Journal Pre-proof

Predicting Failures in Multi-Tier Distributed Systems

Leonardo Mariani, Mauro Pezzè, Oliviero Riganelli, Rui Xin

Please cite this article as: Leonardo Mariani, Mauro Pezzè, Oliviero Riganelli, Rui Xin, Predicting Failures in Multi-Tier Distributed Systems, *The Journal of Systems & Software* (2019), doi: https://doi.org/10.1016/j.jss.2019.110464

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Highlights

- PreMiSE predicts failures and locates faults in multi-tier distributed systems

- PreMiSE combines anomaly-based and signature-based approaches

- Approach combination obtains highest accuracy and lowest false positive rate

- Evaluation confirms excellent precision and low overhead in a cloud-based system

- PreMiSE can scale well to large multi-tier distributed systems

Predicting Failures in Multi-Tier Distributed Systems

Leonardo Mariani[a], Mauro Pezzè[a,b], Oliviero Riganelli[a,*], Rui Xin[b]

[a]*Università di Milano-Bicocca, Milan, Italy*
[b]*Università della Svizzera italiana (University of Lugano), Lugano, Switzerland*

Abstract

Many applications are implemented as multi-tier software systems, and are executed on distributed infrastructures, like cloud infrastructures, to benefit from the cost reduction that derives from dynamically allocating resources on-demand. In these systems, failures are becoming the norm rather than the exception, and predicting their occurrence, as well as locating the responsible faults, are essential enablers of preventive and corrective actions that can mitigate the impact of failures, and significantly improve the dependability of the systems. Current failure prediction approaches suffer either from false positives or limited accuracy, and do not produce enough information to effectively locate the responsible faults.

In this paper, we present *PreMiSE*, a lightweight and precise approach to predict failures and locate the corresponding faults in multi-tier distributed systems. *PreMiSE* blends anomaly-based and signature-based techniques to identify multi-tier failures that impact on performance indicators, with high precision and low false positive rate. The experimental results that we obtained on a Cloud-based IP Multimedia Subsystem indicate that *PreMiSE* can indeed predict and locate possible failure occurrences with high precision and low overhead.

Keywords: Failure prediction, Multi-tier distributed systems, Self-healing systems, Data analytics, Machine learning, Cloud computing

*Corresponding author
Email address: `oliviero.riganelli@unimib.it` (Oliviero Riganelli)

1. Introduction

Multi-tier distributed systems are systems composed of several distributed nodes organized in layered tiers. Each tier implements a set of conceptually homogeneous functionalities that provides services to the tier above in the layered structure, while using services from the tier below in the layered structure. The distributed computing infrastructure and the connection among the vertical and horizontal structures make multi-tier distributed systems extremely complex and difficult to understand even for those who developed them.

Indeed, runtime failures are becoming the norm rather than the exception in many multi-tier distributed systems, such as ultra large systems [1] systems of systems [2, 3] and cloud systems [4, 5, 6]. In these systems, failures become unavoidable due to both their characteristics and the adoption of commodity hardware. The characteristics that increase the chances of failures are the increasing size of the systems, the growing complexity of the system–environment interactions, the heterogeneity of the requirements and the evolution of the operative environment. The adoption of low quality commodity hardware is becoming common practice in many contexts, notably in cloud systems [7, 8], and further reduces the overall system reliability.

Limiting the occurrences of runtime failures is extremely important in many common applications, where runtime failures and the consequent reduced dependability negatively impact on the expectations and the fidelity of the customers, and becomes a necessity in systems with strong dependability requirements, such as telecommunication systems that telecom companies are migrating to cloud-based solutions [7].

Predicting failures at runtime is essential to trigger automatic and operator-driven reactions to either avoid the incoming failures or mitigate their effects with a positive impact on the overall system reliability. Approaches for predicting failures have been studied in several contexts, such as mobile devices [9, 10], system performance deviations [11, 12], distributed systems [13, 14], online and telecommunication applications [15, 16, 17].

3

Current approaches for predicting failures exploit either anomaly- or signature-based strategies. Anomaly-based strategies consider behaviors that significantly deviate from the normal system behavior as symptoms of failures that may occur in the near future [18, 12, 19, 13, 20, 21, 22]. Anomaly-based techniques suffer from false positives, because of the difficulty of distinguishing faulty from rare albeit legal behaviors, in the absence of information about failure patterns.

Signature-based strategies rely on known patterns of failure-prone behaviors, called signatures, to predict failures that match the patterns [15, 10, 11, 23, 14, 16]. By working with known patterns, signature-based techniques cannot cope with emerging failures. Moreover, signature-based techniques usually work with patterns of discrete events, such as error reports and system reboots, and do not cope well with failures that directly impact on performance indicators whose values vary in continuous domains over time. Performance indicators with continuous variables that span a wide range of values are common in multi-tier distributed systems, and signature-based techniques working on simple sample-based discretization often have limited accuracy in the presence of combinations of values not experienced in the past.

In this paper, we present *PreMiSE* (PREdicting failures in Multi-tIer distributed SystEms), a novel approach that can accurately predict failures and precisely locate the responsible faults in multi-tier distributed systems. By addressing the challenges that characterize complex multi-tier distributed systems, *PreMiSE* addresses also the subset of challenges that characterize singe-tier systems. *PreMiSE* originally combines signature-based with anomaly-based approaches, to improve the accuracy of signature-based approaches in predicting failures that impact on performance indicators. As illustrated in Figure 1, *PreMiSE*

- monitors the status of the system by collecting (a large set of) performance indicators from the system nodes, for instance *CPU utilization* for each CPU in the system, that we refer to as Key Performance Indicators (KPIs) (*KPI monitoring* in the figure),
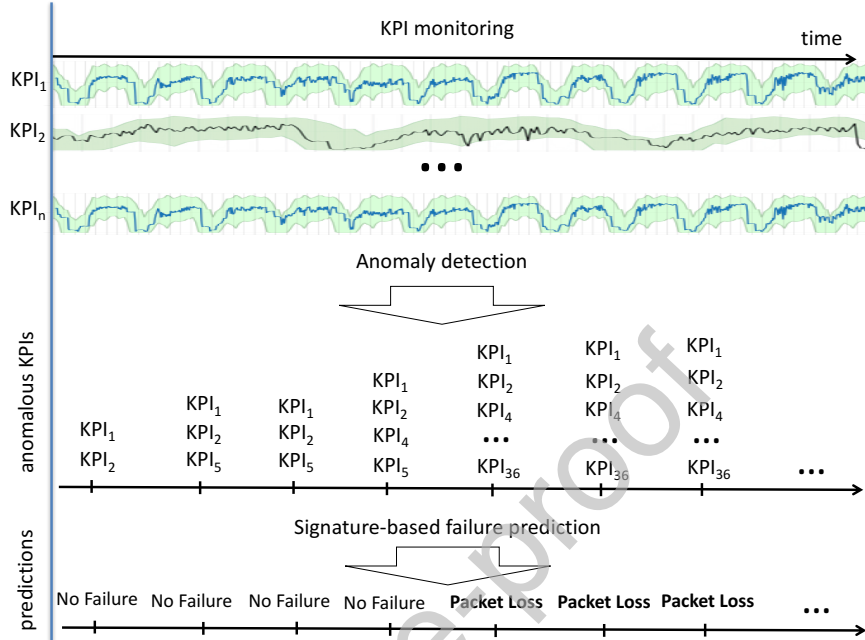
4

Figure 1: The overall flow of *PreMiSE* online activities to predict failures

- identifies deviations from normal behaviors by pinpointing anomalous KPIs with anomaly-based techniques (*Anomaly detection* in the figure),

- identifies incoming failures by identifying symptomatic anomalous KPI sets with signature-based techniques.(*Signature-based failure prediction* in the figure).

In the *KPI monitoring* activity, *PreMiSE* collects KPIs from different layers of the target multi-tier distributed system. KPIs are metrics collected on specific resources, and are the performance indicators that failure prediction approaches use to estimate the status of the system. In the *anomaly detection* activity, *PreMiSE* exploits multivariate time series analysis to identify anomalies. In details, *PreMiSE* elaborates the KPI values collected during a training phase to produce a baseline model that represents the legal behavior of the system, and relies on time series analysis to combine the information from multiple

5

KPIs provided in the baseline model for revealing anomalous behaviors. For example the baseline model can identify a simultaneous increase in both memory usage and memory cached as either a symptom of an anomalous behavior when occurring in the presence of a normal workload, or as a normal albeit infrequent behavior when occurring in the presence of a high workload. The baseline model accurately reveals anomalies in the behavior of the system as a whole, but cannot (i) distinguish between malign and benign anomalies, that is, symptoms of incoming failures from normal albeit uncommon behaviors, (ii) predict the type of the incoming failures, and (iii) locate the sources of the incoming failures.

In the *failure prediction* activity, *PreMiSE* exploits signature-based techniques to accurately distinguish malign from benign anomalies: It identifies the incoming failures that correspond to malign anomalies, predicts the type of incoming failures, and locates the sources of incoming failures. More in details, *PreMiSE* uses historical data about correct and failing behaviors to learn patterns that correlate malign anomalies to failure types, and to relate failures to failure sources. For example, the signature-based failure prediction activity may discard as benign series of anomalous combination of memory usage, memory cached and normal workload, and identify an excessive re-transmission of network packets jointly with a lack of system service response as symptoms of a possible packet loss problem in a network node, problem that may cause a system failure in the long run.

We evaluated *PreMiSE* on a prototype multi-tier distributed architecture that implements telecommunication services. The experimental data indicate that *PreMiSE* can predict failures and locate faults with high precision and low false positive rates for some relevant classes of faults, thus confirming our research hypotheses.

The main contributions of this paper are:

- An approach that combines anomaly- and signature-based techniques to predict failure occurrences and locate the corresponding faults with high precision and low false positive rates, by exploiting information collected

from performance indicators in multi-tier distributed systems. The pro-
posed *PreMiSE* approach can distinguish between anomalous albeit legal
behaviors from erroneous behaviors that can lead to failures, and can
identify the type and location of the causing faults.

- A set of experimental results obtained on a multi-tier distributed sys-
tem that hosts a telecommunication system, which resembles an industrial
telecommunication infrastructure, and which provides evidence of the pre-
cision and accuracy of the approach in the context of cloud systems, a
relevant type of multi-tier distributed systems.

The paper is organized as follows. Section 2 introduces the *PreMiSE* ap-
proach. Section 3 discusses the offline training of the models. Section 4 presents
the online failure prediction mechanism, based on an original combination of
anomaly- and signature-based techniques. Section 5 illustrates the methodol-
ogy that we followed to evaluate the approach, introduces the evaluation metrics
and the experimental setting, provides the essential implementation details of
the evaluation infrastructure, and presents both the types of faults injected in
the system and the reference workload used to evaluate the approach. Section 6
discusses the experimental results about the effectiveness and the overhead of
the proposed approach. Section 7 overviews the main related approaches, high-
lighting the original contribution of our approach. Section 8 summarizes the
main contribution of the paper, and indicates the research directions open with
the results documented in this paper.

2. The *PreMiSE* approach

PreMiSE detects failure symptoms, correlates the detected symptoms to
failure types, and locates the resources responsible of the possible failures which
may occur in the near future.

Several anomalous behaviors of many types can often be observed well in
advance with respect to system failures, which can be frequently mitigated or

7

avoided, especially in multi-tier distributed systems. For instance in cloud systems, early observed communication issues can trigger dynamic reallocation of resources to mitigate or avoid failures. Differently from current approaches, which simply report anomalous behaviors [21, 24, 20, 19], *PreMiSE*

- distinguishes anomalous behaviors that are caused by software faults and that can lead to failures from anomalous behaviors that are derived from exceptional albeit legal situations and that do not lead to failures, thus reducing the amount of false alarms of current failure prediction approaches,

- correlates anomalous behaviors detected at the system level to specific types of faults, and predicts not only the occurrence but also the type of possible failures, thus simplifying the identification of effective corrective actions, and

- identifies the resources likely responsible for the predicted failure, thus providing the developers with a useful starting point for investigating and solving the problem.

As illustrated in Figure 2, *PreMiSE* is composed of an offline model training and an online failure prediction phase. As discussed in details in the next sections, in the *offline model training* phase, *PreMiSE* builds baseline and signature models that capture the system behavior, and in the *online failure prediction* phase, *PreMiSE* uses the baseline and signature models to detect anomalies and predict failures, respectively.

3. Offline Model Training

In the offline learning phase *PreMiSE* builds a *baseline model* and a *signature model*. The baseline model identifies anomalous behaviors that might be interpreted as symptoms of failures, while the *signature model* associates sets of anomalous behaviors to either legal albeit spurious behaviors or symptoms of future failures, and locate the resources likely responsible for the failure.
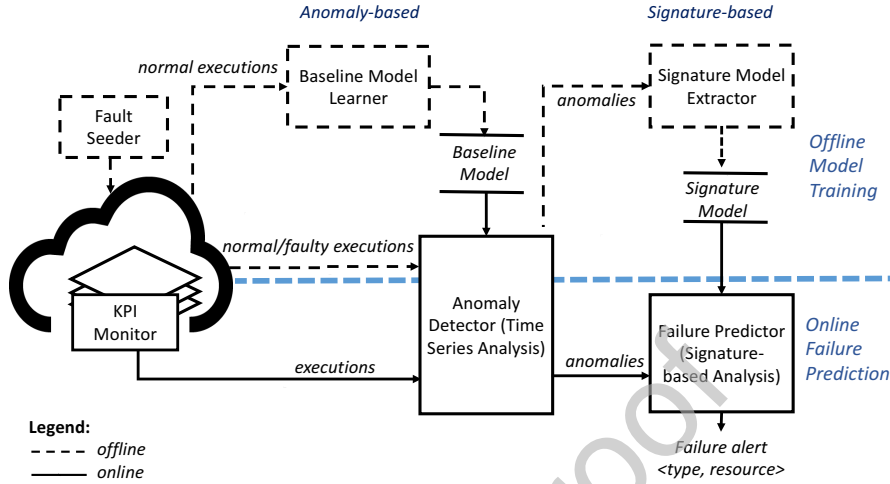
8

Figure 2: The *PreMiSE* learning and predicting phases

As illustrated in Figure 2 in the offline learning phase, *PreMiSE monitors*
160 *series of KPIs* over time under normal execution conditions to *learn the baseline*
model, and *seeds faults* of the target types to *extract the signature model*.

The baseline model is a system model and, as such, it is obtained by modeling
only the failure-free behavior, that is, the normal behavior of the system. The
model is used to calculate the expected values, at which the measured current
165 values are compared to. If the expected and actual values differ significantly,
the system is suspected to not behave as intended. The detection of several
anomalous values is a relevant indicator of failures that may happen in the
future.

In contrast with the baseline model, which focuses on failure-free behaviors,
170 the generation of the *signature model* requires training data for both the failure-
prone and failure-free executions. *PreMiSE* uses the *signature model* to decide
whether sets of anomalies are due to novel but normal behaviors or specific
classes of failures.

PreMiSE can build the models from different kinds of KPIs, granted that
175 their values can be monitored as series of values over time, and can train the sig-

9

nature model with different kinds of seeded faults, granted that the consequent failures occur after some system degradation over time.

As a simple example, *PreMiSE* might detect combinations of anomalous rates of packet re-transmission and aborted operations, by means of the baseline
180 model. It may then associate these anomalous behaviors to either a transient situation due to a high and unexpected peak of requests or to a communication problem that will likely cause a system failure in the future, by means of the signature model. It may also identify the subsystems likely responsible for the incoming communication problems, from the information provided with the
185 detected violations patterns.

While model incompleteness is both possible and probable, this can be compensated by incrementally collecting additional evidence about the behavior of the system. For instance, the baseline model can be improved incrementally and the signature model can be retrained regularly.

190 *3.1. KPI Monitor*

PreMiSE collects an extensive number of KPIs from different tiers of many system components without interfering with the system behavior by relying on lightweight monitoring infrastructures, often natively available at the different levels [25, 26], and elaborates the collected data on an independent node that
195 executes the data processing routines. In this way *PreMiSE* affects the monitored nodes only with the negligible costs of collecting data, and not with the relevant costs of the computation, which is relegated to an independent node. The empirical results reported in Section 6 confirm the non-intrusiveness of the monitoring infrastructure.

200 The values monitored for each KPI are time series data, that is, sequences of numeric values, each associated with a timestamp and a resource of the monitored system. Table 1 reports a sample excerpt of the time series data for the KPI *BytesSentPerSec* collected from a resource named *Homer*[1]. Columns

---

[1]Resource *Homer* is one of the virtual machines used in our empirical setting, a protoype

10

Timestamp, *Resource* and *BytesSentPerSec* indicate the time information, the name of the resource that produced the KPI value, and the number of bytes sent in the last second, respectively.

In the context of this paper, KPIs are metrics measured on specific resources. More formally, a KPI is a pair $< resource, metric >$. For example, *BytesSent-PerSec* collected at *Homer* is a KPI, and the same metric collected at another resource is a different KPI. Thus, the number of collected KPIs depends on the product of monitored metrics and resources.

PreMiSE can be customized with different sets of KPIs, collected at heterogeneous levels. The selection of KPIs depends on the characteristics of the target system, and impacts on the type of failures that *PreMiSE* can detect: *PreMiSE* can detect only failures whose occurrence follows some anomalous behaviors that reflect in anomalies in the series of KPIs monitored over time. We experimented with over 600 KPIs of over 90 different types, collected KPIs at different abstraction levels, ranging from the Linux operating system to the Clearwater application level, and predicted failures of different types, ranging from network to memory failures. We discuss the experimental setting and the results in details in Section 5.3.

Table 1: Sample time series for KPI *BytesSentPerSec* collected at node *Homer*

Timestamp	Resource	BytesSentPerSec
. . .	. . .	. . .
Dec. 20, 2016 22:22:35	Homer	101376
Dec. 20, 2016 22:23:36	Homer	121580
Dec. 20, 2016 22:24:36	Homer	124662
Dec. 20, 2016 22:25:36	Homer	106854
. . .	. . .	. . .

---

of a cloud infrastructure used by telecommunication companies to provide SIP services, as described in Section 5.3. Resource *Homer* is a standard XML Document Management Server that stores MMTEL (MultiMedia TELephony) service settings of the users.

11

3.2. Baseline Model Learner

The *baseline model learner* derives the baseline model from series of KPIs collected under normal system executions, and thus represents correct system

225 behaviors. The *baseline model learner* generates models with inference solutions that capture temporal relationships in time series data, by including trends and seasonalities [27]. In particular, the *baseline model learner* applies Granger causality tests [28] to determine wether a time series variable can predict the evolution of another variable.

230 A time series x is said to be a *Granger cause* of a time series y, if and only if the regression analysis of y based on past values of both y and x is statistically more accurate than the regression analysis of y based on past values of y only. The ability of Granger causality analysis to analyze the dependency between KPIs is a key factor for improving the accuracy of the analysis, because many

235 KPIs are correlated. For instance the CPU load often depends on the rate of incoming requests, and several phenomena could be fully interpreted only by considering multiple time series jointly. For instance, a high CPU load might be anomalous or not depending on the rate of incoming requests that are received by the system.

240 The *PreMiSE* baseline model includes both models for the single KPIs and models of the correlation among KPIs. Figure 3 illustrates a baseline model of a single KPI, namely the model inferred for KPI *BytesSentPerSec* collected from the *Homer* virtual machine. The figure indicates the average value of the time series (dark blue line) and the confidence interval for new samples

245 (light green area around the line). Figure 4 shows an excerpt of a Granger causality graph that represents the causal dependencies among KPIs. Causal dependencies indicate the strength of the correlation between pairs of KPIs, that is, the extent to which changes of one KPI are related to changes of another KPI. Nodes in the causality graph correspond to KPIs, and weighted edges

250 indicate the causal relationships among KPIs, as a value in the interval $[0, 1]$, indicating the increasing strength of the correlation. In the example, the values of *BytesSentPerSec* metric in node *Homer* are strongly correlated to and can
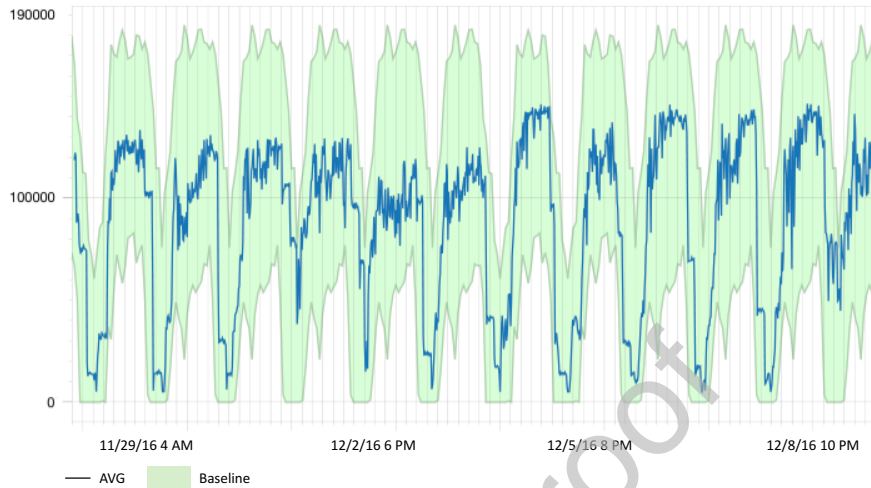
12

Figure 3: A sample baseline model of a single KPI: The *BytesSentPerSec* KPI for the *Homer* virtual machine

thus be used to predict values of *Sscpuidle* metric in node *Homer*.

3.3. Fault Seeder

²⁵⁵   The baseline model captures both the shape of the KPI values over time for single KPIs and the correlation among KPIs under normal execution conditions. The signature model captures the relations among anomalous KPIs observed both during normal execution conditions and with seeded faults. The Signature Model Extractor can be trained with different types of seeded faults,
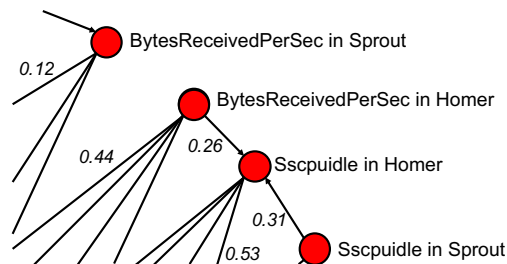

Figure 4: A baseline model of the correlation among KPIs: an excerpt from a Granger causality graph

260 whose consequent failures occur after some system degradation over time. Being trained with seeded faults, the signature model can build patterns of anomalies related to failures, and thus distinguish between benign and failure-prone anomalies when monitoring the system execution. The *Fault seeder* injects a fault of a given type in a system location for each system run. *PreMiSE* can

265 accurately predict failures and locate faults of the types of faults injected in the training phase. Following common practice, we chose the faults to inject according to the Pareto distribution of the frequency and severity of the fault types. The signature model can be extended incrementally to new types of faults.

3.4. Signature Model Extractor

270 The *Signature model extractor* derives the signature model from a sample set of anomalous behaviors that correspond to correct as well as faulty executions. The *Signature model extractor* learns the model from anomalies identified by the Anomaly Detector[2]. Anomalies are tuples $\langle (a_1, \ldots, a_n), f, r \rangle$, where $(a_1, \ldots, a_n)$ is a (possibly empty) sequence of anomalous KPIs that are

275 detected during an execution window of a fixed length, f is a failure type, and r is the resource responsible for the failure. Thus, anomalous KPIs are KPIs without time stamp, and indicate that the KPIs assume anomalous values for at least a time stamp within the considered window. For instance, the tuple $\langle (\langle BytesReceivedPerSec, Homer \rangle, \langle Sprouthomerlatencyhwm, Sprout \rangle,$

280 $\langle Sscpuidle, Sprout \rangle), Packetloss, Sprout \rangle$ indicates three correlated KPIs that assume anomalous values in the considered execution window, and signals a predicted packet loss failure in node Sprout with a likelihood encoded in the tuple $\langle 30, 1 \rangle$, as discussed after in this section.

Both f and r are empty when the execution window corresponds to a normal

285 execution with no active faults. In the training phase *PreMiSE* seeds at most a fault per execution window, and considers execution windows that originate

---

[2]We discuss the Anomaly Detector in details in Section 4 reveals during the training phase, by relying on the baseline model and faulty execution traces.

with the activation of the fault and slide through the faulty execution up to a maximum size, and thus collects anomalies that occur immediately after the fault activation as well as along a possibly long lasting failing execution. We discuss the tuning of the size of the sliding window in Section 6.

PreMiSE records both the type of the failure and the resource seeded with the fault to learn signatures that can predict the failure type and locate the responsible resource. The *Signature Model Extractor* relies on several faults for each type, seeded in different locations, and uses multi-label probabilistic classifiers as signature extractors.

Probabilistic classifiers generate probability distributions over sets of class labels from given sets of samples. *PreMiSE* uses the probability distributions to compute the confidence of the predictions, thus producing a signature model that the *Failure predictor* can exploit to predict both the type of the failure and the location of the resources that are most likely responsible for the failure, and to compute the confidence on the prediction. We empirically investigated signature extractors based on *Support Vector Machine (SVM)*, *Bayesian Network (BN)*, *Best-First Decision Tree (BFDT)*, *Naïve Bayes (NB)*, *Decision Table (DT))*, *Logistic Model Tree (LMT)* and *Hidden Naïve Bayes (HNB)* algorithms. We introduce the algorithms in Section 5.3, and discuss their experimental evaluation in Section 6.

As an example of signature model, Figure 5 shows an excerpt of a decision tree that *PreMiSE* inferred for packet loss failures[3]. Nodes correspond to KPIs and edges indicate the *anomaly* relation. Leaf nodes are annotated with the confidence level of the prediction indicates as pairs $\langle total, correct \rangle$, where *total* is the amount of samples that reach the node, and *correct* is the amount of samples that are correctly classified according to the leaf, that is, the number of samples corresponding to failed executions of the specific type caused by the specific resource, as indicated in the model. The ratio between *correct* and *total*

---

[3]We experimented with different models. Here we report a signature in the form of a decision tree because decision trees are easier to visualise and discuss than other models.
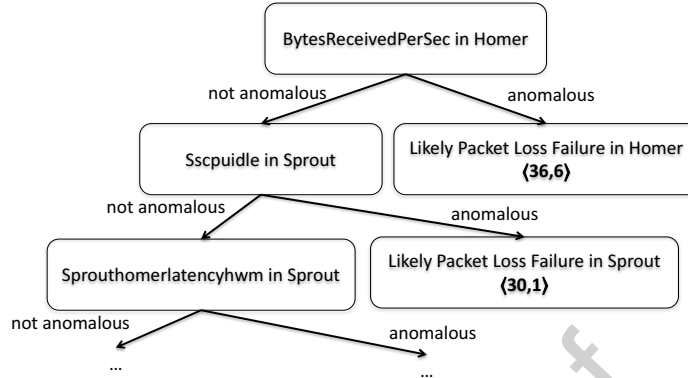
Figure 5: A sample signature model based on decision trees

indicates the likelihood of the prediction to be correct.

The model indicates that anomalous values of *BytesReceivedPerSec* in node *Homer* are a symptom of a possible packet loss failure in node *Homer*, that a combination of non-anomalous values of *BytesReceivedPerSec* in node *Homer* with anomalous values of *Sscpuidle* in node *Sprout* are a symptom of a possible packet loss failure in node *Sprout*, and that the likelihood of a failure increases when both *BytesReceivedPerSec* in *Homer* and *Sscpuidle* in *Sprout* are anomalous. This may happen because packet loss problems may cause a drop in the number of accesses to the user service settings stored in the *Homer* XDMS server, since a packet loss problem may decrease the frequency of authentication requests received by *Sprout* and thus increasing the CPU idle time. The branches of the decision tree not reported in the figure indicate additional relationship between symptoms and failures.

4. Online Failure Prediction

In the online failure prediction phase, *PreMiSE* uses the baseline model to detect anomalies and the signature model to predict failures.
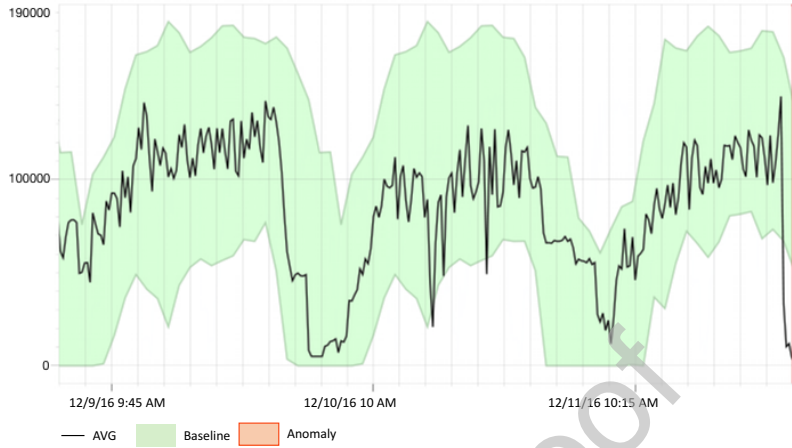
16

Figure 6: A sample univariate anomalous behavior

4.1. Anomaly Detector

Anomalies are behaviors that differ from the expectations, and are thus suspicious. The baseline model encodes expected behavior as a collection of time series of single KPIs and as the Granger correlation among KPIs, as illustrated in Figures 3 and 4, respectively. The *Anomaly Detector* signals univariate and multivariate anomalies when the values of the collected or correlated KPIs differ enough from the baseline model. Univariate anomalies depend on single KPIs, while multivariate anomalies depend on the combination of more than one KPI, each of which may or may not be identified as anomalous by the univariate analysis.

The *Anomaly Detector* detects univariate anomalies as samples out of range, as shown in Figure 6. Given an observed value y_t of a time series y at time t, and the corresponding expected value $\hat{y}_t$ in y, y_t is anomalous if the variance $\hat{\sigma}^2(y_t, \hat{y}_t)$ is above an inferred threshold.

The *Anomaly Detector* detects multivariate anomalies as joint unexpected values of subsets of samples for different variables. It deduces multivariate anomalies among the KPI variables when their relation violates the Granger correlation encoded in the Granger causality graph. For example, it can in-

17

fer that *successful call rate* and *number of incoming calls* are correlated: the

350 *successful call rate* usually decreases with an increasing *number of incoming calls*, and thus the anomaly detector may signal a multivariate anomaly in the presence of a decreasing *successful call rate* without a corresponding increase of *number of incoming calls*, regardless of the results of the univariate analysis of two values. The *Anomaly Detector* identifies multivariate anomalies with

355 the Granger causality test that checks if a set of correlated KPIs preserves the inferred casual relationships.

4.2. Failure Predictor

The *Failure Predictor* identifies possible failures as sets of anomalies that find a matching in the signature model.

360 As discussed in Section 3.4, *PreMiSE* trains the signature model with sets of anomalies detected during execution windows of fixed size in terms of anomalous KPI samples. The *PreMiSE* failure predictor analyzes the sets of anomalies detected in a sliding window of the same size of the windows used during training. For instance, the *Failure Predictor* can predict an incoming packet loss failure in

365 the presence of an anomalous value of *Sscpuidle* (idle time for the authentication service) in node Sprout when occurring with a normal value of *BytesReceivePerSec* (number of received requests) in the Homer XDMS server, based on the signature model shown in Figure 5. In fact, the sequence $\langle\langle BytesReceivePerSec$ $in\ Homer, not\ anomalous\rangle, \langle Sscpuidle\ in\ Sprout, anomalous\rangle\rangle$ in Figure 5 leads

370 to *Likely Packet Loss Failure in Sprout*

PreMiSE generates both *general* and *failure-specific alerts* that correspond to generic failure-prone behaviors and specific failures, respectively. Following common practice in failure prediction solutions that focus their capability to make prediction on recent observations [15], *PreMiSE* collects anomalies in

375 overlapping windows sliding over time. Anomalies first occur in the sliding window that includes the first occurrence of the anomalous KPI, and persist in the following windows, until the anomaly falls out of the windows themselves.

18

Right after injecting a fault, sliding windows include mostly anomalies produced during the previous failure-free execution segments and only few anomalies caused by the injected fault, while forward moving sliding windows include increasingly many anomalies caused by the activated fault. When sliding windows includes only a small portion of anomalies, the prediction might be imprecise. The *Failure Predictor* refines the predicted failure type over time, until the prediction stabilizes. The *Failure Predictor* copes with this transitory phase by refining an initially general prediction into a failure-specific prediction once the prediction stabilizes, that is, it predicts the same failure type with a confidence level of at least 90% for 4 consecutive times.

In the training phase, *PreMiSE* builds signature models starting with data collected just after activating the injected fault, and thus the signature model encodes early predictors, that is, sets of anomalies that occur as early as the fault is activated, often long before the consequent failure. This strategy allows *PreMiSE* to quickly refine a general into a failure-specific prediction, as confirmed by the experimental results reported in Section 6.

The predictions indicates the type of expected failure and the set of anomalous KPIs that substantiate the prediction. *PreMiSE* uses the information about the anomalous KPIs to localize the source of the problem, which might be a resource different from the resources responsible for the anomalous KPIs. For instance in our experiments, *PreMiSE* correctly predicted a packet loss failure in a specific virtual machine by analyzing a set of 37 anomalous KPIs generated by 14 different resources. This is a good example of the importance of locating the fault given a large set of resources involved in the anomalous samples.

5. Evaluation Methodology

In this section, we introduce the research questions (Section 5.1), the testbed that implements a realistic telecom cloud-based system (Section 5.2), the prototype implementation that we used in the experiments (Section 5.3), the fault seeding strategy that we adopted to collect data about failures caused by dif-

19

ferent types of faults (Section 5.4), the workflow that we simulated in the experiments (Section 5.5) and the quality measures that we used to evaluate the results (Section 5.6).

5.1. Research Questions

We address six research questions that evaluate the effectiveness of *PreMiSE* , compare *PreMiSE* with state of the art approaches and quantify the *PreMiSE* overhead.

Effectiveness

To evaluate the capability of *PreMiSE* to successfully predict failures in a realistic cloud-based system we investigate four research questions:

RQ1 *Does the size of the sliding window impact on the effectiveness of* PreMiSE *?* We executed *PreMiSE* with different window sizes, and measured the impact of the window size on the ability to correctly predict failures. We used the results of this experiment to identify an appropriate window size that we used in the other experiments.

RQ2 *Can* PreMiSE *accurately predict failures and localize faults?* We executed *PreMiSE* with different failure types and failure patterns, and measured its ability to predict failures occurrence, types and locations. We experimented with several multi-label mining algorithms, and compare their performance and effectiveness in predicting failures. We used the most effective algorithm in the other experiments.

RQ3 *Can* PreMiSE *correctly identify normal behaviors not experienced in the past?* We executed *PreMiSE* with workflows that differ significantly from the workflow used in the training phase and measured its ability to classify these executions as normal executions.

RQ4 *How early can* PreMiSE *predict a failure?* We executed a number of experiments to determine how early *PreMiSE* can predict failure occurrences, for different types of failures.

20

435   RQ1 is intended to analyze the sensitivity of failure prediction and fault localization to changes in the window parameter. RQ2 focuses on the effectiveness of *PreMiSE* mainly in case of faulty executions, while RQ3 studies *PreMiSE* with perturbed workloads under normal conditions to study the false positive rate. RQ4 investigates prediction time in faulty executions.

440   *Comparison to state-of-the-art approaches*

[R2.1]We compare *PreMiSE* with *IBM OA-PI — Operational Analytics - Predictive Insights* [22], an industrial anomaly-based approach, and with the Grey-Box Detection Approach (G-BDA) of Sauvanaud et al. [22], a state-of-the-art signature-based approach. We discuss the following research question:

445   **RQ5** *Can* PreMiSE *predict failures more accurately than state-of-the-art approaches?* We compare *PreMiSE* to OA-PI and G-BDA by executing all approaches on the same set of normal and failing executions, and comparing their ability to predict failures. Since OA-PI cannot predict the type of failure and locate the corresponding fault, we only evaluated its ability 450 to predict failure occurrences.

Overhead

We investigated the impact of *PreMiSE* on the overall performance of a cloud-based system by addressing the following research question:

RQ6 *What is the overhead of* PreMiSE *on the performance of the target sys-* 455 *tem?* This question is particularly relevant in the context of multi-tier distributed systems with strict performance requirements, like telecommunication infrastructures. Thus, we designed an experiment referring to such applications. *PreMiSE* executes the resource-intensive tasks, that is, anomaly detection and failure prediction, on a dedicated physical server, 460 and thus the overhead on the system derives only from monitoring the KPIs.

21

We evaluated the impact of monitoring the KPIs on the system performance by measuring the consumption of the different resources when running the system with and without KPI monitoring active. Both *PreMiSE*
₄₆₅ and data analytics solutions monitor the same KPIs, and thus share the same performance overhead, but *PreMiSE* further processes the anomalies revealed with data analytics approaches, and presents more accurate predictions than competing approaches.

5.2. Testbed

₄₇₀ As representative case of multi-tier distributed system, we considered the case of a complete cloud-based environment running an industrial-level IP multimedia sub-system. To control the study, we created a private cloud consisting of (i) a controller node responsible for running the management services necessary for the virtualization infrastructure, (ii) six compute nodes that run VM
₄₇₅ instances, (iii) a network node responsible for network communication among virtual machines. The characteristics of the different nodes are summarized in Table 2.

Table 2: Hardware configuration

Host	Controller	Network	Compute (x2)	Compute (x4)
CPU	*Intel(R) Core(TM)2 Quad CPU Q9650 (12M Cache, 3.00 GHz, 1333 MHz FSB)*			
RAM	4 GB	4 GB	8 GB	4 GB
Disk	250 GB SATA hard disk			
NIC	Intel(R) 82545EM Gigabit Ethernet Controller			

We used OpenStack [29] version Icehouse on Ubuntu 14.04 LTS as open source cloud operating system and KVM [30] as hypervisor.

₄₈₀ To evaluate our approach, we deployed Clearwater [31] on the cloud-based infrastructure. Clearwater is an open source IP Multimedia Subsystem (IMS) and provides IP-based voice, video and message services. Clearwater is specifically designed to massively scale on a cloud-based infrastructure, and is a product

originated from the current trend of migrating traditional network functions
from inflexible and expensive hardware appliances to cloud-based software solutions. Our Clearwater deployment consists of the following virtual machines:

Bono: the entry point for all clients communication in the Clearwater system.

Sprout: the handler of client authentications and registrations.

Homestead: a Web service interface to Sprout for retrieving authentication credentials and user profile information.

Homer: a standard XML Document Management Server that stores MMTEL (MultiMedia Telephony) service settings for each user.

Ralf: a service for offline billing capabilities.

Ellis: a service for self sign-up, password management, line management and control of multimedia telephony service settings.

Each component is running on a different VM. Each VM is configured with 2 vCPU, 2GB of RAM and 20GB hard disk space, and runs the Ubuntu 12.04.5 LTS operating system.

Our multi-tier distributed system is thus composed of eight machines running components from three tiers: the operating system, infrastructure and application tiers, running Linux, OpenStack, and virtual machines with Clearwater, respectively. We refer to this environment as the *testbed*.

5.3. Prototype Implementation

Our prototype implementation of the monitoring infrastructure collects a total of 633 KPIs of 96 different types from the 14 physical and virtual machines that comprise the protoype. We collected KPIs at three levels: 162 KPIs at the application level with the SNMPv2c (Simple Network Management Protocol) monitoring service for Clearwater [25], 121 KPIs at the IaaS level with the OpenStack telemetry service (Ceilometer) for OpenStack [26] and 350 KPIs at the operating system level with a Linux OS agent that we implemented for Ubuntu.

23

We selected the KPIs referring to the multi-tired distributed nature of our prototype and the low-impact requirements that characterize most industrial scale systems. We collected KPIs from all the tiers characterizing the system, by relying on already available services, when possible, and on ad-hoc build monitors

515   otherwise. We collected only KPIs that can be monitored with no functional impact and negligible performance overhead. As expected, *PreMiSE* did not impose any limitation on the set of collected and processed KPIs, and we expect this to be valid in general. Studying the impact of noisy and redundant KPIs on the performance of PreMiSE may further improve the technique.

520   At the application tier, *PreMiSE* collects both standard SNMP KPIs, such as communication latency between virtual machines, and Clearwater specific KPIs, such as the number of rejected IP-voice calls. At the IaaS tier, *PreMiSE* collects KPIs about the cloud resource usage, such as the rate of read and write operations executed by OpenStack. At the operating system tier, *PreMiSE* col-

525   lects KPIs about the usage of the physical resources, such as consumption of computational, storage, and network resources. In our evaluation, we used a sampling rate of 60 seconds.

PreMiSE elaborates KPIs from both simple and aggregated metrics, that is, metrics that can be sampled directly, such as CPU usage, and metrics derived

530   from multiple simple metrics, for example the call success rate, which can be derived from the number of total and successful calls, respectively. The *KPI Monitor* sends the data collected at each node to the predictor node that runs *PreMiSE* on a Red Hat Enterprise Linux Server release 6.3 with Intel(R) Core (TM) 2 Quad Q9650 processor at 3GHz frequency and 16GB RAM.

535   We implemented the *Baseline Model Learner* and the *Anomaly Detector* on release 1.3 of OA-PI [22], a state-of-the-art tool that computes the correlation between pairs of KPIs. OA-PI detects anomalies by implementing the following anomaly detection criteria: normal baseline variance, normal-to-flat variation, variance reduction, Granger causality, unexpected level, out-of-range

24

values, rare values[4], and issues alarms after revealing anomalies in few consecutive samples. OA-PI can analyze large volumes of data in real-time (the official IBM documentation show an example server configuration to manage $1,000,000$ KPIs)[5], and thus enables *PreMiSE* to deal with the amount of KPIs that characterise large-scale distributed systems. The OP-PI learning phase requires data from at least two weeks of normal operation behaviors, thus determining the *PreMiSE* two weeks training interval.

We implemented the *Signature Model Extractor* and the *Failure Predictor* on top of the Weka library [32], a widely used open-source library that supports several classic machine learning algorithms. We empirically compared the effectiveness of seven popular algorithms for solving classification problems when used to generate signatures:

- a function-based *Support Vector Machine (SVM)* algorithm that implements a sequential minimal optimization [33],

- a *Bayesian Network (BN)* algorithm based on hill climbing [34],

- a best-first *Best-First Decision Tree (BFDT)* algorithm that builds a decision tree using a best-first search strategy [35],

- a *Naïve Bayes (NB)* algorithm that implements a simple form of Bayesian network that assumes that the predictive attributes are conditionally independent, and that no hidden or latent attributes influence the prediction process [36],

- a *Decision Table (DT))* algorithm based on a decision table format that may include multiple exact condition matches for a data item, computing the result by a majority vote [37],

---

[4]https://www.ibm.com/support/knowledgecenter/SSJQQ3_1.3.3/com.ibm.scapi.doc/
intro/r_oapi_adminguide_algorithms.html
[5]https://www.ibm.com/support/knowledgecenter/en/SSJQQ3_1.3.3/com.ibm.scapi.
doc/intro/c_tasp_intro_deploymentscenarios.html

- a *Logistic Model Tree (LMT)* algorithm that combines linear logistic re-
₅₆₅ gression and tree induction [38],

- a *Hidden Naïve Bayes (HNB)* algorithm that uses the mutual information
attribute weighted method to weight one-dependence estimators [39].

As discussed in Section 6 and illustrated in Table 5, the results of our evalu-
ation do not indicate major differences among the considered algorithms, with
₅₇₀ a slightly better performance of Logistic Model Trees that we adopt in the ex-
periments.

5.4. Fault Seeding

In this section, we discuss the methodology that we followed to seed faults in
the testbed. Fault seeding consists of introducing faults in a system to reproduce
₅₇₅ the effects of real faults, and is a common approach to evaluate the dependability
of systems and study the effectiveness of fault-tolerance mechanisms [40, 41] in
test or production environments [18, 42].

Since we use a cloud-based system to evaluate *PreMiSE*, we identify a set
of faults that are well representative of the problems that affect cloud-based
₅₈₀ applications. We analyze a set of issue reports[6] of some relevant cloud projects
to determine the most relevant fault types that threat Cloud applications. We
analyze a total of 106 issue reports, 18 about KVM[7], 62 about OpenStack[8],
19 about CloudFoundry[9], and 7 about Amazon[10], and we informally assess
the results with our industrial partners that operate in the telecommunication
₅₈₅ infrastructure domain.

We classify the analyzed faults in thirteen main categories. Figure 7 plots
the percentage of faults per category in decreasing order of occurrence for the

---

[6]We conducted the analysis in July 2014 selecting the most recent issue reports at the time
of the inspection.

[7]https://bugzilla.kernel.org/buglist.cgi?component=kvm

[8]https://bugs.launchpad.net/openstack

[9]https://www.pivotaltracker.com/n/projects/956238

[10]http://aws.amazon.com

analyzed fault repositories. The figure indicates a gap between the three more frequent and the other categories of faults, and we thus experimented with
590 the three most frequent categories: *Network*, *Resource leaks* and *High overhead* faults. *Network* faults consist of networking issues that typically affect the network and transport layers, such as packet loss problems. *Resource leaks* occur when resources that should be available for executing the system are not obtainable, for instance because a faulty process does not release memory when
595 not needed any more. *High overhead* faults occur when a system component cannot meet its overall objectives due to inadequate performance, for instance because of poorly implemented APIs or resource-intensive activities.
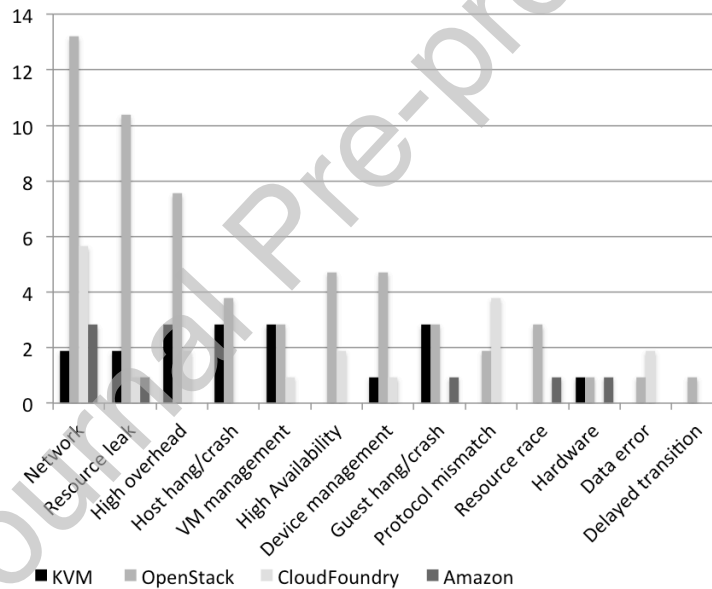
Figure 7: Occurrences of categories of faults in the analyzed repositories

Based on the results of this analysis, we evaluate *PreMiSE* with injected faults of six types, that characterize the three top ranked categories of faults
600 in Figure 7: *Network faults* that depend on *Packet Loss* due to *Hardware* and *Excessive workload* conditions, increased *Packet Latency* due to network delay and *Packet corruption* due to errors in packet transmission and reception, *Re-*

source leak faults that depend on *Memory Leaks*, and *High overhead faults* that depend on *CPU Hogs*. In details, (i) A packet loss due to hardware conditions
605 drops a fraction of the network packets, and simulates the degradation of the cloud network; (ii) A packet loss due to excessive workload conditions corresponds to an extremely intensive workload, and causes an intensive packet loss; (iii) An increased packet latency and (iv) corruption due to channel noise, routing anomalies or path failures, simulates degraded packet delivery performances;
610 (v) A memory leak fault periodically allocates some memory without releasing it, simulates a common software bug, which severely threaten the dependability of cloud systems; (vi) A CPU Hog fault executes some CPU intensive processes that consume most of the CPU time and cause poor system performance.

We limited our investigation to the most relevant categories of faults to
615 control the size of the experiment, which already involves an extremely large number of executions. The results that we discuss in Section 6 demonstrate the effectiveness of *PreMiSE* across all the faults considered in the experiments. We expect comparable results for other fault categories with the same characteristics of the considered ones, namely faults that lead to the degradation of some KPI
620 values over time before a failure. This is the case of most of the fault categories of Figure 7, with the exception of host and guest crashes, which may sometime occur suddenly and without an observable degradation of KPI values over time. Confirming this hypothesis and thus extending the results to a broader range of fault categories would require additional experiments.

625 We inject packet loss, packet latency, packet corruption, memory leaks and CPU Hogs faults into both the host (Openstack) and guest (Clearwater) layers, and excessive workload faults by altering the nature of the workload, following the approaches proposed in previous studies on dependability of cloud systems [40] and on problem determination in dynamic clouds [41].

630 We study a wide range of situations by injecting faults according to three activation patterns:

Constant: the fault is triggered with a same frequency over time.

28

Exponential: the fault is activated with a frequency that increases exponentially, resulting in a shorter time to failure.

635 **Random:** the fault is activated randomly over time.

Overall, we seeded 12 faults in different hosts and VMs. Each fault is characterized by a fault type and an activation pattern.

5.5. Workload Characteristics

In practice, it is hard to know if a set of executions is general enough. In our 640 specific settings, we define the workload used in the experimental evaluation to replicate the shape of real SIP traffic as experienced by our industrial partners in the telecommunication domain. We carefully tuned the peak of the workflow to use as much as 80% of CPU and memory. We generate the SIP traffic with the SIPp traffic generator [43], which is an open source initiative from Hewlett-645 Packard (HP) and is the de facto standard for SIP performance benchmarking.

SIPp can simulate the generation of multiple calls using a single machine. The generated calls follow user-defined scenarios that include the exact definition of both the SIP dialog and the structure of the individual SIP messages. In our evaluation, we use the main SIP call flow dialogs as documented in Clearwater[11].

Our workload includes a certain degree of randomness, and generates new calls based on a call rate that changes according to calendar patterns. In particular, we consider two workload patterns:

Daily variations The system is busier on certain days of the week. In particu-655 lar, we consider a higher traffic in working days (Monday through Friday) and lower traffic in the weekend days (Saturday and Sunday). Figure 8 graphically illustrates the structure of our workload over a period of a week.

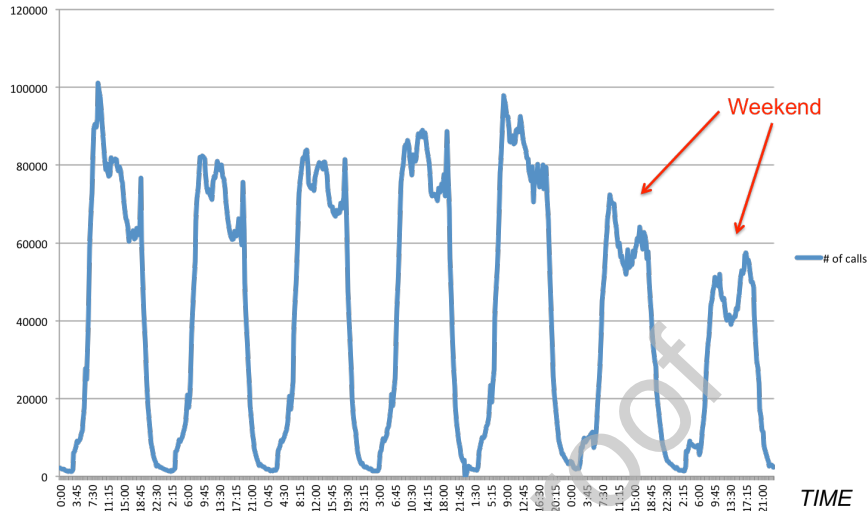[11]http://www.projectclearwater.org/technical/call-flows/

29

Figure 8: Plot with calls per second generated by our workload over a week

Hourly variations To resemble daily usage patterns, our workload is lighter
₆₆₀ during the night and heavier during the day with two peaks at 9am and
7pm, as graphically illustrated in Figure 9.

In our empirical evaluation, we obtained good results already with the work-
load that we designed, without the need of introducing extensive variability in
the normal executions used for training. This is probably a positive side effect
₆₆₅ of the usage of anomaly detection and failure prediction in a pipeline. In fact,
the failure predictor component can compensate the noise and false positives
produced by anomaly detector.

5.6. Evaluation Measures

We addressed the research questions RQ1, RQ2 and RQ5 by using 10-fold
₆₇₀ cross-validation [44]. *PreMiSE* analyzes time series data, and collects anomalous
KPIs every 5 minutes, to comply with the requirements of IBM OA-PI [22],
the time series analyzer used in *PreMiSE* . Signature-base analysis does not
consider the order in which the sliding windows are arranged, thus we collected
the *samples* necessary to apply 10-fold cross validation during the execution of
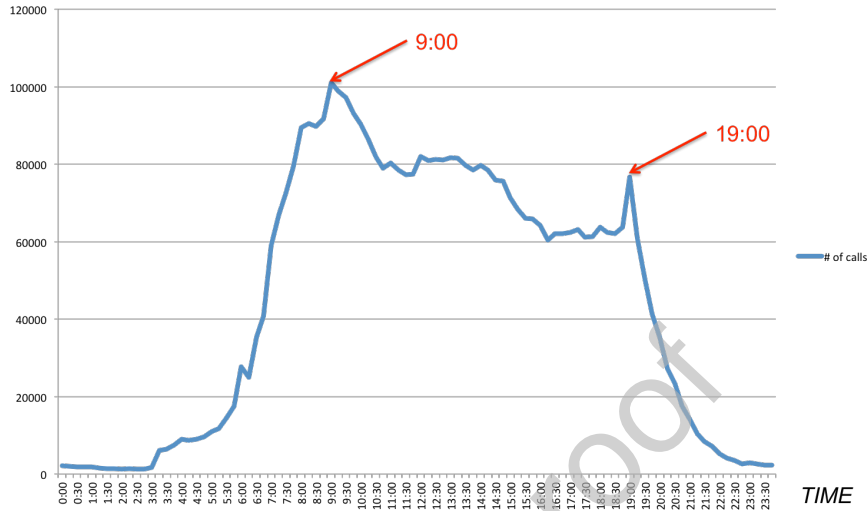
30

Figure 9: Plot with calls per second generated by our workload over a day

our workload with sliding windows of length l. Since each run lasts 120 minutes and the size of the interval in the sliding window is 5 minutes, each workload execution produces $(120 - l)/5$ samples that can be used for prediction. In the evaluation, we first studied the impact of l on the results (RQ1), and then used the best value in our contest for the other experiments.

Overall we collected samples from a total of 648 runs, which include 24 passing executions and 24 failing executions for each type of failure. A failing execution is characterized by a fault of a given type injected in a given resource with a given activation pattern. As discussed in Section 5.4, we injected faults of six different types (packet loss, excessive workload, packet latency, packet corruption, memory leak and cpu hog) following three activation patterns (constant, exponential and random). For all but excessive workload, we injected faults on five different target resources (the Bono, Sprout, and Homestead virtual machines in Clearwater and two compute nodes in OpenStack), resulting in $5 \times 3 \times 5 = 75$ failure cases. For excessive workload, we injected faults with three patterns with no specific target resource, since excessive workload faults target the system and not a specific resource. We thus obtained $75 + 3 = 78$

31

failure cases. To avoid biases due to the fault injection pattern, we repeated every experiment 8 times, thus obtaining 624 failing executions for the evaluation. The extensive investigation of the different fault types, activation patterns, and affected resources made the set of executions available for the experiment unbalanced between passing executions (24 cases) and failing executions (624 cases).

Since we use $l = 90$ for RQ2 and RQ5, we obtained a total of 4,782 samples collected from both passing and failing executions. The number of samples available for RQ1 is higher because we tried different values for l. To apply 10-fold cross-validation, we split the set of samples into 10 sets of equals size, using nine of them to learn the prediction model and the remaining set to compute the quality of the model. The *PreMiSE* failure prediction algorithm does not consider the order of the samples in time, since it classifies each sample independently from the others.

We evaluated the quality of a prediction model using the standard measures that are used to define contingency tables and that cover the four possible outcomes of failure prediction (see Table 3). We also measured the following derived metrics:

Precision: the ratio of correctly predicted failures over all predicted failures. This measure can be used to assess the rate of false alarms, and thus the rate of unnecessary reactions that might be triggered by the failure predictor.

Recall: the ratio of correctly predicted failures over actual failures. This measure can be used to assess the percentage of failures that can be predicted with the failure predictor.

F-Measure: the uniformly weighted harmonic mean of precision and recall. This measure captures with a single number the tradeoff between precision and recall.

Accuracy: the ratio of correct predictions over the total number of predictions.

The accuracy provides a quantitative measure of the capability to predict both failures and correct executions.

FPR (False Positive Rate): the ratio of incorrectly predicted failures to the number of all correct executions. The FPR provides a measure of the false warning frequency.

Table 4 summarizes the derived metrics that we used by presenting their mathematical formulas and meanings.

Table 3: Contingency table

		Predicted	
		Failure	Not-Failure
Actual	Failure	True Positive (TP) *(correct warning)*	False Negative (FN) *(missed warning)*
	Not-failure	False Positive (FP) *(false warning)*	True Negative (TN) *(correct no-warning)*

We addressed the research question RQ3 by computing the *percentage of samples that* PreMiSE *correctly classifies as failure-free* given a set of samples collected by running workflows that differ significantly from the workflow used during the training phase. To this end, we designed two new workflows: *random40* and *random100*. The *random40* workflow behaves like the training workflow with a uniformly random deviation between 0% to 40%, while the *random100* workflow behaves with a deviation of up to 100%.

We addressed the research question RQ4 by computing *the time needed to generate a prediction* and *the time between a failure prediction and its occurrence* from a total of 18 faulty runs lasting up to twelve hours. The former time measures the capability of *PreMiSE* to identify and report erroneous behaviors. The latter time estimates how early *PreMiSE* can predict failure occurrences. As shown in Figure 10, we define four specific measures:

Time-To-General-Prediction ($TTGP$): the distance between the time a

33

Table 4: Selected metrics obtained from the contingency table

Metric	Formula	Meaning
Precision	$\frac{TP}{(TP+FP)}$	How many predicted failures are actual failures?
Recall	$\frac{TP}{(TP+FN)}$	How many actual failures are correctly predicted as failures?
F-measure	$2 * \frac{(Precision*Recall)}{(Precision+Recall)}$	Harmonic mean of $Precision$ and $Recall$
Accuracy	$\frac{(TP+TN)}{(TP+TN+FP+FN)}$	How many predictions are correct?
FPR	$\frac{(FP)}{(TN+FP)}$	How many correct executions are predicted as failures?

fault is active for the first time and the time *PreMiSE* produces a general prediction,

Time-To-Failure-Specific-Prediction (*TTFSP*): the distance between the time a fault is active for the first time and the time *PreMiSE* predicts a specific failure type,

Time-To-Failure for General Prediction (*TTF(GP)*): the distance between the time *PreMiSE* predicts a general failure and the time the failure happens,

Time-To-Failure for Failure-Specific Prediction (*TTF(FSP)*): the distance between the time *PreMiSE* predicts a specific failure type and the time the system fails,
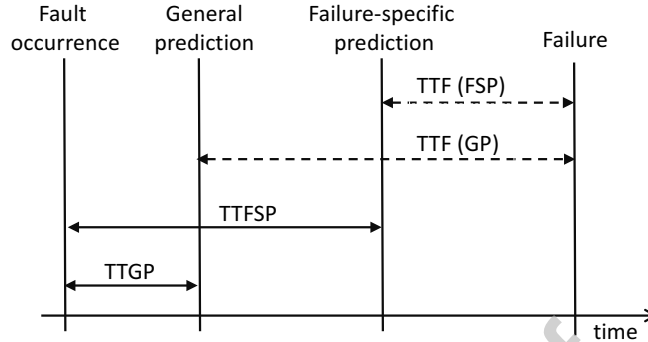
34

Figure 10: Prediction time measures

where the *Fault occurrence* is the time the seeded fault becomes active in the system, the *General prediction* is the first time *PreMiSE* signals the presence of a failure without indicating the fault yet, that is, it identifies an anomaly with an empty fault and resource, the *Failure-specific prediction* is the first time *PreMiSE* indicates also the fault type and the faulty resource, the *Failure* is the time the delivered service deviated from the system function. Failures depend on the seeded faults. In our case, failures manifest either as system crashes or as success rate dropping below 60%, as indicated in Section 6 when discussing RQ4.

To answer RQ6, we measured the resource consumption as (i) the percentage of *CPU* used by the monitoring activities, (ii) the amount of *memory* used by the monitoring activities, (iii) the amount of *bytes read/written* per second by the monitoring activities, and (iv) the packets received/sent per second over the *network* interfaces by the monitoring activities.

6. Experimental Results

In this section we discuss the results of the experiments that we executed to answer the research questions that we introduced in the former section.

RQ1: Sliding window size

PreMiSE builds the prediction models and analyses anomalies referring to time sliding windows of fixed size. The sliding windows should be big enough to
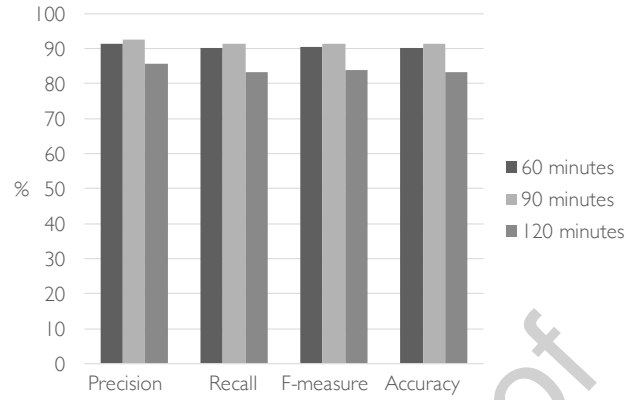
Figure 11: Average effectiveness of failure prediction approaches with different sliding window sizes
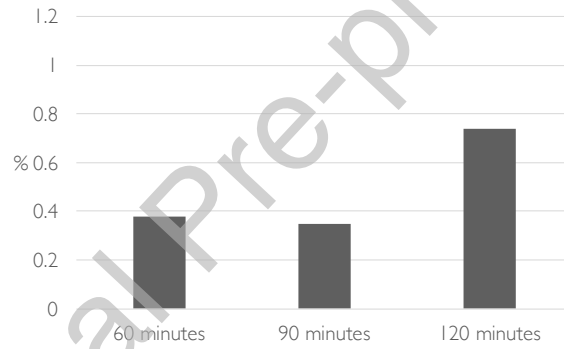
Figure 12: Average false positive rate for different sliding window sizes

Table 5: Comparative evaluation of the effectiveness of *PreMiSE* prediction and localization with the different algorithms for generating signatures

Model	Precision	Recall	F-measure	Accuracy	FPR
BN	84.906	82.438	82.430	82.438	0.685
BFDT	97.746	97.719	97.726	97.719	0.093
NB	83.931	80.925	80.786	80.925	0.745
SVM	98.632	98.632	98.632	98.632	0.057
DT	92.650	88.555	89.943	88.555	0.470
LMT	98.798	98.797	98.797	98.797	0.050
HNB	92.307	91.831	91.765	91.831	0.325

contain a sufficient amount of information to predict failures and small enough to be practical and sensitive to failure symptoms.

775　　With this first set of experiments, we investigate the impact of the window size on the effectiveness of the prediction. We experimented with the seven algorithms described in Section 5.3, each with sliding windows of size 60, 90 and 120 minutes to study the impact of the window size, and to chose the size for the next experiments. We built a total of 27 prediction models. We

780　executed the prototype tool with the different prediction models both with and without seeded faults, for a total of 24 execution for 27 configurations, 26 of which corresponding to configurations each seeded with a different fault, and one no-faulty configuration, for a total of 648 executions. The configurations correspond to the raw of Table 6 that we discuss later in this section.

785　　Figure 11 compares the average precision, recall, F-measure and accuracy over all the experiments. These results indicate that the window size has a moderate impact on the predictions, and that a window size of 90 minutes reaches the best prediction effectiveness among the experimented sizes. Figure 12 shows the average false positive rates for the different window sizes, and confirms the

790　choice of a window of 90 minutes as the optimal choice among the evaluated sizes. The results collected for the individual algorithms are consistent with the average ones. In all the remaining experiments, we use 90-minutes windows.

RQ2: Predicting Failures and locating faults

　　We evaluated the effectiveness of *PreMiSE* as the ability of predicting in-
795　coming failures and identifying the kind and location of the related faults.

　　Table 5 shows the precision, recall, F-measure, accuracy and False Positive Rate (FPR) of failure prediction and fault localization for *PreMiSE* with the prediction algorithms presented at the end of Section 5.3. The table indicates that *PreMiSE* performs well with all the algorithms, with slightly better
800　indicators for *LMTs (Logistic Model Trees)* that we select for the remaining experiments.

　　Table 6 shows the effectiveness of *PreMiSE* with LMT for the different fault

37

types and locations. The metrics were calculated on a window basis as you need to make a forecast about each window. This means that windows that belong

₈₀₅ to both failed and correct executions are taken into account. The results in the table indicate that the approach is extremely accurate: *PreMiSE* suffered from only 74 false predictions out of 4,782 window samples. *PreMiSE* can quickly complete the offline training phase. To learn the *baseline model*, the data collected from two weeks of execution required less than 90 minutes of

₈₁₀ processing time. When the training phase runs in parallel to the data collection process, it completes almost immediately after the data collection process has finished. The *signature model extractor* has taken less than 15 minutes to be learnt using the anomalies from two weeks.

RQ3: Detecting Legal Executions

₈₁₅ While the workload conditions do not alter the failure detection and fault localization capabilities, they may impact on the false positive rate in the absence of faults. Thus experimented with different types of workloads in the absence of faults: workload *random40* that differs from the workload used in the training phase for 40% of the cases, and *random100* that differs completely from the

₈₂₀ workload used in the training phase.

We generated 72 samples for *random40* and *random100* by running each workload for 2 hours, producing a total of 144 samples. *PreMiSE* has been able to correctly classify all the samples as belonging to failure-free executions. Jointly with the results discussed for RQ2, we can say that *PreMiSE* shows a

₈₂₅ very low number of false positives, even if we are analyzing data from normal executions with workloads completely different from those used in the training phase.

RQ4: Prediction Earliness

We evaluated the earliness of the prediction as the Time-To-General-Prediction

₈₃₀ (*TTGP*), the Time-To-Failure-Specific-Prediction (*TTFSP*), the Time-To-Failure for General Prediction (*TTF(GP)*) and the Time-To-Failure for Failure-Specific

Table 6: Effectiveness of the LogicModel tree (LMT) failure prediction algorithm for fault type and location

Fault type (Location)	Precision	Recall	F-Measure	Accuracy	FPR
CPU hog (Bono)	100%	93.529%	96.657%	0.998%	0%
CPU hog (Sprout)	100%	97.059%	98.507%	0.999%	0%
CPU hog (Homestead)	100%	97.041%	98.498%	0.999%	0%
CPU hog (Compute #5)	93.820%	98.817%	96.254%	0.997%	0.236%
CPU hog (Compute #7)	96.875%	91.716%	94.225%	0.996%	0.107%
Excessive workload	100%	100%	100%	1.000%	0%
Memory leak (Bono)	100%	98.810%	99.401%	1.000%	0%
Memory leak (Sprout)	100%	95.833%	97.872%	0.999%	0%
Memory leak (Homestead)	100%	96.429%	98.182%	0.999%	0%
Memory leak (Compute #5)	76.119%	91.071%	82.927%	0.987%	1.031%
Memory leak (Compute #7)	93.333%	75.000%	83.168%	0.989%	0.193%
Packet corruption (Bono)	85.973%	99.476%	92.233%	0.993%	0.669%
Packet corruption (Sprout)	87.558%	99.476%	93.137%	0.994%	0.583%
Packet corruption (Homestead)	99.429%	91.579%	95.342%	0.996%	0.022%
Packet corruption (Compute #5)	100%	100%	100%	1.000%	0%
Packet corruption (Compute #7)	100%	100%	100%	1.000%	0%
Packet latency (Bono)	96.000%	100%	97.959%	0.998%	0.173%
Packet latency (Sprout)	76.777%	84.375%	80.397%	0.984%	1.058%
Packet latency (Homestead)	72.028%	53.646%	61.493%	0.973%	0.864%
Packet latency (Compute #5)	82.857%	75.521%	79.019%	0.984%	0.648%
Packet latency (Compute #7)	62.069%	75.000%	67.925%	0.972%	1.900%
Packet loss (Bono)	100%	73.837%	84.950%	0.991%	0%
Packet loss (Sprout)	99.429%	100%	99.713%	1.000%	0.022%
Packet loss (Homestead)	94.152%	95.833%	94.985%	0.996%	0.215%
Packet loss (Compute #5)	100%	100%	100%	1.000%	0%
Packet loss (Compute #7)	82.266%	99.405%	90.027%	0.992%	0.773%
Correct execution	100%	100%	100%	1.000%	0%

Prediction (*TTF(FSP)*) illustrated in Figure 10.

In the experiments, failures correspond to either system crashes or drops in the successful SIP call rate below 60% for 5 consecutive minutes. Table 7 reports the results of the experiment. The columns *from fault occurrence to failure prediction* show the time that *PreMiSE* needed to predict a general (TTGP) and specific (TTFSP) failure, respectively. *PreMiSE* has been able to produce a general failure prediction in some minutes: 5 minutes in the best case, less than 31 minutes for most of the faults, and 65 minutes in the worst case. Moreover, *PreMiSE* has generated the failure specific prediction few minutes after the general prediction, with a worst case of 35 minutes from the general to the specific prediction. The readers should notice that we measure the time to prediction starting with the first activation of the seeded fault, which may not immediately lead to faulty symptoms.

The columns *From failure prediction to failure* indicate that the failures are predicted well in advance, leaving time for a manual resolution of the problem. *PreMiSE* has detected both the general and failure specific predictions at least 48 minutes before the failure, which is usually sufficient for a manual intervention. These results are also valuable for the deployment of self-healing routines, which might be activated well in advance with respect to failures.

PreMiSE predicts failure based on the analysis of *OA-PI*, which works with sampling intervals of 5 minutes. Indeed *PreMiSE* can effectively predict a failure with few anomalous samples. It could predict failures in a shorter time than 5 minutes with an anomaly detector that requires smaller sampling intervals.

Faults of different type have very different impacts on the system, and can thus result in largely different patterns. Figure 13 exemplifies the different impact of faults of various types by plotting the percentage of successful calls in the experiments characterized by the longest and shortest Time-to-Failure, which correspond to CPU hog and packet corruption faults, respectively. Packet corruption faults have a gradual impact on the system, while the CPU hog faults do not cause failures in the first three hours of execution for the reported experiment.
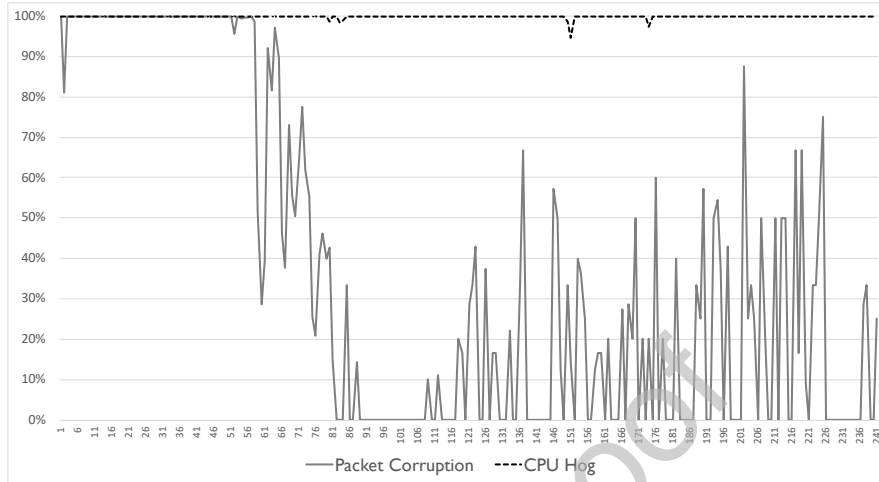
40

Figure 13: Call success rate over time

Overall, *PreMiSE* demonstrated to be able to effectively predict failures, including their type well in advance to the failure time for the four classes of problems that have been investigated.

RQ5: Comparative Evaluation

We compare *PreMiSE* to both *OA-PI* and *G-BDA* on the same testbed. *OA-PI* is a widely adopted industrial anomaly-based tool, *G-BDA* is a state-of-the-art signature-based approach. We use *OA-PI* as a baseline approach, and *G-BDA* as a relevant representative of competing approaches. Table 8 reports precision, recall, F-Measure, accuracy and false positive rate of *PreMiSE* , OA-PI and G-BDA.

OA-PI infers the threshold of normal performance for KPI values, and raises alarms only for persistent anomalies, that is, if the probability that a KPI is anomalous for 3 of the last 6 intervals is above a certain threshold value [45]. Columns *OA-PI (anomalies)* and *OA-PI (alarms)* of Table 8 report all and the persistent anomalies that OA-PI detects and signal, respectively. In both cases OA-PI is less effective than *PreMiSE*: OA-PI does not raise any alarm, thus failing to predict the failure (recall = 0%, precision and F-measure not

41

Table 7: *PreMiSE* prediction earliness for fault type and pattern

Fault Type (Pattern)	From fault occurrence to failure prediction		From failure prediction to failure	
	TTGP	TTFSP	TTF (GP)	TTF (FSP)
CPU hog (Random)	65 mins	80 mins	>12 hours	>12 hours
CPU hog (Constant)	45 mins	60 mins	>12 hours	>12 hours
CPU hog (Exponential)	5 mins	30 mins	>12 hours	>12 hours
Excessive workload (Random)	35 mins	50 mins	192 mins	177 mins
Excessive workload (Constant)	40 mins	55 mins	110 mins	95 mins
Excessive workload (Exponential)	30 mins	45 mins	80 mins	65 mins
Memory leak (Random)	5 mins	20 mins	55 mins	40 mins
Memory leak (Constant)	5 mins	20 mins	56 mins	41 mins
Memory leak (Exponential)	5 mins	20 mins	56 mins	41 mins
Packet corruption (Random)	30 mins	60 mins	121 mins	91 mins
Packet corruption (Constant)	30 mins	60 mins	172 mins	148 mins
Packet corruption (Exponential)	30 mins	55 mins	48 mins	23 mins
Packet latency (Random)	45 mins	70 mins	132 mins	107 mins
Packet latency (Constant)	30 mins	60 mins	132 mins	102 mins
Packet latency (Exponential)	45 mins	60 mins	59 mins	44 mins
Packet loss (Random)	50 mins	65 mins	142 mins	127 mins
Packet loss (Constant)	30 mins	65 mins	85 mins	50 mins
Packet loss (Exponential)	50 mins42	65 mins	52 mins	37 mins

>12 hours indicates the cases of failures that have not been observed within 12 hours,

although in the presence of active faults that would eventually lead to the system failures.

Table 8: Comparative evaluation of *PreMiSE* and state-of-art approches

Measures	*PreMiSE*	OA-PI (alarms)	OA-PI (anomalies)	G-BDA (single-tier)	G-BDA (multi-tier)
Precision	98.798%	–	94.118%	90.967%	87.933%
Recall	98.797%	0%	100%	90.567%	87.533%
F-Measure	98.797%	–	96.970%	90.367%	87.400%
Accuracy	98.797%	5.882%	94.118%	90.567%	87.533%
FPR	0.05%	0%	100%	2.833%	2.3%

computable), and records far too many anomalies, thus signalling all potential failures (recall of 100%) diluted in myriads false alarms (false positive rate = 100%). In a nutshell, OA-PI reports every legal executions as a possible failure. *PreMiSE* is effective: The high values of the five measures indicate that *PreMiSE* predicts most failures with a negligible amount of false positives.

G-BDA is a signature-based approach that collects VM metrics to detect preliminary symptoms of failures. G-BDA detects both excessive workload and anomalous virtual machines. G-BDA analyzes a single tier of a distributed system. Columns *G-BDA (single-tier)* and *G-BDA (multi-tier)* of Table 8 report precision, recall, F-measure, accuracy and FPR of G-BDA, by referring to the analysis of faults injected in a single VM and faults injected in different tiers, respectively. In both cases *PreMiSE* outperforms G-BDA on all five measures, and reduces FPR from over 2% to 0.05%.

In summary, the *PreMiSE* combination of anomaly detection and signature-based analysis is more effective than either of the two techniques used in isolation.

RQ6: Overhead

PreMiSE interacts directly with the system only with the *KPI Monitor*, which in our prototype implementation collects the KPIs by means of the SN-MPv2c monitoring service for Clearwater [25], the Ceilometer telemetry service for OpenStack [26] and a Linux OS agent that we implemented for Ubuntu. All other computation is performed on a dedicated node, and does not impact on

43

the overall performance of the target system. Thus, the *PreMiSE* overhead on the running system is limited to the overhead of the monitoring services that we expect to be very low.
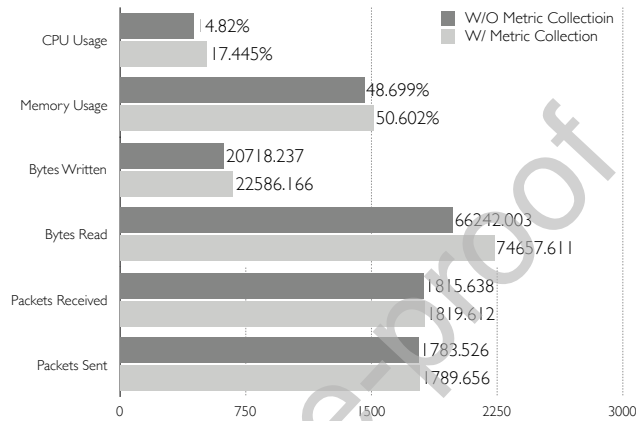

Figure 14: *PreMiSE* overhead

The experimental results confirm the absence of overhead, which means no measurable difference, on the target system. We only observe small differences in resource consumption as reported in Figure 14, which reports cpu, memory, disk and network consumption when the system is executed with and without the monitoring infrastructure. The monitoring infrastructure has a negligible impact on disk (measured as read and written bytes) and network (measured as number of sent and received packets) usage, accounting for few hundreds bytes over tens of thousands and few packets over thousands, respectively. The impact on CPU and memory usage is also quite low, with an average increase of 2.63% and 1.91%, respectively. These results are perfectly compatible with systems with strong performance requirements, such as telecommunication infrastructures.

44

Threats To Validity

In this article, we reported our experience with an IMS in a network function virtualization environment. Although we have achieved success predictors under different runtime conditions, this may not generalize to other cloud systems. While the approach is generalised easily, it cannot be assumed in advance that the results of a study will generalise beyond the specific environment in which it was conducted. This is an external threat to the validity. One way to mitigate this threat is to analyze other real-world cloud systems. However, there is no publicly available benchmark from realistic cloud deployments such as Project Clearwater. To overcome this limitation, we are partnering with industrial companies to test PreMiSE in their pre-production systems.

An internal threat to validity is the limited number of faults we examined in the study. We chose popular faults without apriori knowledge of their behavior. However, it is possible that there are faults that do not exhibit any performance deviations. To mitigate the threat mentioned above, we plan to extend the study with a larger set of experiments, so that statistical significant test can be meaningfully applicable.

7. Related Work

State-of-the-art techniques for predicting failures and locating the corresponding faults are designed to support system administrators, enable self-healing solutions or dealing with performance issues [46, 47]. Current techniques to predict system failures derive abstractions of the behavior of a system in the form of models and rules, and exploit either *signature-* or *anomaly-based* strategies to dynamically reveal symptoms of problems, and predict related failures.

Signature-based approaches capture failure-prone behaviors that indicate how the monitored system behaves when affected by specific faults, and aim to reveal faults of the same kinds at runtime. *Anomaly-based approaches* capture non-failure-prone behaviors that represent the correct behavior of the monitored system and aim to reveal behaviors that violate these abstractions at

runtime. *Performance-related approaches* dynamically identify anomalies and bottlenecks.

Signature-based approaches can accurately predict the occurrences of failures whose symptoms are encoded in the models that capture the fault signatures,
₉₅₀ but are ineffective against failures that do not correspond to signatures encoded in the models. Anomaly-based approaches can potentially predict any failure, since they reveal violations of models of the positive behaviors of the application, but depend on the completeness of the models, and suffer from many false alarms. In a nutshell, *signature-based approaches may miss several failures while*
₉₅₅ *anomaly-based approaches may generate many false alarms.*

PreMiSE integrates anomaly- and signature-based approaches to benefit from both the generality of anomaly-based techniques and the accuracy of signature-based techniques. While current signature-based approaches derive failure signatures from application events [23, 14, 16], the original *PreMiSE* ap-
₉₆₀ proach derives failure signatures from anomalies that are good representative of failure-prone behaviors, and thus particularly effective in predicting failures.

Performance-related approaches address performance problems by detecting anomalies and bottlenecks that do not affect the functional behavior of the system, and as such are largely complementary to *PreMiSE* and related
₉₆₅ approaches.

7.1. Signature-Based Approaches

The main signature-based approaches are the Vilalta et al.'s approach [23], hPrefects [14], SEIP [16], Seer [15], Sauvanaud et al. [18], SunCat [10] and the approach defined by Malik et al. [11].

₉₇₀ Vilalta et al. introduced an approach that mines failure reports to learn associative rules that relate events that frequently occur prior to system failures to the failures themselves, and use the mined rules to predict failures at runtime, before their occurrence [23]. Fu and Zu's *hPrefects* approach extends Vilalta et al.'s rules to clustered architectures [14]. *hPrefects* learns how failures propagate
₉₇₅ in time and space from failure records, represents temporal correlations with a

spherical covariance model, and spatial correlations with stochastic models, and includes a cluster-wide failure predictor that uses the learned models to estimate the probability that a failure occurs in the current execution.

Salfner et al.'s *SEIP* approach synthesizes a semi-Markov chain model that includes information about error frequency and error patterns [16], and signals a possible system failure, when the model indicates that the probability that the current execution will produce a failure exceeds a given threshold.

Ozchelik and Yilmaz's *Seer* technique combines hardware and software monitoring to reduce the runtime overhead, which is particularly important in telecommunication systems [15]. *Seers* trains a set of classifiers by labeling the monitored data, such as caller-callee information and number of machine instructions executed in a function call, as passing or failing executions, and uses the classifiers to identify the signatures of incoming failures.

Sauvanaud et al. capture symptoms of service level agreement violations: They collect application-agnostic data, and classify system behaviors as normal and anomalous with a Random Forest algorithm, and show that collecting data from an architectural tier impacts on the accuracy of the predictions [18].

Nistor and Ravindranath's *SunCat* approach predicts performance problems in smartphone applications by identifying calling patterns of string getters that may cause performance problems for large inputs, by analyzing similar calling patterns for small inputs [10].

Malik et al. [11] developed an automated approach to detect performance deviations before they become critical problems. The approach collects performance counter variables, extracts performance signatures, and then uses signatures to predict deviations. Malik et al. built signatures with a supervised and three unsupervised approaches, and provide experimental evidence that the supervised approach is more accurate than the unsupervised ones even with small and manageable subsets of performance counters.

Lin et al.'s [48] *MING* technique uses an ensemble of supervised machine learning models to predict failures in cloud systems by analyzing both temporal and spatial data. Compared to PreMiSe, MING does not consider the multi-

47

level nature of cloud systems and can predict failures only at the granularity of the host.

El-Sayed et al. [49] note that unsuccessful jobs across different clusters exhibit patterns that distinguish them from successful executions. On the basis of this observation, they use random forests to identify signatures of unsuccessful terminations of jobs or tasks running in the cluster. Predictions at the job level are then used to mitigate the effect of unsuccessful job executions.

PreMiSE introduces several novel features that improve over current signature-based approaches: (i) it creates signatures from anomalies, which better represent failure occurrences than general events, (ii) predicts the type of failure that will occur, (iii) integrates and correlates data extracted from all layers and components of a multi-tier distributed architecture, and (iv) restricts the scope of the location of the causing faults.

7.2. Anomaly-Based Approaches

The main anomaly-based approaches are the algorithms proposed by Fulp et al. [50], Jin et al. [12] and Guan et al. [19], and the *Tiresias* [13], *ALERT* [20], *PREPARE* [21] and *OA-PI* [22] technologies.

Fulp et al.'s approach and *PREPARE* address specific classes of failures. Fulp et al. defined a spectrum-kernel support vector machine approach to predict disk failures using system log files [50], while *PREPARE* addresses performance anomalies in virtualized systems [21]. Fulp et al. exploit the sequential nature of system messages, the message types and the message tags, to distill features, and use support vector machine models to identify message sequences that deviate from the identified features as symptoms of incoming failures. *PREPARE* combines a 2-dependent Markov model to predict attribute values with a tree-augmented Bayesian network to predict anomalies. Differently from both thees approaches that are specific to some classes of failures, *PreMiSE* is general and can predict multiple types of failures simultaneously.

Guan et al. proposed an ensemble of Bayesian Network models to characterize the normal execution states of a cloud system [19], and to signal incoming

48

failures when detecting states not encoded in the models. *ALERT* introduces the notion of alert states, and exploits a triple-state multi-variant stream classification scheme to capture special alert states and generate warnings about ₁₀₄₀ incoming failures [20]. *Tiresias* integrates anomaly detection and Dispersion Frame Technique (DFT) to predict anomalies [13].

Jin et al. use benchmarking and production system monitoring to build an analytic model of the system that can then be used to predict the performance of a legacy system under different conditions to avoid unsatisfactory service levels ₁₀₄₅ due to load increases [12].

Anomaly-based approaches are inevitably affected by the risk of generating many false positives as soon as novel legal behaviors emerge in the monitored system. *PreMiSE* overcomes the issue of false positives by integrating an anomaly detection approach with a signature-based technique that issues ₁₀₅₀ alarms only when the failure evidence is precise enough. The results reported in Section 6 show that *PreMiSE* dramatically improves over current anomaly-based detection techniques, including modern industrial-level solutions such as IBM *OA-PI* [22].

7.3. Performance-Related Approaches

₁₀₅₅ Performance anomaly detection approaches predict performance issues and identify bottlenecks in production systems, while performance regression approaches detect performance changes [46].

Classic performance anomaly detection approaches work with historical data: they build statistical models of low-level system metrics to detect performance ₁₀₆₀ issues of distributed applications [51, 52, 53, 54]. They derive formal representations, called signatures, that are easy to compute and retrieve, to capture the state of the system, and quickly identify similar performance issues that occurred in the past. These approaches aim to discriminate different types of performance issues in order to aid root cause analysis.

₁₀₆₅ The most recent performance anomaly detectors, BARCA, Root and TaskInsight, do not need historical data. BARCA monitors system metrics, computes

49

performance indicators, like mean, standard deviation, skewness and kurtosis, and combines SVMs, to detects anomalies, with multi-class classifier analysis, to identify related anomalous behaviors, like deadlock, livelock, unwanted syn-
₁₀₇₀ chronization, and memory leaks [55]. Root works as a Platform-as-a-Service (PaaS) extension [56]. It detect performance anomalies in the application tier, classifies their cause as either workload change or internal bottleneck, and locates the most likely causes of internal bottlenecks with weighted algorithms. TaskInsight detects performance anomalies in cloud applications, by analysing
₁₀₇₅ system level metrics, such as CPU and memory utilization, with a clustering algorithm, to identify abnormal application threads[57]. It detects and identifies abnormal application threads by analyzing system level metrics such as CPU and memory utilization.

Differently from *PreMiSE*, these approaches (i) do not locate the faulty re-
₁₀₈₀ source that causes the performance anomaly, and (ii) cannot detect performance problems at different tiers, which remains largely an open challenge [46].

Performance regression approaches detect changes in software system performance during development aiming to prevent performance degradation in the production system [58]. They reveal changes in the overall performance of
₁₀₈₅ the development system due to changes in the code. Ghaith et al. [59] detect performance regression by comparing transaction profiles to reveal performance anomalies that can occur only if the application changes. Transaction profiles reflects the lower bound of the response time in a transaction under idle condition, and do not depend on the workload. Foo et al. [60] detect performance
₁₀₉₀ regressions in heterogeneous environments in the context of data centers, by building an ensemble of models to detect performance deviations. Foo et al. aggregate performance deviations from different models, by using simple voting as well as weighted algorithms to determine whether the current behavior really deviate from the expected one, and is not a simple environment-specific vari-
₁₀₉₅ ation. Performance regression approaches assume a variable system code base and a stable runtime environment, while *PreMiSE* collects operational data to

50

predict failures and localize faults caused by a variable production environment in an otherwise stable system code base.

8. Conclusions

In this paper, we presented *PreMiSE*, an original approach to automatically predict failures and locate the corresponding faults in multi-tier distributed systems, where faults are becoming the norm rather then the exception. Predicting failure occurrence as well as locating the responsible faults produce information that is essential for mitigating the impact of failures and improving the dependability of the systems. Current failure prediction approaches rarely produce enough information to locate the faults corresponding to the predicted failures, and either suffer from false positives (anomaly-based) or work with patterns of discrete events and do not cope well with failures that impact on continuous indicators (signature-based).

PreMiSE originally blends anomaly- and signature-based techniques to address failures that impact on continuous indicators, and to precisely locate the corresponding faults. It uses data time series analysis and Granger causality tests to accurately reveal anomalies in the behavior of the system as a whole, probabilistic classifiers to distill signatures that can distinguish failure-free albeit anomalous behaviors from failure-prone executions, and signature-based techniques to accurately distinguish malign from benign anomalies, predict the type of the incoming failures, and locate the sources of the incoming failures. *PreMiSE* executes on a node independent from the target system, and limits the online interactions with the monitored applications to metric collection.

In this paper, we report the results of experiments executed on the implementation of a Clearwater IP Multimedia Subsystem, which is a system commonly adopted by telecommunication companies for their VOIP (voice over IP), video and message services. The results confirm that *PreMiSE* can predict failures and locate faults with higher precision and less false positives than state of the approaches, without incurring in extra execution costs on the target system.

51

Differently from state-of-the-art approaches, *PreMiSE* can effectively identify the type of the possible failure and locate the related faults for the kinds of faults and failures used in the training phase.

We designed and studied *PreMiSE* in the context of multi-tier distributed ₁₁₃₀ systems, to predict failures and locate faults at the level of individual tier of the nodes of the system. Studying the *PreMiSE* approach in the context of other systems that can be extensively monitored is a promising research direction.

9. Acknowledgements

References

₁₁₄₀ [1] P. Feiler, R. P. Gabriel, J. Goodenough, R. Linger, T. Longstaff, R. Kazman, M. Klein, L. Northrop, D. Schmidt, K. Sullivan, et al., Ultra-large-scale systems: The software challenge of the future, Software Engineering Institute 1.

[2] I. Sommerville, D. Cliff, R. Calinescu, J. Keen, T. Kelly, M. Kwiatkowska, ₁₁₄₅ J. Mcdermid, R. Paige, Large-scale complex it systems, Commun. ACM 55 (7) (2012) 71–77. doi:10.1145/2209249.2209268.
URL http://doi.acm.org/10.1145/2209249.2209268

[3] C. B. Nielsen, P. G. Larsen, J. Fitzgerald, J. Woodcock, J. Peleska, Systems of systems engineering: basic concepts, model-based techniques, and ₁₁₅₀ research directions, ACM Computing Surveys 48 (2) (2015) 18.

[4] C. Xin, L. Charng-Da, P. Karthik, Failure analysis of jobs in compute clouds: A google cluster case study, in: Proceedings of the International

Symposium on Software Reliability Engineering, ISSRE '14, IEEE Computer Society, 2014, pp. 167–177.

[5] K. Ryan K.l., L. Stephen S.G., R. Veerappa, Understanding cloud failures, IEEE Spectrum 49 (12) (2012) 84–84.

[6] K. V. Vishwanath, N. Nagappan, Characterizing cloud computing hardware reliability, in: Proceedings of the Annual Symposium on Cloud Computing, SoCC '10, ACM, 2010, pp. 193–204.

[7] European Telecommunications Standards Institute, Network Functions Virtualisation, `http://www.etsi.org/technologies-clusters/technologies/nfv`, last access: May 2015.

[8] E. Bauer, R. Adams, Reliability and Availability of Cloud Computing, Wiley, 2012.

[9] O. Riganelli, R. Grosu, S. R. Das, C. R. Ramakrishnan, S. A. Smolka, Power optimization in fault-tolerant mobile ad hoc networks, in: Proceedings of IEEE High Assurance Systems Engineering Symposium, HASE08, IEEE Computer Society, 2008, pp. 362–370.

[10] A. Nistor, L. Ravindranath, Suncat: Helping developers understand and predict performance problems in smartphone applications, in: Proceedings of the International Symposium on Software Testing and Analysis, ISSTA '14, ACM, 2014, pp. 282–292.

[11] H. Malik, H. Hemmati, A. E. Hassan, Automatic detection of performance deviations in the load testing of Large Scale Systems, in: Proceedings of the International Conference on Software Engineering, ICSE '13, IEEE Computer Society, 2013, pp. 1012–1021.

[12] Y. Jin, A. Tang, J. Han, Y. Liu, Performance evaluation and prediction for legacy information systems, in: Proceedings of the International Conference on Software Engineering, ICSE '07, IEEE Computer Society, 2007, pp. 540–549.

53

[13] A. W. Williams, S. M. Pertet, P. Narasimhan, Tiresias: Black-box failure prediction in distributed systems, in: Proceedings of the International Parallel and Distributed Processing Symposium, IPDPS '07, IEEE Computer Society, 2007, pp. 1–8.

[14] S. Fu, C.-Z. Xu, Exploring event correlation for failure prediction in coalitions of clusters, in: Proceedings of the Annual International Conference on Supercomputing, SC '07, IEEE Computer Society, 2007, pp. 1–12.

[15] B. Ozcelik, C. Yilmaz, Seer: A Lightweight Online Failure Prediction Approach, IEEE Transactions on Software Engineering 42 (1) (2016) 26–46.

[16] F. Salfner, M. Schieschke, M. Malek, Predicting failures of computer systems: A case study for a telecommunication system, in: Proceedings of the International Parallel and Distributed Processing Symposium, IPDPS '06, IEEE Computer Society, 2006, pp. 8–pp.

[17] M. Haran, A. Karr, A. Orso, A. Porter, A. Sanil, Applying Classification Techniques to Remotely-collected Program Execution Data, in: Proceedings of the ACM SIGSOFT International Symposium on Foundations of Software Engineering, FSE '05, ACM, 2015, pp. 146–155.

[18] C. Sauvanaud, K. Lazri, M. Kaaniche, K. Kanoun, Anomaly detection and root cause localization in virtual network functions, in: Proceedings of the International Symposium on Software Reliability Engineering, ISSRE '16, IEEE Computer Society, 2016.

[19] G. Qiang, Z. Ziming, F. Song, Ensemble of bayesian predictors for autonomic failure management in cloud computing, in: Proceedings of the International Conference on Computer Communications and Networks, ICCCN '10, IEEE Computer Society, 2010, pp. 1–6.

[20] Y. Tan, X. Gu, H. Wang, Adaptive system anomaly prediction for large-scale hosting infrastructures, in: Proceedings of the Symposium on Principles of Distributed Computing, PODC '12, ACM, 2010, pp. 173–182.

54

[21] T. Yongmin, N. Hiep, S. Zhiming, G. Xiaohui, V. Chitra, R. Deepak, Pre-
pare: Predictive performance anomaly prevention for virtualized cloud sys-
tems, in: Proceedings of the International Conference on Distributed Com-
puting Systems, ICDCS '12, IEEE Computer Society, 2012, pp. 285–294.

[22] IBM Corporation, IBM Operation Analytics - Predictive Insights,
`https://www.ibm.com/support/knowledgecenter/en/SSJQQ3_1.3.3/`
`com.ibm.scapi.doc/kc_welcome-scapi.html`, last access: July 2019.

[23] R. Vilalta, S. Ma, Predicting rare events in temporal domains, in: Pro-
ceedings of the International Conference on Data Mining, ICDM '02, IEEE
Computer Society, 2002, pp. 474–481.

[24] D. J. Dean, H. Nguyen, X. Gu, Ubl: Unsupervised behavior learning for
predicting performance anomalies in virtualized cloud systems, in: Pro-
ceedings of the International Conference on Autonomic Computing, ICAC
'12, IEEE Computer Society, 2012, pp. 191–200.

[25] J. D. Case, K. McCloghrie, S. Rose, M.and Waldbusser, Introduction to
community-based snmpv2, IETF RFC 1901 (January 1996).

[26] The OpenStack Project, Ceilometer, `https://wiki.openstack.org/`
`wiki/Ceilometer`, last access: May 2015.

[27] G. E. P. Box, G. Jenkins, R. Gregory, Time Series Analysis: Forecasting
and Control, Wiley, 2008.

[28] A. Arnold, Y. Liu, N. Abe, Temporal causal modeling with graphical
granger methods, in: Proceedings of the ACM SIGKDD International Con-
ference on Knowledge Discovery and Data Mining, KDD '07, ACM, 2007,
pp. 66–75.

[29] The OpenStack Project, Open source software for creating private and
public clouds, `https://www.openstack.org`, last access: May 2015.

55

[1235] [30] The KVM Project, Kernel based virtual machine, `http://www.linux-kvm.org`, last access: May 2015.

[31] Project Clearwater, IMS in the cloud, `http://www.projectclearwater.org`, last access: May 2015.

[32] University of Waikato, Weka 3: Data mining software in java, `http://www.cs.waikato.ac.nz/ml/weka/`, last access: May 2015.

[33] J. Platt, et al., Fast training of support vector machines using sequential minimal optimization, in: Advances in Kernel Methods: Support Vector Learning, MIT Press, 1998, pp. 185–208.

[34] C. Gregory F., H. Edward, A bayesian method for the induction of probabilistic networks from data, Machine Learning 9 (4) (1992) 309–347.

[35] J. Friedman, T. Hastie, R. Tibshirani, et al., Additive logistic regression: a statistical view of boosting, Annals of Statistics 95 (2) (2000) 337–407.

[36] G. H. John, P. Langley, Estimating continuous distributions in bayesian classifiers, in: Proceedings of the Conference on Uncertainty in Artificial Intelligence, UAI'95, Morgan Kaufmann Publishers, 1995, pp. 338–345.

[37] R. Kohavi, The power of decision tables, in: Proceedings of the European Conference on Machine Learning, ECML'95, Springer, 1995, pp. 174–189.

[38] N. Landwehr, M. Hall, E. Frank, Logistic model trees, Machine Learning 59 (1-2) (2005) 161–205.

[39] H. Zhang, L. Jiang, J. Su, Hidden naive bayes, in: Proceedings of the National Conference on Artificial Intelligence, AAAI'05, AAAI Press, 2005, pp. 919–924.

[40] C. Bennett, Chaos Monkey, `https://github.com/Netflix/SimianArmy/wiki/Chaos-Monkey` (May 2015).

[41] B. Sharma, P. Jayachandran, A. Verma, C. R. Das, Cloudpd: Problem determination and diagnosis in shared dynamic clouds, in: Proceedings of the International Conference on Dependable Systems and Networks, DSN '13, IEEE Computer Society, 2013, pp. 1–12.

[42] A. Blohowiak, A. Basiri, L. Hochstein, C. Rosenthal, A platform for automating chaos experiments, ISSREW '16, 2016, pp. 5–8.

[43] G. Richard, J. Olivier, SIPp, `http://sipp.sourceforge.net`, last access: May 2015.

[44] I. H. Witten, E. Frank, M. A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann Publishers, 2011.

[45] IBM Corporation, Operations Analytics - Predictive Insights 1.3.1 (Tutorial), document Revision R2E2 (2015).

[46] O. Ibidunmoye, F. Hernández-Rodriguez, E. Elmroth, Performance anomaly detection and bottleneck identification, ACM Computer Surveys 48 (1) (2015) 4:1–4:35.

[47] F. Salfner, M. Lenk, M. Malek, A survey of online failure prediction methods, ACM Computing Surveys 42 (3) (2010) 1–42.

[48] Q. Lin, K. Hsieh, Y. Dang, H. Zhang, K. Sui, Y. Xu, J.-G. Lou, C. Li, Y. Wu, R. Yao, M. Chintalapati, D. Zhang, Predicting node failure in cloud service systems, in: Proceedings of the European Software Engineering Conference held jointly with the ACM SIGSOFT International Symposium on Foundations of Software Engineering, ESEC/FSE '18, ACM, 2018, pp. 480–490.

[49] N. El-Sayed, H. Zhu, B. Schroeder, Learning from failure across multiple clusters: A trace-driven approach to understanding, predicting, and mitigating job terminations, in: Proceedings of the International Conference on Distributed Computing Systems, ICDCS'17, 2017, pp. 1333–1344.

57

[50] E. W. Fulp, G. A. Fink, J. N. Haack, Predicting computer system failures using support vector machines., in: Proceedings of the USENIX conference on Analysis of system logs, WASL'08, USENIX Association, 2008, pp. 5–5.

[51] I. Cohen, S. Zhang, M. Goldszmidt, J. Symons, T. Kelly, A. Fox, Capturing, indexing, clustering, and retrieving system history, in: Proceedings of the ACM Symposium on Operating Systems Principles, SOSP '05, ACM, 2005, pp. 105–118.

[52] P. Bodik, M. Goldszmidt, A. Fox, D. B. Woodard, H. Andersen, Fingerprinting the datacenter: Automated classification of performance crises, in: Proceedings of the European Conference on Computer Systems, EuroSys '10, ACM, 2010, pp. 111–124.

[53] M. Lim, J. Lou, H. Zhang, Q. Fu, A. B. J. Teoh, Q. Lin, R. Ding, D. Zhang, Identifying recurrent and unknown performance issues, in: Proceedings of the International Conference on Data Mining, ICDM '14, 2014, pp. 320–329.

[54] S. He, Q. Lin, J.-G. Lou, H. Zhang, M. R. Lyu, D. Zhang, Identifying impactful service system problems via log analysis, in: Proceedings of the 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2018, ACM, pp. 60–70.

[55] J. A. Cid-Fuentes, C. Szabo, K. Falkner, Adaptive performance anomaly detection in distributed systems using online svms, IEEE Transactions on Dependable and Secure Computing (Early Access).

[56] H. Jayathilaka, C. Krintz, R. M. Wolski, Detecting performance anomalies in cloud platform applications, IEEE Transactions on Cloud Computing (Early Access).

[57] X. Zhang, F. Meng, P. Chen, J. Xu, Taskinsight: A fine-grained performance anomaly detection and problem locating system, in: Proceedings of

1315 the International Conference on Cloud Computing, CLOUD '16, 2016, pp. 917–920.

[58] J. Chen, W. Shang, An exploratory study of performance regression introducing code changes, in: Proceedings of the IEEE International Conference on Software Maintenance and Evolution, IEEE Computer Society, 2017, pp.
1320 341–352.

[59] S. Ghaith, M. Wang, P. Perry, J. Murphy, Profile-based, load-independent anomaly detection and analysis in performance regression testing of software systems, in: Proceedings of the European Conference on Software Maintenance and Reengineering, CSMR '13, 2013.

1325 [60] K. C. Foo, Z. M. Jiang, B. Adams, A. E. Hassan, Y. Zou, P. Flora, An industrial case study on the automated detection of performance regressions in heterogeneous environments, in: Proceedings of the International Conference on Software Engineering, ICSE '15, 2015.

59

Appendix A. KPI List

₁₃₃₀ Metrics used in the experiments grouped by tier.

Linux server

CPU	user cpu utility, system cpu utility, busy cpu utility, wait io cpu utility
Network	bytes received per sec, bytes transmitted per sec
System	context switches per sec, pages swapped in per sec, pages swapped out per sec, pages faults per sec, total num of processes per sec
Virtual Memory	percentage of swapped space used, percentage of memory used, percentage of memory in buffers, percentage of memory cached.
Socket	sockets in use
I/O	device name, avg wait time, avg request queue length, read bytes per sec, write bytes per sec

OpenStack

Compute	existence of instance and instance type, allocated and used RAM in MB, CPU time used, avg CPU utilisation, num of VCPUs, num of read and write requests, avg rate of read and write requests per sec, volume of reads and writes in Byte, avg rate of reads and writes in Byte per sec, num of incoming bytes on a VM network interface, avg rate per sec of incoming bytes on a VM network interface, num of outgoing bytes on a VM network interface, avg rate per sec of outgoing bytes on a VM network interface, num of incoming packets on a VM network interface, avg rate per sec of incoming packets on a VM network interface, num of outgoing packets on a VM network interface, avg rate per sec of outgoing packets on a VM network interface
Network	existence of network, creation requests for this network, update requests for this network, existence of subnet, creation requests for this subnet, update requests for this subnet, existence of port, creation requests for this port, update requests for this port, existence of router, creation requests for this router, update requests for this router, existence of floating ip, creation requests for this floating ip, update requests for this floating ip
Controller	image polling, uploaded image size, num of update on the image, num of upload of the image, num of delete on the image, image is downloaded, image is served out

1335

Clearwater

CPU and Memory	SNMP CPU and memory usage stats
Latency	avg latency, variance, highest call latency, lowest call latency
Incoming Requests	num of incoming requests
Rejected Requests	num of requests rejected due to overload
Queue	avg request queue size, variance, highest queue size, lowest queue
Cx Interface	avg latency, variance, highest latency and lowest latency seen on the Cx interface
Multimedia-Auth Requests	avg latency, variance, highest latency and lowest latency seen on Multimedia-Auth Requests
Server-Assignment Requests	avg latency, variance, highest latency and lowest latency seen on Server-Assignment Requests
User-Authorization Requests	avg latency, variance, highest latency and lowest latency seen on User-Authorization Requests
Location-Information Requests	avg latency, variance, highest latency and lowest latency seen on Location-Information Requests
Sprout	avg latency, variance, highest and lowest latency between Sprout and Homer XDMS
TCP Connections	num of parallel TCP connections

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Leonardo Mariani is a Full Professor at the University of Milano Bicocca. He holds a Ph.D. in Computer Science received from the same university in 2005. His research interests include software engineering, in particular software testing, program analysis, automated debugging, and self-healing and self-repairing systems. He has authored more than 100 papers appeared at top software engineering conferences and journals. He has been awarded with the ERC Consolidator Grant in 2015, an ERC Proof of Concept grant in 2018, and he is currently active in several European and National projects. He is regularly involved in organizing and program committees of major software engineering conferences.

Mauro Pezzé is a professor of software engineering at the Universitádi Milano Bicocca and at the Universitádella Svizzera italiana. He is editor in chief of Transactions on Software Engineering, and has served as an associate editor of the IEEE Transactions on Software Engineering, general chair of the ACM International Symposium on Software Testing and Analysis in 2013, program chair of the International Conference on Software Engineering in 2012 and of the ACM International Symposium on Software Testing and Analysis in 2006. He is known for his work on software testing, program analysis, self-healing and self-adaptive software systems. He is a senior member of the IEEE and disinghuised member of ACM.

Oliviero Riganelli is an Assistant Professor at the University of Milano Bicocca. He holds a Ph.D, in Computer Science and Complex System from the University of Camerino in 2009. He is a Software Engineer Scientist with a passion for Software Quality and Test Automation. His research interests focus on effective methods for designing and developing high-quality systems, including software testing, static and dynamic software analysis, and self-healing and self-adaptive systems. He is and has been involved in several international research and development projects in close collaboration with leading worldwide information and communication companies. He is also regularly involved in the program committees of workshops and conferences in his areas of interest.

Rui Xin is a Ph.D student in the Department of Informatics, Universitá della Svizzera italiana. Rui Xin got his masters degree in Software Engineering from Shanghai Jiao Tong University, China, 2014. His current research interest is self-healing cloud applications.