

CLAIMS

1. A computer-implemented method, comprising:
 - determining characteristics of a plurality of cloud vendors, including:
 - running capability and cost application programming interfaces (APIs) to perform scans of the cloud vendors,
 - and
 - parsing one or more fix databases to determine existing solutions to existing security problems for the cloud vendor;
 - wherein for at least some of the cloud vendors, the characteristics of the cloud vendors include capabilities of the cloud vendors, a cost of implementing the respective cloud vendor, and a security level implemented by the respective cloud vendor;
 - storing the characteristics of the plurality of cloud vendors;
 - dividing a workload into a plurality of logical stages according to points of data input and output within the workload, as well as dependencies associated with input to the workload;
 - for each of the logical stages;
 - determining a complexity of the logical stage by comparing inputs and outputs for the logical stage to historical stages, and
 - determining characteristics of each of the logical stages based on the complexity of the logical stage by comparing inputs, outputs, and intermediate results within the logical stage to historical workload stages to determine the complexity of the respective logical stage, the characteristics including one or more performance characteristics and one or more security requirements;
 - for each of the logical stages, assigning the logical stage to one of the cloud vendors, based on a comparison of the characteristics of the cloud vendors to the characteristics of the logical stage to determine the cloud vendor that is capable of meeting requirements of the logical stage, including comparing the characteristics of the logical stage to the characteristics of each of the cloud vendors to determine one or more of the cloud vendors that are capable of meeting the one or more performance characteristics and the one or more security requirements; and
 - performing migration between the cloud vendors of data operated on during an implementation of the workload to ensure the data is located at necessary cloud vendors during the corresponding tasks of the workload.
2. The computer-implemented method of claim 1, comprising collecting, via the scans, security database information; and parsing the security database information to identify reports, trends, vulnerabilities, and security problems for the cloud vendors.
3. The computer-implemented method of Claim 1, wherein at least some of the characteristics of the cloud vendors are determined by analyzing the cloud vendors, the analyzing including collecting and parsing one or more

public and private security database information to identify one or more of reports, trends, vulnerabilities, and security problems for each of the cloud vendors.

4. The computer-implemented method of Claim 1, wherein at least some of the characteristics of the cloud vendors are determined by analyzing the cloud vendors, the analyzing including parsing one or more fix databases to determine any existing solutions to any existing security problems for one or more of the cloud vendors.

5. The computer-implemented method of Claim 1, wherein at least some of the characteristics of the cloud vendors are determined by estimating one or more viability factors for each of the respective cloud vendors, based on collected review information for the cloud vendors, where the viability factors include serviceability, a net promoter score (NPS), user reviews, performance benchmarks, and tuning flexibility.

6. The computer-implemented method of Claim 1, wherein for at least some of the cloud vendors, the characteristics of a particular one of the cloud vendors include capabilities of the cloud vendor, a cost of implementing the cloud vendor, and viability factors associated with the cloud vendor.

7. The computer-implemented method of Claim 1, wherein the characteristics of the cloud vendors are compared to one or more predefined thresholds in order to determine a level for each of the characteristics of the cloud vendors.

8. The computer-implemented method of Claim 1, wherein for at least some of the cloud vendors, the characteristics for the cloud vendors include:

a cyber security characteristic indicating a level of security provided by the cloud vendor during workload implementation, and

a cyber resiliency characteristic indicating a level of crash protection, malware protection, and redundant data protection provided by the cloud vendor during workload implementation,

an estimated execution time,

one or more performance characteristics, and

one or more resource requirements.

9. The computer-implemented method of Claim 1, wherein dividing the workload includes parsing the workload to identify the points of data input and output within the workload.

10. The computer-implemented method of Claim 1, wherein source code of the workload is scanned to predict instances of data input and output within the workload.

11. The computer-implemented method of Claim 1, wherein at least some of the logical stages includes data input that is not dependent on other logical stages within the workload.
12. The computer-implemented method of Claim 1, wherein the complexity of each of the logical stages is determined based on intermediate results within the logical stage.
13. The computer-implemented method of claim 1, wherein: at least some of the characteristics of the cloud vendors are determined by
parsing one or more fix databases to determine existing solutions to existing security problems for one or more of the cloud vendors; and
wherein dividing the workload includes parsing the workload to identify points of data input and output within the workload.
14. The computer-implemented method of Claim 1, wherein assigning the logical stage to a cloud vendor includes mapping the logical stage to the cloud vendor so that the cloud vendor receives input required by the logical stage, performs operations required by the logical stage, and outputs data required by the logical stage.
15. The computer-implemented method of Claim 1, further comprising presenting a mapping of each logical stage to the cloud vendors to one or more users, using a graphical user interface (GUI).
16. The computer-implemented method of Claim 1, further comprising adjusting resource allocation within each logical stage based on user priorities.
17. The computer-implemented method of claim 1, wherein the migration includes migrating data from a first of the cloud vendors to a second of the cloud vendors, and migrating the data back from the second cloud vendor to the first cloud vendor.
18. A computer program product comprising one or more computer readable storage media, and program instructions collectively stored on the one or more computer readable storage media, the program instructions comprising instructions configured to cause one or more processors to perform a method comprising:
analyzing, by the one or more processors, a plurality of cloud vendors, the analyzing including running capability and cost application programming interfaces (APIs) to perform a scan of each cloud vendor for determining characteristics of each of the cloud vendors, the analyzing including parsing one or more fix databases to determine existing solutions to existing security problems for the cloud vendor, wherein for at least some of the cloud vendors, the characteristics of the cloud vendors include capabilities of the cloud vendors, a cost of implementing the respective cloud vendor, and a security level implemented by the respective cloud vendor;

determining, by the one or more processors, a relative level for each of the characteristics determined for the cloud vendors, the relative levels including relatively higher levels and relatively lower levels;

scanning, by the one or more processors, source code of a workload to predict instances of data input and output within the workload;

dividing, by the one or more processors, the workload into a plurality of logical stages, wherein dividing the workload includes parsing the workload to identify points of data input and output within the workload, as well as dependencies associated with input to the workload, wherein the dividing is based at least in part on the predicted instances of data input and output within the workload for increasing an accuracy of the dividing; for each of the logical stages:

determining, by the one or more processors, a complexity of the logical stage by comparing inputs and outputs for the logical stage to historical stages, and

determining, by the one or more processors, characteristics of each of the logical stages based on the complexity of the logical stage by comparing inputs, outputs, and intermediate results within the logical stage to historical workload stages to determine the complexity of the respective logical stage, the characteristics including one or more performance characteristics and one or more security requirements; comparing, by the one or more processors, the characteristics of the cloud vendors to the characteristics of the logical stages to determine which of the cloud vendors is capable of meeting requirements of the logical stage, the comparing including comparing the characteristics of the logical stage to the characteristics of each of the cloud vendors to determine one or more of the cloud vendors that are capable of meeting the one or more performance characteristics and the one or more security requirements; assigning, by the one or more processors based on the comparing, the logical stages to different ones of the cloud vendors for execution of the logical stages by the cloud vendors; and performing migration between the cloud vendors of data operated on during an implementation of the workload to ensure the data is located at necessary cloud vendors during the corresponding tasks of the workload.

19. The computer program product of claim 18, wherein the cloud vendors execute the logical stage(s) assigned thereto.

20. The computer program product of Claim 18, wherein the characteristics of at least some of the cloud vendors are determined by analyzing the respective cloud vendor, the analyzing including collecting and parsing one or more public and private security database information to identify one or more of reports, trends, vulnerabilities and security problems for each of the cloud vendors.

21. The computer program product of claim 18, comprising program instructions configured to cause the one or more processors to implement a life cycle management, including performing migration between the cloud vendors of data operated on during an implementation of the workload to ensure the data is located at necessary cloud vendors for operation thereupon during a corresponding task of the workload.

22. A system, comprising:

a processor; and

logic integrated with the processor, executable by the processor, or integrated with and executable by the processor, the logic being configured to:

running application programming interfaces (APIs) to scan a plurality of cloud vendors to determine characteristics of the plurality of cloud vendors;

parsing one or more fix databases to determine existing solutions to existing security problems for the cloud vendor to determine characteristics of the plurality of cloud vendors, wherein for at least some of the cloud vendors, the characteristics of the cloud vendors include capabilities of the cloud vendors, a cost of implementing the respective cloud vendor, and a security level implemented by the respective cloud vendor;

store the characteristics of the plurality of cloud vendors;

scan source code of a workload to predict instances of data input and output within the workload;

divide the workload into a plurality of logical stages according to the predicted instances of data input and output within the workload, as well as dependencies associated with input to the workload;

for each of the logical stages:

determine a complexity of the logical stage by comparing inputs and outputs for the logical stage to historical stages, and

determine characteristics of each of the logical stages based on the complexity of the logical stage by comparing inputs, outputs, and intermediate results within the logical stage to historical workload stages to determine the complexity of the respective logical stage, the characteristics including one or more performance characteristics and one or more security requirements;

for each of the logical stages, assign the logical stage to one of the cloud vendors, based on a comparison of the characteristics of the cloud vendors to the characteristics of the logical stage to determine the cloud vendor that is capable of meeting requirements of the logical stage,

wherein comparing the characteristics of the logical stage to the characteristics of the cloud vendors includes determining that one or more of the cloud vendors is capable of meeting one or more performance characteristics, the one or more security requirements, one or more resource requirements, and one or more cyber resiliency requirements of the logical stage; and

perform migration between the cloud vendors of data operated on during an implementation of the workload to ensure the data is located at necessary cloud vendors for operation thereupon during the corresponding tasks of the workload.

23. A computer-implemented method, comprising:

- determining characteristics of a plurality of cloud vendors including, for each of the cloud vendors:
 - running an application programming interface (API) to perform a scan of the cloud vendor, collecting and parsing security database information to identify reports, trends, vulnerabilities, and security problems for the cloud vendor,
 - parsing one or more fix databases to determine existing solutions to existing security problems for the cloud vendor, and
 - estimating viability factors for the cloud vendor, the viability factors including a serviceability, a net promoter score (NPS), performance benchmarks, and tuning flexibility for the cloud vendor,
- wherein the characteristics include capabilities of the cloud vendor, a cost of implementing the cloud vendor, a security level implemented by the cloud vendor, and viability factors associated with the cloud vendor;
- scanning source code of a workload to predict instances of data input and output within the workload;
- dividing the workload into a plurality of logical stages;
- determining characteristics of each of the logical stages, including, for each of the logical stages:
 - comparing inputs, outputs, and intermediate results within the logical stage to historical workload stages to determine a complexity for the logical stage,
 - wherein the characteristics of the logical stage are determined based on the complexity for the logical stage,
 - wherein the characteristics of the logical stage include an estimated execution time, one or more performance characteristics, one or more security requirements, one or more resource requirements, and one or more cyber resiliency requirements; and
- for each of the logical stages, assigning the logical stage to one of the cloud vendors, based on a comparison of the characteristics of the cloud vendors to the characteristics of the logical stage, including:
 - comparing the characteristics of the logical stage to the characteristics of each of the cloud vendors to determine one or more cloud vendors that are capable of meeting the one or more performance characteristics, the one or more security requirements, the one or more resource requirements, and the one or more cyber resiliency requirements of the logical stage; and
 - performing data migration between the cloud vendors during an implementation of the workload to ensure data is located at necessary cloud vendors during the corresponding tasks of the workload.

24. A computer program product comprising one or more computer readable storage media, and program instructions collectively stored on the one or more computer readable storage media, the program instructions comprising instructions configured to cause one or more processors to perform a method comprising:

- determining , by the one or more processors, characteristics of a plurality of cloud vendors, including, for each of the cloud vendors:

running capability and cost application programming interfaces (APIs) to perform a scan of the cloud vendor, and

parsing one or more fix databases to determine existing solutions to existing security problems for the cloud vendor,

wherein the characteristics include capabilities of the cloud vendor, a cost of implementing the cloud vendor, and a security level implemented by the cloud vendor;

scanning, by the one or more processors, source code of a workload to predict instances of data input and output within the workload;

dividing, by the one or more processors, the workload into a plurality of logical stages, including

parsing the workload to identify points of data input and output within the workload, as well as dependencies associated with input to the workload;

determining, by the one or more processors, characteristics of each of the logical stages, including, for each of the logical stages:

comparing inputs, outputs, and intermediate results within the logical stage to historical workload stages to determine a complexity for the logical stage,

wherein the characteristics of the logical stage are determined based on the complexity for the logical stage,

wherein the characteristics of the logical stage include an estimated execution time, one or more performance characteristics, one or more security requirements, one or more resource requirements, and one or more cyber resiliency requirements; and

for each of the logical stages, assigning, by the one or more processors, the logical stage to one of the cloud vendors, based on a comparison of the characteristics of the cloud vendors to the characteristics of the logical stage, including:

comparing the characteristics of the logical stage to the characteristics of each of the cloud vendors to determine one or more cloud vendors that are capable of meeting the one or more performance characteristics, one or more security requirements, one or more resource requirements, and one or more cyber resiliency requirements of the logical stage; and

implementing a life cycle management, including performing data migration between the cloud vendors during an implementation of the workload to ensure data is located at necessary cloud vendors during the corresponding tasks of the workload.