CLAIMS:

1. A method for analysing log data, the method comprising:

receiving log data comprising traces having multiple log events from multiple different respective process executions, each of the multiple log events being associated with an event time;

creating a single stream of log events comprising the multiple log events from the multiple respective different process executions, wherein the single stream of log events is sorted by the associated event time;

iterating over the single stream of log events, and for each log event, executing one or more update functions that define updates of a set of variables based on the log events, the set of variables comprising at least one cross-trace variable to calculate an updated value of one or more of the set of variables, wherein the one or more update functions define updates of the at least one cross-trace variable in response to the log events of more than one of the traces; and

executing one or more evaluation functions on the set of variables to determine compliance in relation to the log data based on the updated value, the one or more evaluation functions representing compliance rules based on the set of variables including the cross-trace variable.

2. The method of claim 1, wherein the method comprises executing the one or more evaluation functions for each log event.

3. The method of claim 1 or 2, wherein the method comprises performing the steps of creating, iterating and executing in real-time to determine compliance while receiving further log data.

4. The method of any one of the preceding claims, wherein the compliance rules comprise a conditional obligation.

5. The method of any one of the preceding claims, wherein the compliance rules are defined across multiple processes.

6. The method of any one of the preceding claims, wherein the update functions define an update of one of the set of variables in response to log data from multiple processes or multiple process instances.

7. The method of any one of the preceding claims, wherein the log data comprises log data generated by a computer system executing an operating system.

8. The method of claim 7, wherein the log data is generated by different processes executed by the operating system.

9. The method of any one of the preceding claims, wherein the multiple log events comprise start log events that indicate the beginning of a task and stop events that indicate the end of a task.

10. The method of any one of the preceding claims, wherein the one or more evaluation functions are represented by evaluation predicates.

11. The method of claim 10, wherein the evaluation predicates are associated with a logical value indicating a predetermined occurrence of log events.

12. The method of claim 10 or 11, wherein the evaluation predicates are defined on a graph structure.

13. The method of claim 15, wherein the graph structure defines a precedence among the evaluation predicates.

14. The method of claim 14, wherein the method further comprises determining a set of evaluation functions or update functions that require execution based on the

graph structure and executing only the set of evaluation functions or update functions in that iteration.

15. The method of claim 14, wherein the method further comprises traversing the graph structure to assess compliance by, at each step:

adding evaluation functions and update functions the set,

executing the evaluation functions and update functions in the set, and

removing evaluation functions and update function from the set as defined by the graph structure.

16. The method of claim 14 or 15, wherein the set is stored on volatile computer memory.

17. The method of any one of claims 13 to 16, wherein the graph structure represents a combination of the state that has been checked and the evaluation functions or update functions that require execution.

18. The method of any one of the preceding claims, further comprising:

generating an instance of an update function or evaluation function or both to represent a rule;

storing the generated instance in volatile computer memory;

executing the generated instance in the volatile computer memory; and

discarding or overwriting the generated instance in the volatile computer memory while further determining compliance.

19. The method of claim 16, further comprising determining compliance of multiple traces in parallel against multiple rules.

20. The method of any one of the preceding claims, wherein the one or more evaluation functions are executed for an in-force time interval defined by the rules.

21. Software that, when installed on a computer, causes the computer to perform the method of any one of the preceding claims.

22. A computer system for monitoring compliance of another system by analysing log data, the computer system comprising a processor configured to:

receive the log data comprising traces having multiple log events from multiple respective different process execution, each of the multiple log events being associated with an event time;

create a single stream of log events comprising the multiple log events from the multiple respective different process executions, wherein the single stream of log events is sorted by the associated event time;

iterate over the single stream of log events, and for each log event, executing one or more update functions that define updates of a set of variables based on the log events, the set of variables comprising at least one cross-trace variable to calculate an updated value of one or more of the set of variables, wherein the one or more update functions define updates of the at least one cross-trace variable in response to the log events of more than one of the traces; and

execute one or more evaluation functions on the set of variables to determine compliance in relation to the log data based on the updated value, the one or more evaluation functions representing compliance rules based on the set of variables including the cross-trace variable.

~~AMENDED CLAIMS~~

~~received by the International Bureau on 17 August 2021 (17.08.2021)~~

CLAIMS:

1. A method for analysing log data, the method comprising:

receiving log data comprising traces having multiple log events from multiple different respective process executions, each of the multiple log events being associated with an event time;

creating a single stream of log events comprising the multiple log events from the multiple respective different process executions, wherein the single stream of log events is sorted by the associated event time;

iterating over the single stream of log events, and for each log event, executing one or more update functions that define updates of a set of variables based on the log events, the set of variables comprising at least one cross-trace variable to calculate an updated value of one or more of the set of variables, wherein the one or more update functions define updates of the at least one cross-trace variable in response to the log events of more than one of the traces; and

executing one or more evaluation functions on the set of variables to determine compliance in relation to the log data based on the updated value, the one or more evaluation functions representing compliance rules based on the set of variables including the cross-trace variable.

2. The method of claim 1, wherein the method comprises executing the one or more evaluation functions for each log event.

3. The method of claim 1 or 2, wherein the method comprises performing the steps of creating, iterating and executing in real-time to determine compliance while receiving further log data.

4. The method of any one of the preceding claims, wherein the compliance rules comprise a conditional obligation.

5. The method of any one of the preceding claims, wherein the compliance rules are defined across multiple processes.

6. The method of any one of the preceding claims, wherein the update functions define an update of one of the set of variables in response to log data from multiple processes or multiple process instances.

7. The method of any one of the preceding claims, wherein the log data comprises log data generated by a computer system executing an operating system.

8. The method of claim 7, wherein the log data is generated by different processes executed by the operating system.

9. The method of any one of the preceding claims, wherein the multiple log events comprise start log events that indicate the beginning of a task and stop events that indicate the end of a task.

10. The method of any one of the preceding claims, wherein the one or more evaluation functions are represented by evaluation predicates.

11. The method of claim 10, wherein the evaluation predicates are associated with a logical value indicating a predetermined occurrence of log events.

12. The method of claim 10 or 11, wherein the evaluation predicates are defined on a graph structure.

13. The method of claim 12, wherein the graph structure defines a precedence among the evaluation predicates.

14. The method of claim 12 or 13, wherein the method further comprises determining a set of evaluation functions or update functions that require execution based on the graph structure and executing only the set of evaluation functions or update functions in that iteration.

15. The method of claim 14, wherein the method further comprises traversing the graph structure to assess compliance by, at each step:

adding evaluation functions and update functions the set,

executing the evaluation functions and update functions in the set, and

removing evaluation functions and update function from the set as defined by the graph structure.

16. The method of claim 14 or 15, wherein the set is stored on volatile computer memory.

17. The method of any one of claims 13 to 16, wherein the graph structure represents a combination of the state that has been checked and the evaluation functions or update functions that require execution.

18. The method of any one of the preceding claims, further comprising:

generating an instance of an update function or evaluation function or both to represent a rule;

storing the generated instance in volatile computer memory;

executing the generated instance in the volatile computer memory; and

discarding or overwriting the generated instance in the volatile computer memory while further determining compliance.

19. The method of claim 18, further comprising determining compliance of multiple traces in parallel against multiple rules.

20. The method of any one of the preceding claims, wherein the one or more evaluation functions are executed for an in-force time interval defined by the rules.

21. Software that, when installed on a computer, causes the computer to perform the method of any one of the preceding claims.

22. A computer system for monitoring compliance of another system by analysing log data, the computer system comprising a processor configured to:

receive the log data comprising traces having multiple log events from multiple respective different process execution, each of the multiple log events being associated with an event time;

create a single stream of log events comprising the multiple log events from the multiple respective different process executions, wherein the single stream of log events is sorted by the associated event time;

iterate over the single stream of log events, and for each log event, executing one or more update functions that define updates of a set of variables based on the log events, the set of variables comprising at least one cross-trace variable to calculate an updated value of one or more of the set of variables, wherein the one or more update functions define updates of the at least one cross-trace variable in response to the log events of more than one of the traces; and

execute one or more evaluation functions on the set of variables to determine compliance in relation to the log data based on the updated value, the one or more evaluation functions representing compliance rules based on the set of variables including the cross-trace variable.