhance secure sharing of cyber-threat intelligence without compromising the information. Rautaray et al. (2025) [27] found that Zero Trust controls led to a 67-73% decrease in insider threats incidents and reduced the mean detection time from 197 days to 12 days. Reddy et al. (2024) [28] used Multi-Agent Systems (MAS) along with collaborative Zero Trust integration to boost the endpoint threat detection efficiency by around 28%. In their study, Daah et al. (2024) [29] implemented a financial security architecture using blockchain, which achieved an increase in authentication reliability of more than 35%. Batan et al. (2024) [30] showed that by applying continuous monitoring and least-privilege mechanisms, unauthorized data access incidents can be reduced by almost 60%.

Other research focuses have been enterprise risk management and intelligent access governance. Rahman, et al. (2024) [31] have demonstrated that Zero Trust Architecture (ZTA) has high positive correlation of $r = 0.721$ and a high variance explained of 58.4% for enterprise security performance. In remote workplaces, the study by Rautaray et al. (2024) [32] found a 68% decrease in security incidents, 73% quicker threat detection, and a 54% increase in adherence to compliance standards. Nangi et al. (2023) [33] presented an AI-based ZT model which was able to detect attacks with 94.7% accuracy, 3.2% false positives and access latency of 1.8 seconds. Nagarajan et al. (2023) [34] proposed an AI-based cloud security solution that integrates federated learning and differential privacy to minimize the risks of unauthorized access by over 70%, while maintaining regulatory compliance. In spite of these progresses, most current methods mainly focus on the static evaluation of trust, the localized risk analysis or on domain-specific implementations. Thus, a Dynamic Trust Boundary Framework, which dynamically adjusts trust based on situational risk factors, is still important for an all-encompassing enterprise data leakage prevention system.

While Zero Trust, blockchain security, anomaly detection using AI, and Data Leakage Prevention systems have made strides, current practices continue to focus on a single approach with static trust assessments and predetermined policies. There are few frameworks that have real-time contextual factors like user action, device status, network state and data sensitivity that recalculate trust continuously. Besides, existing approaches are limited to particular domains and do not offer coherent adaptive access control. As such, Dynamic Trust Boundary Framework is required to facilitate proactive, context-aware and scalable enterprise data leakage prevention.

3. Research methodology

In this study, a “Dynamic Trust Boundary Framework (DTBF)” is proposed for enterprise data leakage prevention (eDLP) based on the CERT Insider Threat Dataset. The methodology combines the data preprocessing, behavioral profiling, anomaly detection, dynamic trust computation, risk estimation, and adaptive access control steps, all of which evaluate the user trustworthiness and security risks continuously. First, the enterprise activity logs are cleaned and normalized and then these logs are transformed to meaningful behavioral features. Figure 2 represent framework of methodology.

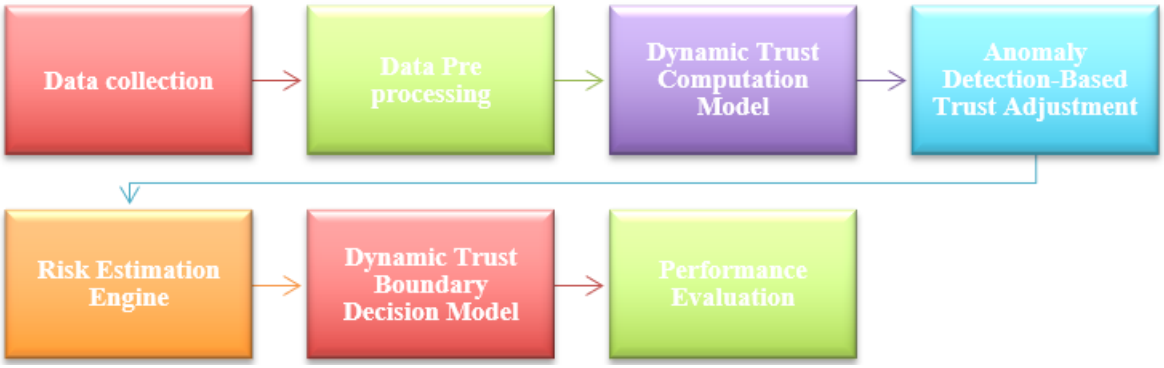

Figure 2: Framework of Methodology

3.1 Data collection

The Carnegie-Mellon University CERT Division has released the CERT Insider Threat Dataset [35] that is widely adopted for insider threat detection research. Recreates authentic employee events in an enterprise environment, such as logon/logoff, email, file access, web browsing, USB device usage and organizational information. This dataset includes both normal and malicious insider activities, allowing researchers to detect data leakage, unauthorized access, and suspicious activities. The CERT dataset is well suited for trust computation, anomaly detection, behavioral analytics and enterprise data leakage prevention studies because of the fact that it contains comprehensive user activity logs and labeled threat scenarios.

3.2 Data Pre processing

- **Data Cleaning**

Raw Raw CERT logs may have duplicate, incomplete and inconsistent logs that could negatively impact trust computation. Data cleaning identifies and eliminates duplicate data and addresses missing data to increase the reliability of the data set. This process guarantees that the user activities are correctly represented prior to analysis.

$$D_{clean} = D_{raw} - D_{duplicate} - D_{missing} \quad (1)$$

where (D_{raw}) is the original dataset, ($D_{duplicate}$) represents duplicate records, and ($D_{missing}$) denotes incomplete entries removed during preprocessing.

- **Feature Extraction**

Behavioral and security data related to user activities like file access, web browsing, email transactions, login times and USB usage are retrieved. These features are used to build trust and detect anomalies:

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \quad (2)$$

where (F) represents the extracted feature set and (f_n) denotes individual behavioral or security attributes used for trust boundary analysis.

- **Data Normalization**

Some values of feature do not have the same scale, so normalization is performed to ensure all the features are within the range of 0 to 1. This keeps the features that have higher values from overwhelming the learning.

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (3)$$

where (X) is the original feature value, (X_{min}) is the minimum value, and (X_{max}) is the maximum value.

- **Behavioral Profiling**

Employee baseline behaviour profiles are developed based on employee historical activity records. This profile is for normal user activity and is used as a reference to detect suspicious activity and insider threats.

$$BP_i = \frac{\sum_{j=1}^{n} A_{ij}}{n} \quad (4)$$

where (BP_i) is the behavioral profile of user (i), (A_{ij}) is the activity record, and (n) is the total number of observations.

- **Anomaly Detection**

Their profile is compared to user activity to determine if there are any deviations that could be a sign of data leakage attempts. If the activity is above a certain threshold then it is considered anomalous.

$$AS_i = |X_i - \mu_i| \quad (5)$$

where (AS_i) is the anomaly score, (X_i) is the current activity value, and is the mean historical behavior. If ($AS\_i > \epsilon$), the activity is flagged as suspicious.

3.3 Dynamic Trust Computation Model

The Dynamic Trust Computation Model continuously assesses the trustworthiness of enterprise users, devices and applications on the basis of enterprise context information. The proposed model differs from the traditional security systems which assume a static level of trust with the user or device. At the outset each entity is given a default Trust score (T0). When new contextual information is available, the trust score is re-calculated based on that latest information and thus the score is adjusted accordingly to the entity's latest security posture. A higher scored means that the behavior is a valid one, while a lower score means suspected behavior. The ongoing trust assessment allows for adaptive security enforcement and greatly reduces enterprise data leakage risks.

Initial Trust Score $T_i(0) = T_0$ (6)

Dynamic Trust Update $T_i(t+1) = \alpha T_i(t) + \beta UB_i + \gamma DS_i + \delta NS_i$ (7)

Subject to: $\alpha + \beta + \gamma + \delta = 1$ (8)

Normalized Trust Score $TS_i = \frac{T_i(t+1)}{T_{max}}$ (9)

where (TS_i in [0,1]).

where (TSi in [0,1]).

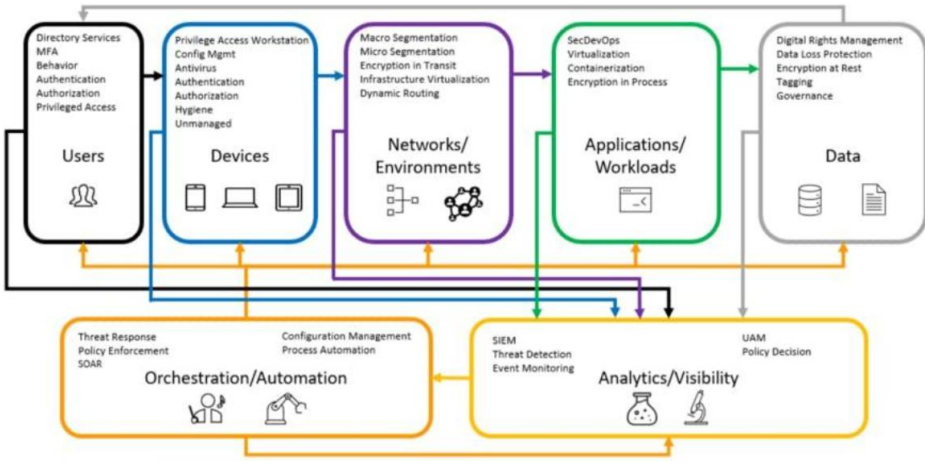

Figure 3: Zero Trust Security Architecture

3.4 Anomaly Detection-Based Trust Adjustment

The Anomaly Detection Based Trust Adjustment module detects user behaviours that are characterized as being out of the ordinary. Out of the ordinary behaviours could be indicative of insider threats, compromised accounts, or attempts to steal sensitive information. To identify any deviation from a user's typical behaviour, the system will continuously compare an active user's actions to a history of their previous actions in real time and then generate an

anomaly score based on how much the user's current behaviour deviates from their normal behaviour. If their anomaly score exceeds the threshold set within the system, the user's trust will be applyed a penalty, which will diminish their trust score. This process enables the system to dynamically alter trust boundaries while they are still in existence and continue to allow access for users who have been flagged by the system for suspicious behaviour to access only limited privileges and continue to grant unrestricted access to users that are deemed to be trusted.

Trust Penalty Function $TP_i = \lambda \times AS_i$ (10)

Updated Trust Score $TS_i^{new} = TS_i - TP_i$ (11)

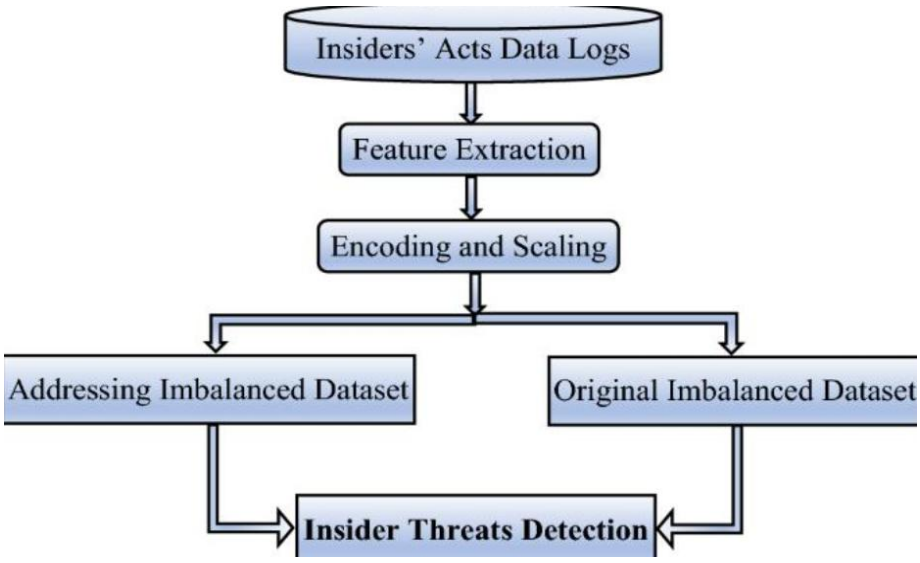

Figure 4: Insider Threat Detection Workflow [36]

3.5 Risk Estimation Engine

The Risk Estimation Engine combines trust information, data sensitivity and threat severity to measure the security risk of each access request. The goal is to prioritize security controls by impacting potential of a security incident. High risk is achieved when a low trust score is associated with sensitive data and high threat levels. On the other hand, trusted users who access low-sensitivity resources pose low risk. The risk score calculated by the framework helps to make smart access control decisions, avoiding the disclosure of sensitive enterprise information by third parties. Enterprises' security infrastructures become more adaptable and responsive through continuous risk evaluation. Risk Score.

$$R_i = (1 - TS_i) \times DL_i \times TH_i \quad (12)$$

3.6 Dynamic Trust Boundary Decision Model

The Dynamic Trust Boundary Decision Model relies on trust and risk values to decide whether or not to approve, deny, or limit access requests. The proposed model re-evaluates trust boundaries dynamically during the running of user sessions, unlike static access control models. Highly trusted entities automatically gain trust and anomalous behavior or increased risks cause trust to shrink. By enforcing least-privilege principles in real-time, this adaptive mechanism helps to reduce the attack surface of enterprise resources and to minimize their associated risks. This helps to reduce the risk of unauthorized access and data leakage, while keeping things running smoothly and productive for users.

Access Decision Function

$$AD = f(TS_i, R_i) \quad (13)$$

The model is able to monitor the user's activities continuously and dynamically adjust the access permissions based on the changing trust and risk conditions.

Algorithm 1: Dynamic Trust Boundary-Based Data Leakage Prevention
Input: User Request URURUR, Context Data C_i
Output: Access Decision AD
Initialize Trust Score $TS_i=T_0$
Collect Context Information $C_i(t)$
Extract User, Device, Network, and Data Features
Compute Dynamic Trust Score
Calculate Anomaly Score
Update Trust Boundary
Estimate Risk Score
Apply Access Policies
Grant, Restrict, or Deny Access
Continuously Monitor User Session
Periodically Recalculate Trust Score

3.7 Performance Evaluation

The proposed model is assessed for the effectiveness with the commonly used classification metrics.

- **Accuracy:** $Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$ (14)
- **Precision:** $Precision = \frac{TP}{TP+FP}$ (15)
- **Recall:** $Recall = \frac{TP}{TP+FN}$ (16)
- **F1-Score:** $F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall}$ (17)

4. Result and Discussion

The proposed Dynamic Trust Boundary Framework (DTBF) with the CERT Insider Threat Dataset using a series of experiments that included: Data Preprocessing, Behavioral Profiling, Anomaly Detection, Trust Computation, and Risk Estimation. The results achieved show the effectiveness of DTBF in the detection of suspicious activities, its ability to dynamically alter trust values, its ability to reduce risks of data leakage from enterprise, and its improvement of the overall security performance. The statistics from the CERT Insider Threat Dataset after data cleaning are shown in Figure 4. The original data set had 25,000 entries, of which 1,520 were duplicated, 1,100 were missing and 850 were inconsistent. Such deviations may have a negative impact on model training and trust score calculation. Data was preprocessed by removing duplicate records, handling missing values with imputation methods, and fixing inconsistent data. Overall, the cleaning process contributed to the overall quality of the data set, with a significant improvement in the integrity of the data and the removal of noise and inaccuracies. This means that the cleaned data set can be used to create reliable data profiles, detect anomalies, establish trust in data over time, and perform enterprise data leakage prevention analysis.

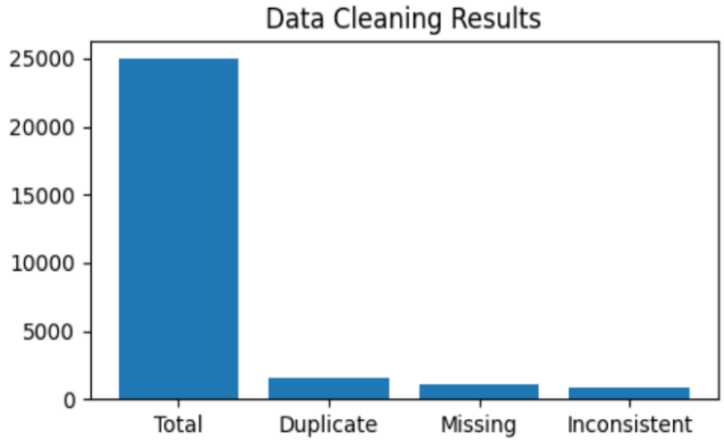

Figure 4: Data Cleaning Results

Figure 5 shows the relative importance of the features extracted and applied in the proposed Dynamic Trust Boundary Framework. Frequent logins (with an importance score of 0.92) were the most important factor in user authentication behavior for the evaluation of trust. Access to files had an importance value of 0.88 and email activity an importance value of 0.81, indicating that these factors are very important to insider threat detection. Next, the use of USB came in with 0.75 and the web browsing behaviour with 0.70. The lowest score for importance was for device related activities, at 0.58. The results show that the accuracy of computing trust and detecting anomalies is greatly affected by behavioral attributes.

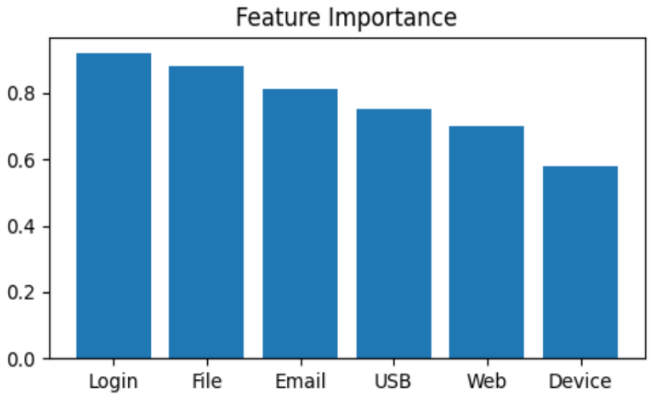

Figure 5: Feature Importance Analysis

The CERT Insider Threat Dataset was used to generate behavioral profiling results using a behavioral profile as shown in Figure 6. The behavioral score was 72 on Day 1, 60 on Day 2, and 68 on Day 3. Day 4 showed the highest behavioral score of 76, which means that there was more legitimate activity. On Day 5, the score dropped to 59, indicating a significant difference from normal. The overall average behavioral score was 67.0. These baseline profiles are used to detect abnormal user activity, to help calculate the trust score, and to improve the accuracy of insider threat detection.

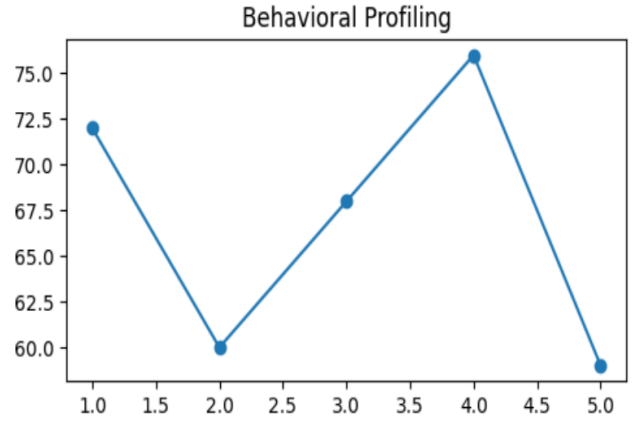

Figure 6: Behavioral Profiling Analysis

The result of the behavioral activity monitoring based anomaly detection is shown in Figure 7. There were three observations with an activity score within the normal range (42, 51, 47). But there is a prominent peak at 95, which means that the behavior is abnormal and is above the pre-defined threshold at observation 4. The score then declined to 44 and then jumped back up to 98 at Observation 6, which is also a high-risk anomaly event. Last observation was 46, and is the return to normal activity. These anomalies are identified and result in updates to the trust score and a risk assessment, which helps to identify insider risks and data leaks in advance.

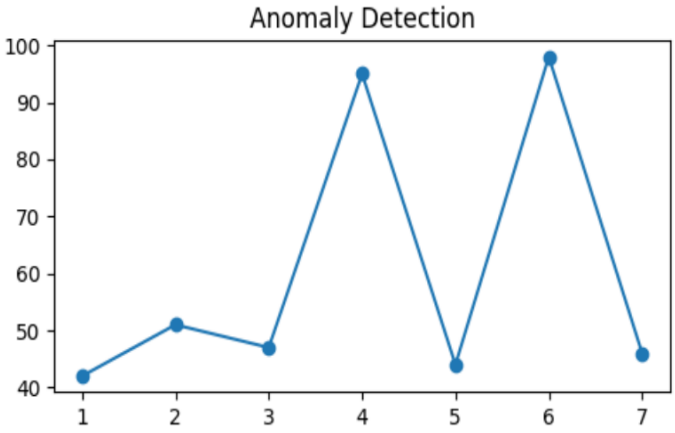

Figure 7: Anomaly Detection Results

The figure 8 shows the change of the proposed Dynamic Trust Boundary Framework's trust scores. The initial trust score was 0.70, and rose to 0.76 and 0.82 in Sessions 2 and 3, demonstrating normal, and trustworthy, user behavior. The score dropped to 0.68 and then to 0.61 in Sessions 4 and 5, respectively, as a result of behavioral deviations that were detected and high risk factors. After the successful verification and normal activity, the trust score was restored to 0.74 and in Session 7 had a score of 0.83. The outcomes of these results prove the framework's ability to adjust trust levels dynamically based on the security situation in real-time and the user's behavior.

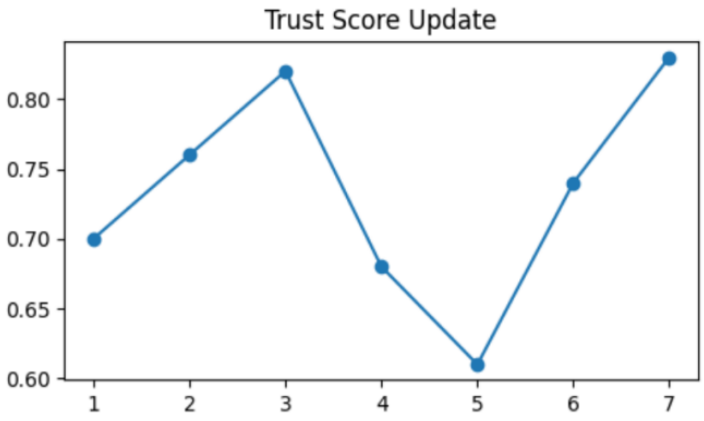

Figure 8: Dynamic Trust Score Update

Figure 9 shows the computed risk values of six enterprise access requests. The lowest risk values were recorded for R1 (0.18) and R6 (0.21) with high levels of trust and low levels of threat exposure on secure access scenarios. Requests that were rated at medium-risk (R2 and R4) were classified as such and will be monitored in addition. R3 had a score of 0.76, above the high-risk threshold of 0.70, while R5 had a score of 0.63, which was close to the high-risk threshold. The results show how well the risk estimation engine prioritizes security responses and how much it can help prevent potential enterprise data leakage incidents.

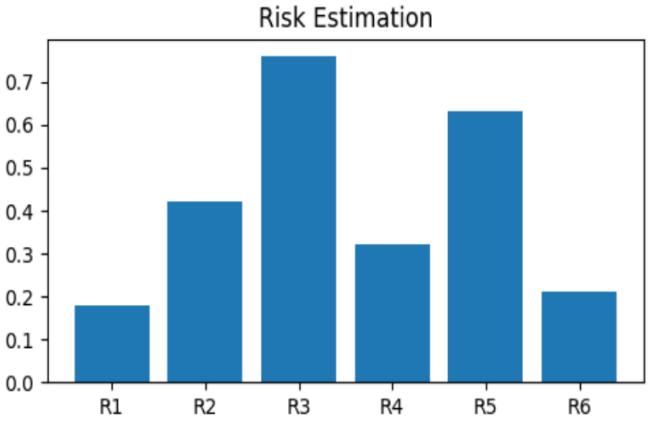

Figure 9: Risk Estimation Analysis

The results of detection performance for enterprise data leakage prevention in different security frameworks are shown in Figure 10. Traditional DLP had 84.6% detection and ZT model had 89.7% detection. The Machine Learning (ML) approach further improved the performance with a detection accuracy of 94.1%. The proposed Dynamic Trust Boundary Framework (DTBF) had the highest detection rate of 98.5% compared to 94.6% for DLP, 99.3% for ZT and 94.1% for the ML model. These results show that the combination of dynamic trust evaluation, anomaly detection and risk-aware access control greatly enhances the effectiveness of enterprise data leakage detection and prevention.

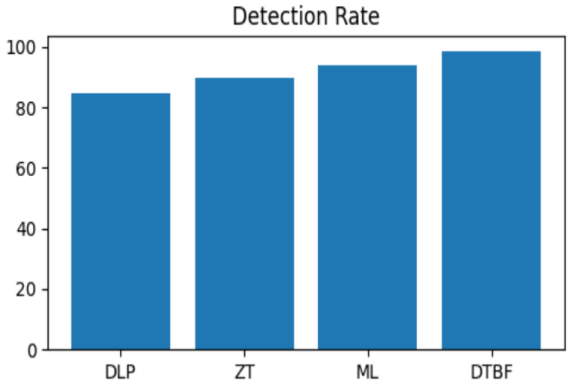

Figure 10: Detection Rate Comparison

The accuracy of classification results in enterprise data leakage detection obtained with different machine learning techniques are shown in the figure 11. The proposed DTBF achieved highest accuracy of 98.2%, which showed that it had the best performance to identify legitimate and malicious activities. The best accuracy achieved by the three models was for the Random Forest (RF) at 93.6%, followed by Support Vector Machine (SVM) with 91.4% and K-Nearest Neighbor (KNN) with 88.7%. The accuracy of DTBF was 4.6%, 6.8% and 9.5% higher than RF, SVM and KNN, respectively. The results demonstrate that the integration of dynamic trust evaluation, anomaly detection and risk-based access control greatly improves the performance of enterprise data leakage prevention.

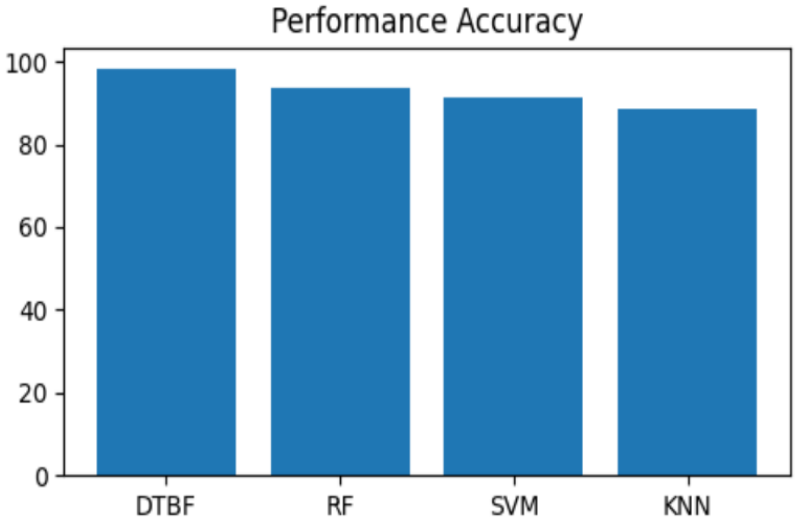

Figure 11: Performance Accuracy Comparison

5. Conclusion

This study proposed a Dynamic Trust Boundary Framework (DTBF) for enterprise data leakage prevention that combines the techniques of behavioral analytics, anomaly detection, dynamic trust computation, risk estimation and adaptive trust-based access control. The proposed framework was evaluated by experiments conducted with the CERT Insider Threat Dataset, that showed its ability to continuously monitor user activities, and dynamically adapt trust boundaries based on the actual security situation of the context. The data quality was enhanced by identifying and eliminating 1,520 duplicate records, 1,100 missing entries and 850 inconsistent records during preprocessing. The most important indicators for insider threat detection, identified during the feature analysis process, were: login behavior (0.92), file access activity (0.88) and email usage (0.81). The anomaly detection module was able to detect high-risk activities with anomaly scores of 95 and 98 with trust computation model dynamically changing trust value between 0.61 and 0.83. The scores from the risk assessment ranged from 0.18 to 0.76, making it possible to prioritize

access decisions. Furthermore, DTBF achieved a 98.5% detection rate and 98.2% classification accuracy, outperforming DLP (84.6%), Zero Trust (89.7%), Random Forest (93.6%), SVM (91.4%), and KNN (88.7%). These findings validate DTBF as a strong and scalable platform for a proactive enterprise data leakage prevention solution.

References

1. Shabtai, Asaf, Yuval Elovici, and Lior Rokach. "Data leakage detection/prevention solutions." In A Survey of Data Leakage Detection and Prevention Solutions, pp. 17-37. Boston, MA: Springer US, 2012.
2. Nurse, Jason RC, Sadie Creese, and David De Roure. "Security risk assessment in internet of things systems." IT professional 19, no. 5 (2017): 20-26.
3. Kindervag, John. "Build security into your network's dna: The zero trust network architecture." Forrester Research Inc 27 (2010): 1-16.
4. Owobu, Wilfred Oseremen, Olumese Anthony Abieba, Peter Gbenle, James Paul Onoja, Andrew Ifesinachi Daraojimba, Adebusayo Hassanat Adepoju, and Ubamadu Bright Chibunna. "Conceptual framework for deploying data loss prevention and cloud access controls in multi-layered security environments." Int. J. Multidiscip. Res. Growth Eval 3, no. 1 (2022): 850-860.
5. Domnik, Jan, and Alexander Holland. "On data leakage prevention maturity: Adapting the C2M2 framework." Journal of Cybersecurity and Privacy 4, no. 2 (2024): 167-195.
6. Wu, Xiaolan, Juan Li, and Wenkun Ren. "Risk Assessment Framework for Data Leakage Prevention Using Machine Learning Techniques." Artificial Intelligence and Machine Learning Review 5, no. 3 (2024): 55-66.
7. Kulkarni, Samarth, and G. N. Girish. "Navigating The Abyss–Illuminating Data Leakage Threats, Mitigations, and Future Horizons." In Cloud Security, pp. 37-51. Chapman and Hall/CRC, 2024.
8. Sachenko, Anatoliy, Petro Vizhevskyi, Oleg Savenko, Viktor Ostroverkhov, and Bogdan Maslyyak. "Modern strategies for data leak detection and prevention in corporate networks." (2025).
9. Onyekaonwu, Chinenye Blessing, Amina Catherine Peter-Anyebe, and Joy Onma Enyejo. "Securing the Digital Vault: Enterprise Data Loss Prevention (DLP) in the Age of GDPR and NDPR."
10. Wong, Wai-Peng, Kim Hua Tan, Kannan Govindan, Di Li, and Ajay Kumar. "A conceptual framework for information-leakage-resilience." Annals of Operations Research 329, no. 1 (2023): 931-951.
11. Atlam, Hany F., Muhammad Ajmal Azad, Madini O. Alassafi, Abdulrahman A. Alshdadi, and Ahmed Alenezi. "Risk-based access control model: A systematic literature review." Future Internet 12, no. 6 (2020): 103.
12. Wettasingha, Ishara Maduranga. "The impact of personal data leakage and perceived risk on brand trust and continuous use of online marketplaces." PhD diss., Vilniaus universitetas., 2025.
13. Oluoha, OLUCHUKWU MODESTA, A. B. I. S. O. L. A. Odeshina, O. L. U. W. A. T. O. S. I. N. Reis, F. R. I. D. A. Y. Okpeke, V. E. R. L. I. N. D. A. Attipoe, and O. Orieno. "A privacy-first framework for data protection and compliance assurance in digital ecosystems." Iconic Research and Engineering Journals 7, no. 4 (2023): 620-646.
14. Herrera Montano, Isabel, Jose Javier Garcia Aranda, Juan Ramos Diaz, Sergio Molina Cardin, Isabel De la Torre Díez, and Joel JPC Rodrigues. "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat." Cluster Computing 25, no. 6 (2022): 4289-4302.
15. Adepu, Rajesh. "Zero trust architecture for large-scale enterprise infrastructure security." International Journal of Engineering & Extended Technologies Research (IJEETR) 5, no. 6 (2023): 171-187.
16. Al Sany, SM Arif, and Siful Islam. "Zero-Trust Architecture Adoption on Financial Data Privacy in Public-Sector ERP Environments." Review of Applied Science and Technology 1, no. 04 (2022): 323-374.
17. Dacayana, Milbert Flores. "Digital Trust Recovery: Effective Data Breach Management Approaches." PhD diss., Walden University, 2026.
18. Asheshemi, Nelson Oghenekevwe, and Michael Adawaren. "Mitigating Insider Threats and Data Breaches in Nigerian Financial Cloud Systems Using a Blockchain-Based Zero Trust Framework." Scientific Journal of Engineering, and Technology 3, no. 1 (2026): 28-43.
19. Pigola, Angélica, Fernando de Souza Meirelles, and Priscila Rezende Da Costa. "Trust Management in the Age of Zero trust: a comprehensive multi-method analysis from enterprise challenges." Enterprise Information Systems 20, no. 1 (2026): 2588753.
20. Khan, Sami Ullah, Abdul Nasir, and Malaika Marwat. "Investigation of threats to data states in data loss prevention using the concept of complex linear diophantine fuzzy relations." Spectrum of Operational Research 3, no. 1 (2026): 128-152.
21. Narajala, Vineeth Sai, and Idan Habler. "Enterprise-grade security for the model context protocol (mcp): Frameworks and mitigation strategies." In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), pp. 1-8. IEEE, 2026.
22. Sun, Ruikang, and Shaopeng Guan. "A blockchain-based privacy-preserving data governance framework for Industry 5.0 smart factories." Peer-to-Peer Networking and Applications 19, no. 1 (2026): 12.
23. Shonubi, Joye Ahmed. "Multi-Layered Zero Trust Architectures for Cross-Domain Data Protection in Federated Enterprise Networks and High-Risk Operational Environments." Int. J. Res. Publ. Rev 6 (2025): 146-169.
24. Park, Jun-Hyung, Sung-Chae Park, and Heung-Youl Youm. "A proposal for a zero-trust-based multi-level security model and its security controls." Applied Sciences 15, no. 2 (2025): 785.

25. Xu, Dan, Iqbal Gondal, Xun Yi, Teo Susnjak, Paul Watters, and Timothy R. McIntosh. "The Erosion of Cybersecurity Zero-Trust Principles Through Generative AI: A Survey on the Challenges and Future Directions." Journal of Cybersecurity and Privacy 5, no. 4 (2025): 87.
26. Kalejaiye, Adebayo Nurudeen. "Federated learning in cybersecurity: privacy-preserving collaborative models for threat intelligence across geopolitically sensitive organizational boundaries." Int J Adv Res Publ Rev 2, no. 07 (2025): 227-50.
27. Rautaray, Aditya. "IMPLEMENTING A ZERO-TRUST SECURITY FRAMEWORK TO MITIGATE INSIDER THREATS IN CLOUD-BASED INFRASTRUCTURES." Power System Protection and Control 53, no. 3 (2025): 271-284.
28. Reddy, Rajender Reddy Pell. "Enhancing endpoint security through collaborative zero-trust integration: a multi-agent approach." International Journal of Computer Trends and Technology 72, no. 8 (2024): 86-90.
29. Daah, Clement, Amna Qureshi, Irfan Awan, and Savas Konur. "Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework." Electronics 13, no. 5 (2024): 865.
30. Batan, Ali. "Investigating the Efficacy of Zero-Trust Security Models in Mitigating Insider Threats in Enterprise Environments." International Journal of Advanced Cybersecurity Systems, Technologies, and Applications 8, no. 12 (2024): 10-19.
31. Rahman, Md Arifur, and BM Taslimul Haque. "Secure Distributed Data Processing Using Privacy-Preserving Artificial Intelligence and Zero Trust Architecture for Enterprise Risk Identification and Performance Evaluation." American Journal of Data Science and Analytics 5, no. 12 (2024): 86-124.
32. Rautaray, Aditya. "ZERO TRUST ARCHITECTURES: ENHANCING DATA PROTECTION IN REMOTE WORK ENVIRONMENTS." Power System Protection and Control 52, no. 2 (2024): 65-75.
33. Nangi, Parameswara Reddy, Chaithanya Kumar Reddy Nala Obannagari, and Sailaja Settipi. "A Multi-Layered Zero-Trust Security Framework for Cloud-Native and Distributed Enterprise Systems Using AI-Driven Identity and Access Intelligence." International Journal of Emerging Trends in Computer Science and Information Technology 4, no. 3 (2023): 144-153.
34. Nagarajan, Geetha. "AI-Integrated Cloud Security and Privacy Framework for Protecting Healthcare Network Information and Cross-Team Collaborative Processes." International Journal of Engineering & Extended Technologies Research (IJEETR) 5, no. 2 (2023): 6292-6297.
35. https://www.kaggle.com/datasets/nitishabharathi/cert-insider-threat
36. Al-Shehari, Taher, and Rakan A. Alsowail. "Random resampling algorithms for addressing the imbalanced dataset classes in insider threat detection." International Journal of Information Security 22, no. 3 (2023): 611-629.