

WHAT IS CLAIMED IS:

1. A method comprising:

obtaining, by a failure detection platform, time series data corresponding to historical network messages;

identifying, by the failure detection platform, a plurality of anomalies in the time series data;

associating, by the failure detection platform, one or more anomalies of the plurality of anomalies with a classification label indicative of a network failure;

training, by the failure detection platform, a first model of a plurality of models utilizing the time series data;

training, by the failure detection platform, a second model of the plurality of models utilizing the time series data, the one or more anomalies associated with the classification label, and a supervised machine-learning algorithm;

training, by the failure detection platform, a third model based at least in part on outputs of the plurality of models;

predicting, by the failure detection platform, a future network failure utilizing the third model; and

performing, by the failure detection platform, one or more remedial actions in response to predicting the future network failure.

2. The method of claim 1, wherein the historical network messages of the time series data correspond to a distributed system comprising a plurality of computing devices.

3. The method of claim 1, wherein the time series data comprises response times corresponding to the historical network messages.

4. The method of claim 1, wherein the historical network messages of the time series data comprise authorization request messages and corresponding authorization response messages.

5. The method of claim 1, wherein detecting an anomaly of the plurality of anomalies comprises determining that a threshold period of time elapsed between an authorization request message during which a corresponding authorization response message was not received.

6. The method of claim 1, further comprising transforming the time series data prior to training the first model.

7. The method of claim 1, wherein at least one of the first model or the second model is a recurrent neural network.

8. The method of claim 1, wherein the first model is an auto-regression integrated moving average (ARIMA) model that is fit to the time series data.

9. The method of claim 1, wherein the first model is trained utilizing a stochastic process with a Markov property.

10. The method of claim 1, wherein identifying the plurality of anomalies utilizes an unsupervised learning technique with the time series data.

11. A computing device of a failure detection platform, the computing device comprising:

a processor; and

a memory comprising a computer readable storage medium that stores computer-executable instructions that, when executed by the processor, cause the computing device to perform operations comprising:

obtaining time series data corresponding to historical network messages of a distributed network;

identifying a plurality of anomalies in the time series data;

associating one or more anomalies of the plurality of anomalies with a classification label indicative of a network failure;

training a first model of a plurality of models utilizing the time series data;

training a second model of the plurality of models utilizing the time series data, the one or more anomalies associated with the classification label, and a supervised machine-learning algorithm;

training a third model based at least in part on outputs of the plurality of models;

predicting a future system failure utilizing the third model; and

performing one or more remedial actions in response to predicting the future system failure.

12. The computing device of claim 11, wherein the plurality of models comprise a first set of models trained utilizing at least one time series forecasting method, a second set of models trained utilizing at least one random distribution of the time series data, a third set of models trained utilizing at least one Markov process, and a fourth set of models comprising one or more recurrent neural networks.

13. The computing device of claim 11, wherein the instructions further cause the computing device to perform additional operations comprising transforming the time series data to a stationary data set, wherein transforming the time series data utilizing a differencing method.

14. The computing device of claim 11, wherein the supplemental data comprises contact data indicating a number of contacts made by users of the distributed network.

15. The computing device of claim 11, wherein the time series data comprises a first value indicating first time at which an authorization request message was sent from a first computing component to a second computing component and a second value, the second value indicating a second time at which an authorization response message corresponding to the authorization request message was received or that the authorization response message corresponding to the authorization request message was not received.

16. The computing device of claim 11, wherein at least one output of the plurality of models comprises a probability value indicating that input data provided to the third model signals a failure of at least one computing component of the distributed network.

17. The computing device of claim 11, wherein at least one output of the plurality of models comprises an additional classification label.

18. The computing device of claim 11, wherein the one or more remedial actions comprises transmitting a notification to at least one computing component of the distributed network, the notification comprising information indicating a failure of the at least one computing component.

19. The computing device of claim 11, wherein the one or more remedial actions comprises requesting that at least one computing component of the distributed network perform a system reset.

20. The computing device of claim 11, wherein the instructions further cause the computing device to perform additional operations comprising converting the times series data utilizing a window function aggregation.