ROMANIAN JOURNAL OF INFORMATION
SCIENCE AND TECHNOLOGY
Volume 29, Number 1, 2026, 29–40
doi: 10.59277/ROMJIST.2026.1.03

An Approach for Considering Human Factors in Root Cause Analysis of Network Systems

Xun LI[1, *], Fan ZHANG[1], Yingying WANG[1], Xiaoxin QI[1], Jinling LIU[2], and Song LI[1]

[1] Air Force Engineering University, Air Defense and Antimissile School, Xi'an, P.R. China
[2] Air Force Engineering University, Graduate School, Xi'an, P.R. China
`Email: lixun2011@stu.xjtu.edu.cn`*`,xiaoxx_2000@163.com,`
`meet2012ying@sina.com,xxqi@stu.xidian.edu.cn,19859808497@163.com,`
`li_song77@163.com`
* Corresponding author

Abstract. Root cause analysis (RCA) has the capability to uncover the underlying reasons for anomalies and offers robust support for network systems recovery. However, one of the most significant challenges in RCA is the difficulty in capturing and analyzing the fine-grained human factors that trigger anomalies. To address this issue, this paper presents an approach for correlating fine-grained events with key performance indicators (KPIs). Specifically, in this approach, captured function events, treated as fine-grained human factors, are analyzed with modified Petri Nets to determine the root cause of anomalies. The experimental results demonstrate that the proposed approach is highly effective in tracing fine-grained human factors during RCA. Moreover, the F1-score in anomaly recognition can reach approximately 0.79.

Key-words: Anomaly KPIs; fine-grained human factors; function event; root cause analysis.

1. Introduction

Currently, many Internet companies deliver services online, where reliability is essential for profitability. Veriflow surveyed 315 professionals, finding human factors as the main cause of service anomalies [1]. Issues often take hours to report and resolve, representing a paradox in which human errors are fixed manually.

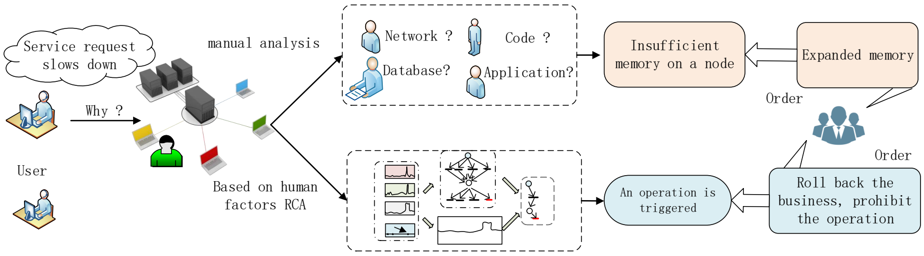


Fig. 1. Effects of different schemes in application scenarios.

To manage anomalies and ensure reliability, companies monitor KPIs, such as quality metrics and request rates. OSSEFS [2] handles missing data. Incidents trigger cascading KPI abnormalities, making root cause analysis (RCA) challenging. Papers [3] and [4] advance prediction and cognition but omit human factors in RCA. Current solutions rarely analyze root causes; even the paper [5], capable of RCA, neglects human elements.

In the scenario shown in Fig. 1, when the system slows down, compared to the traditional method of investigating various KPIs, the RCA considering human factors tries to find human factors that cause insufficient memory resources (e.g., someone performed an incorrect operation at a certain time). It can be seen that an abnormal alarm can be handled by prohibiting improper operations and rolling back the business, rather than adding hardware as soon as an anomaly alarm occurs. Therefore, it is of great importance to take into account human factors for the anomaly RCA. Even in systems that appear to be largely an IT infrastructure [6–8] rather than a human, human factors are involved in the majority of anomalies. Obviously, the finer the granularity, the more accurate the results RCA can achieve.

To date, very few studies have taken the initial step in RCA with human factors. The reviewed studies collectively exhibit methodological commonalities and constraints in multi-dimensional root cause analysis (RCA) frameworks, four principal approaches emerge from the corpus: Multi-dimensional Metric Integration. All examined studies used composite analytical architectures that combined heterogeneous data streams, including network performance metrics and service log analytics. Various technical implementations are observed in all studies: feature correlation matrices [9], risk-weighted prioritization algorithms [10], anomaly propagation graph models [11], and generalized dependency mapping frameworks [12]. Furthermore, deep learning models [13] have a very good guiding effect in predicting anomalies, but all take into account human factors. None human factors data (e.g., operation logs, decision pathways), overlooking team collaboration biases despite [9] mentioning ”service systems,” thereby limiting analysis to technical metrics.

Research conducted in [14–17] analyzes the relationship between KPIs and events. They considered power-off and system refresh as external factors. If these factors are regarded as human factors, they are coarse-grained. The analysis system does not know who performed a specific operation at a specific time. Therefore, it is difficult to locate the root cause of the actual human factor. In addition, Lan [18] proposed a method for system anomaly detection by considering limited human operations. However, this method is only applicable to specific scenarios because it needs to describe the dependence structure in a given dataset.

Thus, the challenges of RCA considering human factors can be listed as: **1)** How to obtain fine-grained human behaviors? **2)** How can RCA effectively account for fine-grained human

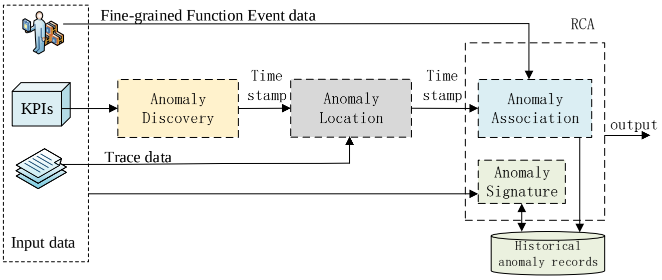


Fig. 2. Proposed framework for considering fine-grained human factors.

factors?

The following solves these two challenges. For the first challenge, the function event is considered a fine-grained human factor. The term ”function event” refers to an occurrence triggered by specific operations, such as system login, data input, or data output. Building upon previous work [19], a method named STAFF was designed and evaluated to capture and utilize these function events. For the second challenge, a modified Petri net is used as a tool to perform anomaly RCA and further improve the RCA against the performance degradation caused by fine-grained human factors.

In summary, STAFF is employed to capture function events, enabling efficient root cause analysis of anomalies by utilizing these function events as fine-grained human factors. The main contributions of this paper are summarized as follows: (1) An RCA framework incorporating human factors into anomaly analysis is proposed. (2) A novel modified Petri net structure, designated as L-Petri, is created to trace root causes.

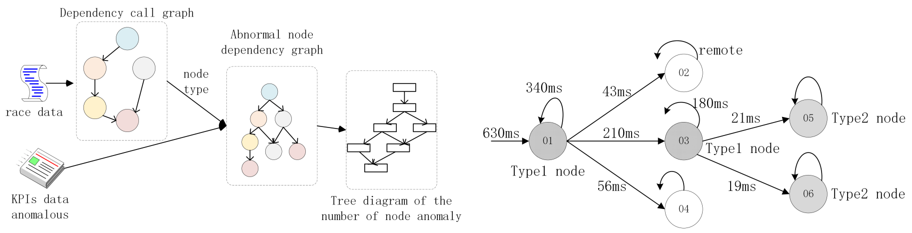
The paper is structured as follows. The framework for RCA considering human factors is treated in Section 2. Section 3 focused on the evaluation. Conclusions are drawn in Section 4.

2. The Framework for RCA Considering Human Factors

Based on the previous work [19] that has been done in automatically identifying fine-grained user behaviors, human factors are incorporated into the root cause analysis to better address the two challenges mentioned in the previous section. As shown in Fig. 2, the proposed framework for Root Cause Analysis (RCA) incorporates human factors and processes three types of input data. It begins by extracting KPI anomalies through an Anomaly Discovery module, followed by pinpointing the affected node via Anomaly Location. Finally, it generates RCA explanations that account for human factors. The determination of the ultimate root cause is achieved by correlating the anomaly’s timestamp with the identified source node in the trace chain and associating it with fine-grained behavioral anomalies.

2.1. Anomaly discovery

The first step is anomaly discovery. The input for this step is the KPIs. For different time series data, integrated methods are used to discover KPIs anomalies to obtain the highest precision and recall. Three types of anomalies were used for feature extraction to facilitate subsequent



(a) Schematic diagram of anomaly location. (b) Illustration of two types of anomaly modes.

Fig. 3. Illustration of anomaly location.

analysis. These anomalies are often encountered in time-series data: outlier data point and turning point. The KPIs of these types of anomalies were extracted for comprehensive calculations.

It is also worth noting that most of the values in the KPI appear normal and the deviation from the predicted value is mainly due to noise. To reduce the influence of noise, three types of abnormal features were amplified. Data magnification was performed using the modified exponential activation,if $x > 0$, $f(\alpha, \beta, x) = e^{min(x,\beta)\times\alpha} - 1$, else, $f(\alpha, \beta, x) = -e^{min(|x|,\beta)\times\alpha} + 1$. It can magnify values that deviate significantly from 0, but has little effect on values close to 0. In this study, the value of α is 0.5. The larger the value, the faster the zooming speed is. The value of β was 10. If $|x| > \beta$, the value of f is not magnified.

Outlier data point is significantly different from the expected value of the time-series at that time. Given a time-series $S = \{S_t|\forall t > 0\}$, predicted value of S_t at time t, denoted by p_t. The simplest measure of deviation is the prediction error, $Pe_t = S_t - p_t$. If the error falls outside some fixed thresholds, the anomaly is identified. This simple idea may work in some cases, but it will not be a good strategy for most because it does not capture the relative error Re_t, $Re_t = \frac{s_t - p_t}{p_t} = \frac{s_t}{p_t} - 1$. By threshold Re_t, one can detect anomalies while normalizing out the dependence on the magnitude of the expected value.

Turning points are those points in time where the behavior of the time series starts to deviate from what is expected. By applying absolute change point detection methods to the sequence of residuals generated via the plug-in approach, changes in the residual distribution can be detected. The error distribution is proposed to be estimated via kernel density estimation [16], and the Kullback-Leibler (KL) [20] divergence, designated TP_e, is subsequently calculated.

Another class of anomaly discovery techniques supported by our framework involves detecting abnormal areas. Abnormal area is a time series with a significant deviation from the average of other time series. The average deviation AA_e of the time series relative to others can be calculated to identify abnormal areas.

2.2. Anomaly location

The solution for anomaly location is as follows: Firstly, a call dependency graph between nodes needs to be generated based on the calling data, as shown in Fig. 3(a); then, calculations are performed using the delay data to mark the suspected anomaly nodes; finally, the abnormal contribution rate is calculated to sort out the anomaly nodes. The dynamic search of trace data along the call relationship leads to the formation of a dependency graph between nodes, where two predefined types of anomaly modes are marked:

- Type1 node: Refers to the child node elapsed time($eTime_c$) divided by the parent node elapsed time ($eTime_p$) greater than or equal to 0.51, i.e.:

$$\frac{eTime_c}{eTime_p} \geq 0.51 \tag{1}$$

- Type2 node: Refers to the parent node elapsed time minus the child node elapsed time, divided by the parent node elapsed time and the result is greater than or equal to 0.51, namely:

$$\frac{eTime_p - \sum eTime_c}{eTime_p} \geq 0.51 \tag{2}$$

To better understand, an example is shown in Fig. 3(b). The node states in the track chain are marked based on the defined node types. Then, the trace chains within a certain time slice are aggregated into a tree graph that marks the number of anomaly occurrences at each node. Through the tree graph, the failure contribution rate of nodes can be calculated at the same depth. After that, using

$$\frac{Tree[depth][status]}{\sum Tree[depth][status]} \geq 0.9 \tag{3}$$

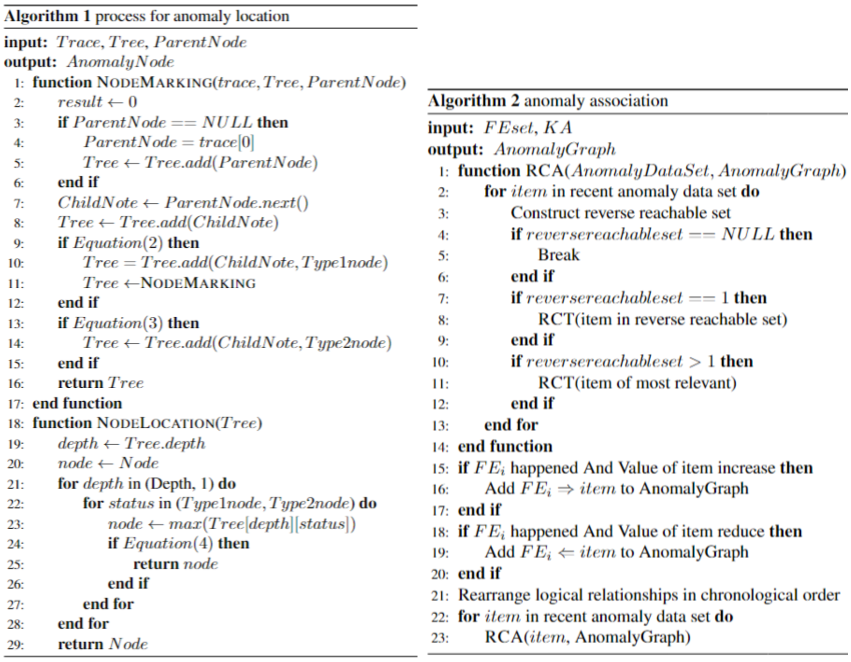
nodes with a failure contribution rate greater than or equal to 90% will be selected. These selected nodes are sorted according to the depth of the hierarchy, forming a set of possible abnormal nodes. Details of the process are shown in Fig. 4(a).

2.3. Anomaly association

The state of the system is changeable, and there is often a connection between the user's operation and the anomalies. Therefore, the association of fine-grained events with anomalies is very important.

The various changes in the system and the relationships between them are described using a Petri Net, which captures the dependencies among system events. However, traditional Petri nets cannot be directly used in our anomaly analysis for the following reasons: 1) There is no one-to-one correspondence between fine-grained events and KPI anomalies, which is a major reason for the difficulty in locating root causes. The KPI anomaly correlation has the characteristic of concurrency. When an anomaly sign appears, the anomaly propagates along multiple paths simultaneously, causing multiple subsequent anomalies. 2) After an abnormal symptom occurs on the Petri net, the factors that cause the abnormal symptom disappear, which obviously does not meet the fact of abnormal diagnosis. 3) The importance of multiple causes of anomalies is different.

Based on the above analysis, a new structure, L-Petri (Fig. 5(a)), is proposed for anomaly graph construction. Each fine-grained event has a KPI anomaly correlation weight k_i that is transmitted and timestamp-distance-dependent (closer timestamps → higher k_i). Anomalies typically result from multiple factors, and a single fine-grained event may trigger multiple anomalies. Here, an anomaly's reverse reachable set is defined as the set of events that can trigger it (e.g., KPI Abnormal 1 in Fig. 5(a) has the set $\{$FE1, FE2$\}$ with weights indicating correlation degree). For fault diagnosis via L-Petri nets, the input library's initial identifier uses tokens to



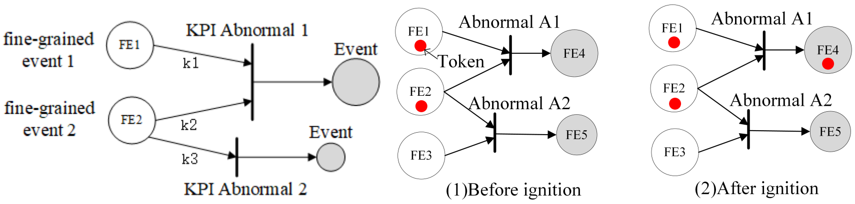
```
Algorithm 1 process for anomaly location
input: $Trace, Tree, ParentNode$
output: $AnomalyNode$
function NodeMarking($trace, Tree, ParentNode$)
    $result \leftarrow 0$
    if $ParentNode == NULL$ then
        $ParentNode = trace[0]$
        $Tree \leftarrow Tree.add(ParentNode)$
    end if
    $ChildNote \leftarrow ParentNode.next()$
    $Tree \leftarrow Tree.add(ChildNote)$
    if $Equation(2)$ then
        $Tree = Tree.add(ChildNote, Type1node)$
        $Tree \leftarrow$NodeMarking
    end if
    if $Equation(3)$ then
        $Tree \leftarrow Tree.add(ChildNote, Type2node)$
    end if
    return $Tree$
end function
function NodeLocation($Tree$)
    $depth \leftarrow Tree.depth$
    $node \leftarrow Node$
    for $depth$ in (Depth, 1) do
        for $status$ in ($Type1node, Type2node$) do
            $node \leftarrow max(Tree[depth][status])$
            if $Equation(4)$ then
                return $node$
            end if
        end for
    end for
    return $Node$
```

(a) Algorithm1: anomaly location

```
Algorithm 2 anomaly association
input: $FEset, KA$
output: $AnomalyGraph$
function RCA($AnomalyDataSet, AnomalyGraph$)
    for $item$ in recent anomaly data set do
        Construct reverse reachable set
        if $reversereachableset == NULL$ then
            Break
        end if
        if $reversereachableset == 1$ then
            RCT(item in reverse reachable set)
        end if
        if $reversereachableset > 1$ then
            RCT(item of most relevant)
        end if
    end for
end function
if $FE_i$ happened And Value of item increase then
    Add $FE_i \Rightarrow item$ to AnomalyGraph
end if
if $FE_i$ happened And Value of item reduce then
    Add $FE_i \Leftarrow item$ to AnomalyGraph
end if
Rearrange logical relationships in chronological order
for $item$ in recent anomaly data set do
    RCA($item$, AnomalyGraph)
```

(b) Algorithm2: anomaly association

Fig. 4. Details of the process algorithm.



(a) Modified Petri net diagram named L-Petri.

(b) Illustration of L-Petri.

Fig. 5. The schematic diagram and examples of L-Petri.

signal fault occurrence (token present = fault sign; empty = no sign). The final diagnosis is determined through L-Petri net reachability and state equations: a token in the target library indicates a fault, while an empty target library indicates no fault (illustrated in Fig. 5(b)).

The next crucial step is to establish a relationship between fine-grained events and KPI anomalies. How to determine the correlation between fine-grained events (FE) and time-series data? This study makes judgments based on when an event occurs; the time series before and after the event occurs are different in terms of data distribution. Select the corresponding N segments of time series data F of length k before (after) FE, and then select a series of data R of length k in the time series. The hypothesis of the test can be expressed as follows: Let $F = R$ be $H0$; otherwise, it is $H1$. If $H0$ is true, it means that the time series and FE are irrelevant. If $H1$ is true, it means that the two sets of data have different distributions, and that time series and

FE are related. If FE and KA(KPI abnormal) are related, This study focuses on determining the temporal order and direction. If they happen at the same time, then $X \Leftrightarrow Y$; if it is negative (i.e., X shifts to the left), then $FE \Leftarrow KA$; otherwise, $FE \Rightarrow KA$. This correlation can be either positive or negative. Finally, relationship diagrams of all correlated abnormalities were obtained. The details of the anomaly association process are shown in Fig. 4(b). After establishing the anomaly graph, the root cause should be traced. To enhance the timeliness of root cause identification and system efficiency, a further extraction of information from historical anomaly cases is performed to leverage prior knowledge for reducing time cost.

3. Evaluation

This section evaluates the performance of the proposed framework with two real-world datasets and one simulation dataset to address research question (RQ1). Subsequently, the Service Provider's real operation and maintenance data is utilized to answer research question (RQ2).

RQ1: How efficiently can the proposed approach detect anomalies?

RQ2: Can the proposed framework trace the fine-grained human factors that are the root cause of anomalies?

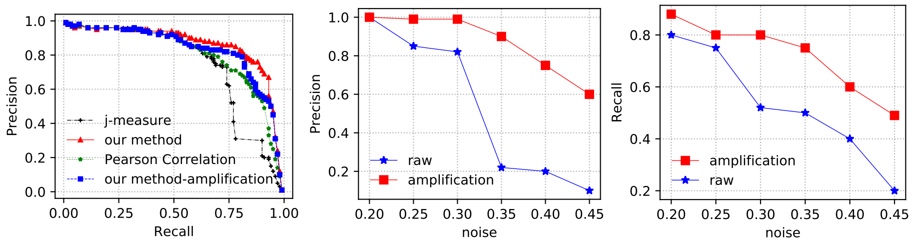
3.1. Answer to RQ1

The empirical study carried out in this paper incorporates two real-world time series datasets in different domains, sourced from the UCR Time Series Classification Archive [21]. These datasets consist of time series in the finance and networking industry domains with a wide range of characteristics. The framework was accompanied by an open-source synthetic time-series generation tool [22] and benchmarking data [23]. In addition, the two datasets from the real-world finance and networking industry domains include most of the outlier data point anomalies. The synthetic dataset includes most of the types of anomalies mentioned in Section 2.1. The root mean square error (RMSE) was used as the evaluation metric to measure the prediction error of the time series. Various commonly used classical methods, such as Support Vector Regression (SVR), Moving Average (MA), and Exponential Smoothing (ES), were utilized for comparison. To objectively evaluate the performance of each method, a simple method was chosen as the baseline: the actual KPI value at time t was set to the predicted KPI value at time $t + 1$. Because the baseline is a rather weak predictor, comparing its performance with that of each method can clearly reveal the actual predictive ability of each method.

Table 1. Comparison of RMSE for anomaly recognition on datasets in different industries

Method	RMSE value in finance dataset \ RMSE value in networking dataset		
	Maximum	Minimum	Average
baseline	0.20\1.62	0.09\0.33	0.07\0.22
SVR	0.17\1.29	0.10\0.62	0.09\0.24
MA	0.21\1.35	0.14\0.37	0.14\0.35
ES	0.18\1.46	0.09\0.31	0.08\0.23
Our approach	**0.16\1.31**	**0.09\0.31**	**0.07\0.20**

RMSE is non-negative, where 0 (rarely attained) indicates perfect fit. Lower values are preferable, but cross-dataset comparisons are invalid due to its scale-dependency. As Table 1



(a) Precision Recall Curve (b) precision of different noise parameters (c) recall of different noise parameters

Fig. 6. The effect of feature magnification.

shows, the proposed combined method achieves lower prediction errors than benchmarks across three KPI characteristics (maximum, minimum, average) and diverse business types, confirming its effectiveness and robustness.

Given the scarcity of real anomaly data, most frameworks are limited to specific time-series patterns and under perform when data characteristics shift. Thus, only classical algorithms were compared. The solution suggested in this paper (without KPI anomaly amplification) was evaluated against J-measure and Pearson analysis. The precision-recall curve in Fig. 6(a) reveals a significant performance gap between non-amplified (blue square curve) and amplified features (red triangle curve). Feature amplification enhances fluctuation prominence and mitigates noise interference. The proposed approach outperforms both J-measure and Pearson correlation: its ensemble approach boosts anomaly recognition accuracy. Pearson surpasses J-measure here because J-measure targets event data correlation, while the test dataset is time-series.

To further illustrate the necessity of data feature amplification, noise was injected into the experimental data to adjust the noise intensity. Fig. 6(b) and (c) shows the changes in accuracy and recall rate of feature data under different noise intensities after using exponential activation to amplify or not. With the increase of noise intensity, the accuracy and recall rate decrease quickly without amplifying the feature data. After feature amplification, the downward trend of accuracy and recall rate has been greatly improved. When the noise intensity is close to 0.45, the accuracy is still at 60% and the recall rate can be maintained at around 0.5. This further illustrates that it is absolutely necessary to enlarge the data features.

Next, the proposed algorithm was further evaluated and compared with different algorithms. The classical algorithms used in the experiments are: 1) random walk (RW), based on the most recent observation; 2) Simple exponential smoothing (SES), which is popular to produce smoothed time-series; 3) HOLT, which smooths the first difference of the smoothed value again; 4) Regression model (RM),which models the relationship between the variables x and y using one or more variables. More details about these algorithms can be found in [24] and [25].

The results of the different datasets described above are shown in Fig. 7. The results are compared in terms of the standard $F_1 - Score = 2 \times \frac{precision \times recall}{precision + recall}$. The results show that there is no absolutely best anomaly discovery algorithm to detect different types of anomalies. Different algorithms are suitable for different data types. Most frameworks target only certain specific time series data. The significance of the approach proposed in this paper is that it integrates a variety of time series models and algorithms to ensure that anomaly discovery has a good effect on different datasets. Three types of KPI anomalies are collected in the synthetic data. This is a reason why the approach proposed in this paper performs particularly well on synthetic datasets.

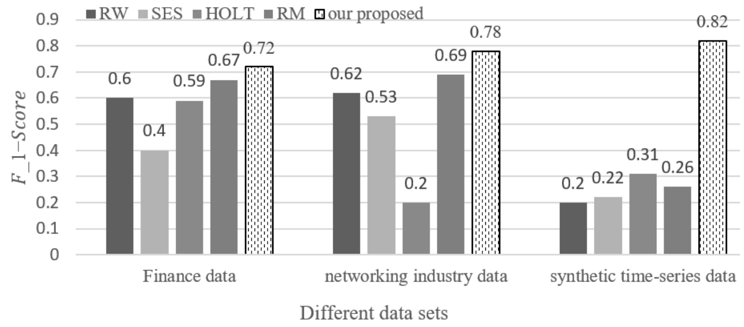


Fig. 7. F1-score comparison of different algorithms on different datasets. Observe that there is no best algorithm on all datasets. For integrating a variety of time series models, the approach proposed in this paper has a good effect.

It also shows the high robustness of the proposed approach.

3.2. Answer to RQ2

To evaluate the ability to analyze the relationship between fine-grained events and KPI anomalies, two baseline algorithms are selected for the experiment. The first is the Pearson correlation [26], which is the widely used method to find correlations in time series. The second baseline is the J-measure [27], which is a widely used method to correlating event data. A single distance measure, Dynamic Time Warping (DTW) [28], is selected for the nearest neighbor method within the algorithm. Collect data for operation and maintenance when the real network service system is running (http://iops.ai/datasetlist/). The $F_1 - Score$ is shown in Table 2.

Table 2. Time Series and Event Data Correlation Test Results Comparison

Method	Real data \ Synthetic data		
	Correlating	Temporal Order	Positive/Negative monotonic
J-Measure	0.62\0.739	N/A\N/A	N/A\N/A
Pearson Correlation	0.691\0.603	N/A\N/A	0.673\0.651
DTW	0.792\0.842	0.81\0.787	0.813\0.833
Our Method	**0.821\0.863**	**0.761\0.811**	**0.878\0.853**

Across different distance measures, no significant performance variation is observed. Comparative experiments demonstrate that the approach proposed in this paper outperforms existing algorithms on the dataset. Notably, the approach proposed in this paper exhibits exceptional capability in temporal order differentiation.

In the experiment, the correlation data presented in Fig. 8 is derived through fine-grained events and time-series association analysis. When a network service anomaly occurs, the backstepping algorithm is initiated, starting from the most recent anomaly. Specifically, once the web service crashes, the algorithm creates a set of reverse-reachable fine-grained events, denoted as {FE7}. Since FE7 is the sole event triggering the transition, the algorithm proceeds with backward calculations from this point. Subsequently, it constructs the reverse-reachable set {FE2, FE3, FE4}. The disk error anomaly has three contributing factors. By applying the conflict res-

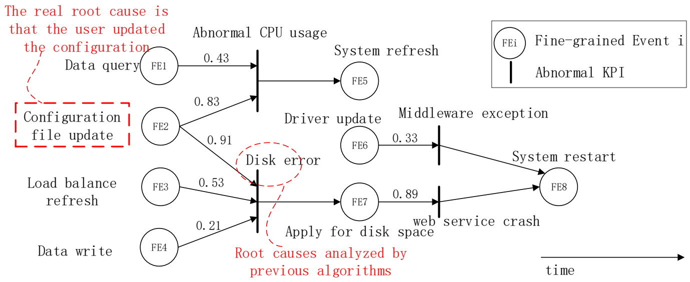
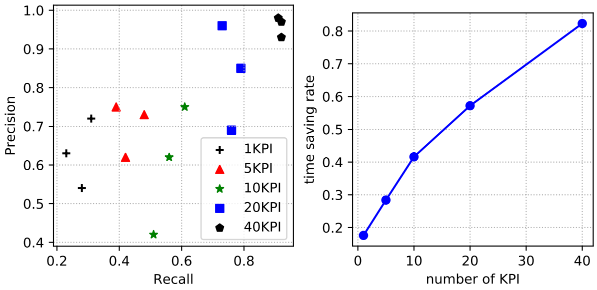


Fig. 8. Anomaly graph of a database constructed by our framework. The previous approaches only trace the root cause to the level of the IT infrastructure itself, but the approach proposed in this paper can trace to the fine-grained human factor level (updated the configuration file).



(a) precision-recalls (b) time saving rate

Fig. 9. The precision-recalls and time savings ratio of different number of KPI.

olution strategy, FE2, which is most closely associated with the change, is selected. Based on this analysis, it is concluded that the disk error resulting from the configuration file update led to the ultimate web-service crash. The root cause is not a hardware problem with the hard disk, but a configuration file update introduced by human factors, with a probability of 0.81 for this conclusion. As a result, operation and maintenance personnel can simply roll back the update to rapidly restore the service. Throughout this process, even though the system issued alarms for abnormal CPU usage and disk errors, these alarms can be ignored. Using human-induced factors, the root cause of the problem can be quickly identified.

As the granularity of root cause analysis becomes increasingly refined, the associated time cost inevitably escalates. To address this challenge, an approach that leverages anomaly signatures is proposed to optimize RCA efficiency. A controlled experiment was conducted with five distinct configurations of monitored KPIs, each repeated three times to ensure statistical robustness. It can be clearly seen from the left side of Fig. 9 that the higher the number of KPI monitored, the more conducive to RCA. The curve on the right side of Fig. 9 shows the comparison of time saving rate, that is $\frac{OTC-TO}{OTC}$. OTC means original time cost and TO refers time cost after optimization. It can be concluded that the more the number of KPI, the more obvious the optimization effect.

4. Conclusions

This paper presents an approach for anomaly RCA that incorporates fine-grained human factors, with a focus on leveraging KPIs to enhance anomaly detection and diagnosis. By integrating function events as fine-grained human factors and using a modified Petri net called the L-Petri net for correlation analysis, the proposed approach effectively traces anomalies back to their root causes, including human-induced errors. Experimental results on real-world and synthetic datasets demonstrate the approach's robustness in identifying KPI anomalies, achieving an F1-score of approximately 0.79. Current approach does not consider the problem of cross-node event combination. This issue is much more complicated, and it will become part of authors' future work.

References

[1] VERIFLOW, *Network complexity, change, and human factors are failing the business*. Accessed: 2019 [Online]. Available: https://www.veriflow.net/survey/.

[2] L. YAN, T. ZHAO, X. XIE and R.-E. PRECUP, *OSSEFS: An online semi-supervised ensemble fuzzy system for data streams learning with missing values*, Expert Systems with Applications **234**, 2023, paper 121060.

[3] C. POZNA and R.-E. PRECUP, *Aspects concerning the observation process modelling in the framework of cognition processes*, Acta Polytechnica Hungarica **9**(1), 2012, pp. 203–223.

[4] S. TRAVIN, O. B. GROMOV, G. DUCA and R.-E. PRECUP, *Statistical computational model of fission products composition of irradiated nuclear fuel and their contribution to gas-aerosol emissions of nuclear power plants*, Romanian Journal of Information Science and Technology **27**(3–4), 2024, pp. 310–322.

[5] Z. YAO, H. YE, C. PEI, G. CHENG, G. WANG, Z. LIU, H. CHEN, H. CUI, Z. LI, J. LI, G. XIE, D. PEI and R. DUCA, *Unsupervised root cause analysis in sparse microservice testing traces*, Proceedings of IEEE 35th International Symposium on Software Reliability Engineering, Tsukuba, Japan, 2025, pp. 1–12.

[6] X. ZHOU, X. PENG, T. XIE, J. SUN, C. JI, D. LIU, Q. XIANG and C. HE, *Latent error prediction and fault localization for micro-service applications by learning from system trace logs*, Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, New York, 2019, pp. 683–694.

[7] Q. DU, T. XIE and Y. HE, *Anomaly detection and diagnosis for container-based micro-services with performance monitoring*, Proceedings of International Conference on Algorithms and Architectures for Parallel Processing, Guanajuato, Mexico, 2018, pp. 560–572.

[8] Z. LAN, Z. ZHENG and Y. LI, *Toward automated anomaly identification in large-scale systems*, IEEE Transactions on Parallel and Distributed Systems **21**(2), 2010, pp. 174-187.

[9] P. JING, Y. HAN, J. SUN,T. LIN and Y. HU, *A novel fault localization schema of multi-dimensional root causes*, Proceedings of 2021 IEEE Wireless Communications and Networking Conference, Nanjing, China, 2021, 1–7.

[10] M. KALANDER, *RiskLoc: localization of multi-dimensional root causes by weighted risk*, arXiv preprint, arXiv:2205.10004, 2022.

[11] Y. SUN, D. CHENG, P. JIN, Q. DING, S. ZHANG, X. CHEN, Y. ZHANG, M. LIANG, D. PEI, J. ZHENG, S. LUO and X. TANG, *Robust anomaly clue localization of multi-dimensional derived measure for online video services*, IEEE Transactions on Services Computing **16**(2), 2022, pp. 1387–1401.

[12] Z. LI, J. CHEN, Y. CHEN, C. LUO, Y. ZHAO, Y. SUN, K. SUI, X. WANG, D. LIU, X. JIN, Q. WANG and D. PEI, *Generic and robust root cause localization for multi-dimensional data in online service systems*, Journal of Systems and Software, **20**, 2023, paper 111748.

[13] U. ESSIZ, C. ACI, E. SARAC and M. ACI, *Deep learning-based prediction models for the detection of vitamin D deficiency and 25-hydroxyvitamin D levels using complete blood count tests*, Romanian Journal of Information Science and Technology **27**(3–4), 2024, pp. 295–309.

[14] H.-D. QIU, Y. LIU, N. A. SUBRAHMANYA and W.-C. LI, *Granger causality for time-series anomaly detection*, Proceedings of IEEE 12th International Conference on Data Mining, Brussels, Belgium, 2012, pp. 1074–1079.

[15] X. NIE, Y. ZHAO, K. SUI, D. PEI, Y. CHEN and X. QU, *Mining causality graph for automatic web-based service diagnosis*, Proceedings of IEEE International Performance Computing and Communications Conference, Orlando, FL, USA, 2016, pp. 1–8.

[16] C. LUO, J. LOU, Q. LIN, Q. FU, R. DING, D. ZHANG and Z. WANG, *Correlating events with time series for incident diagnosis*, Proceedings of 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, NY, USA, 2014, pp. 1583–1592.

[17] V. CHANDOLA, A. BANERJEE and V. KUMAR, *Anomaly detection: A survey*, ACM Computing Surveys **41**(3), 2009, pp. 1–58.

[18] C. HEINZE-DEML, M. H. MAATHUIS and N. MEINSHAUSEN, *Causal structure learning*, Annual Review of Statistics and Its Application, **5**, 2018, pp. 371–391.

[19] Y. TANG, X. LI and L. CHEN, *Automated Signature Generation for Fine-Grained Function Traffic Identification*, Journal of Web Engineering, **17**(5), 2018, pp. 375–398.

[20] V. A. EPANECNIKOV, *Non-parametric estimation of a multivariate probability density*, Theory of Probability & Its Applications **14**(1), 1969, pp. 153–158.

[21] E. KEOGH, X. XI, L. WEI and C. RATANAMAHATANA, *The UCR time series data mining archive* [Online]. Available: https://www.timeseriesclassification.com/dataset.php.

[22] N. LAPTEV and S. AMIZADEH, *Egads source code*. [Online]. Available: https://github.com/yahoo/egads, June 2015.

[23] N. LAPTEV and S. AMIZADEH, *Online dataset for anomaly detection*. [Online]. Available: http://webscope.sandbox.yahoo.com/catalog.php?datatype=s&did=70, April 2015.

[24] R. HYNDMAN and A. B. KOEHLER, *Another look at measures of forecast accuracy*, International Journal of Forecasting **22**(4), 2006, pp. 679–688.

[25] X. WANG, K. SMITH-MILES and R. HYNDMAN, *Rule induction for forecasting method selection: Meta-learning the characteristics of univariate time series*, Neurocomputing **72**(10–12), 2009, pp. 2581–2594.

[26] J. COHEN, *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Hillsdale, NJ, 1988.

[27] G. PIATESKY and W. FRAWLEY, *Knowledge Discovery in Databases*, MIT Press, Cambridge, MA, 1991.

[28] D. BERNDT and J. CLIFFORD, *Using dynamic time warping to find patterns in time series*, Proceedings of 1994 AAAI Workshop on Knowledge Discovery and Data Mining, Seattle, WA, USA, 1994, pp. 359–370.