(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104506552 B
(45)授权公告日 2017.09.12

(21)申请号 201510002564.3

(22)申请日 2015.01.05

(65)同一申请的已公布的文献号
申请公布号 CN 104506552 A

(43)申请公布日 2015.04.08

(73)专利权人 山东金佳园科技股份有限公司
地址 264670 山东省烟台市高新区蓝海路1号4号楼

(72)发明人 刘文义 张兴林

(74)专利代理机构 北京天奇智新知识产权代理有限公司 11340
代理人 杨春

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 101271444 A,2008.09.24,
CN 102170440 A,2011.08.31,
CN 102111382 A,2011.06.29,
US 2012233683 A1,2012.09.13,
WO 2007037570 A1,2007.04.05,

审查员 冯婕

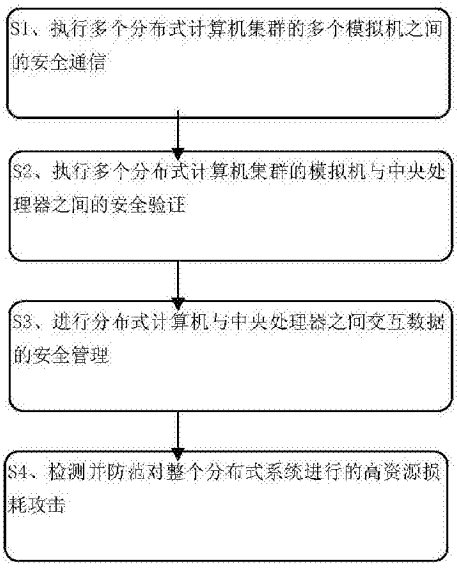
权利要求书2页 说明书8页 附图4页

(54)发明名称

一种信息系统安全监控及访问控制方法

(57)摘要

本发明的信息系统安全监控及访问控制方法通过集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信;通过可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证;通过交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理;以及通过高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击,大大提高了整个信息系统的可靠性和安全性。



CN 104506552 B

1.一种信息系统安全监控及访问控制方法，所述信息系统包括中央处理器、多个分布式计算机集群、多个集群网间连接器、可靠因子运算器、交互数据安全管理单元、高资源损耗攻击防范单元、运行于所述分布式计算机上的模拟机、以及可靠因子存储单元，所示信息系统安全监控及访问控制方法具体包括：

S1、通过集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信；

S2、通过可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证；

S3、通过交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理；以及

S4、通过高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击。

2.一种如权利要求1所述的方法，所述集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信具体包括：

A1、一个分布式计算机集群中的一个第一模拟机向另一个分布式计算机集群中的一个第二模拟机发起数据通信请求；

A2、所述第一模拟机所在分布式计算机集群的集群网间连接器根据所述数据通信请求中所包含的所述第一模拟机的安全识别码判定是否要做风险处理，当需要做风险处理时，执行下一步，否则进一步判断是直接接受该请求消息还是拒绝，若为直接接受，则转入步骤A4，若为拒绝，则抛弃该请求消息的数据包；

A3、所述第一模拟机所在分布式计算机集群的集群网间连接器根据所述第一模拟机与所述第二模拟机的安全识别码查找是否存在相应的预定安全链路，若不存在，创建新的预定安全链路，然后执行下一步，否则，直接执行下一步；

A4、将所述第一模拟机的安全识别码中的信息写入所述数据通信请求的数据包的地址字段，然后将数据包通过预定安全链路转发到所述第二模拟机所在的分布式计算机集群，由所述第二模拟机所在分布式计算机集群的集群网间连接器经由所述预定安全链路接收所述数据包；

A5、由所述第二模拟机的安全识别码与所述第一模拟机的安全识别码得到安全方案，将所述安全方案与所述第一模拟机所在分布式计算机集群的集群网间连接器的安全方案进行比较，在比较结果一致的前提下放行所述数据包，否则抛弃所述数据包；

A6、所述第二模拟机接收到数据包后，根据所述第一模拟机的安全识别码、所述第二模拟机的安全识别码以及数据通信控制方案判断所述第一模拟机对所述第二模拟机的操作类别，根据所述操作类别实现所述第一模拟机对所述第二模拟机的查询或拷贝。

3.一种如权利要求2所述的方法，所述第一模拟机所在分布式计算机集群的集群网间连接器与所述第二模拟机所在分布式计算机集群的集群网间连接器各自对所发送的消息进行加密，对所接收的消息进行解密。

4.一种如权利要求2所述的方法，所述的数据通信控制方案包括：根据模拟机预设的安全级别判断双方进行通信的操作权限，包括查询权限、拷贝权限、禁止访问。

5.一种如权利要求1所述的方法，所述可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全通信具体包括：

B1、模拟机通过可靠因子运算器与中央处理器之间提出建立通信策略并使用存储于可靠因子存储单元的密码进行身份验证；

B2、模拟机通过可靠因子运算器与中央处理器进行会话密码协商；

B3、执行从模拟机到中央处理器的数据传输。

6.一种如权利要求1所述的方法，所述高资源损耗攻击防范单元包括监测单元、防范进程启动单元、攻击防范实施单元；所述高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击具体包括：

C1、监测单元监测分布式系统的中央处理器、资源利用率、网络吞吐量性能与经验值进行对比分析；

C2、当系统性能门限值高于最高门限值时由防范进程启动单元启动防范进程；

C3、攻击防范实施单元在分布式计算机与中央处理器建立传输控制协议连接后，截获集群网间连接器向中央处理器发起的获取请求；其中，传输控制协议连接对中央处理器发送的统一资源定位符所对应的集群网间连接器；

C4、攻击防范实施单元通过中央处理器向这个分布式计算机返回一个包含会话跟踪数据的重定位到统一资源定位符的数据包，该会话跟踪数据是由中央处理器生成的，同时定义重定位次数N＝0；

C5、在重定位次数N＜3的情况下，如果分布式计算机是一个有效主机，则会根据超文本传送协议的规则对这个重定位数据包进行响应，如果分布式计算机是一个肉鸡主机，则不能对这个重定位数据包进行响应或者响应错误，重定位次数N+1，当重定位次数N＞＝3的时候，将此非法用户加入限制名单，禁止访问中央处理器；

C6、攻击防范实施单元根据上述响应对返回正确响应的分布式计算机的定义为有效，允许进行访问，进入C7；如果不能对重定位数据包进行响应或响应错误，则进入C5，再次进行会话跟踪数据的重定位；

C7、对当前系统的性能再次进行分析，当中央处理器、资源利用率、网络吞吐量接近系统最高门限时，对系统资源进行动态增加，同时增加模拟机数量帮助中央处理器接受超文本传送协议请求，对增加的模拟机进行记录，进入C8；当中央处理器、资源利用率、网络吞吐量为系统正常状态时，防范结束，继续监测中央处理器动态；

C8、再次对当前系统性能进行分析，当中央处理器、资源利用率、网络吞吐量恢复到系统正常状态时，恢复原始系统资源，同时移除增加的模拟机，恢复到原始系统，防范结束，继续监测中央处理器动态；当中央处理器、资源利用率、网络吞吐量仍然接近系统最高门限时，返回到C7。

一种信息系统安全监控及访问控制方法

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种信息系统安全监控及访问控制方法。

背景技术

[0002] 分布式计算技术是透过网络将庞大的计算处理程序自动分拆成无数个较小的子程序，再交由多部服务器所组成的庞大系统经搜寻、计算分析之后将处理结果回传给用户。透过这项技术，网络服务提供者可以在数秒之内，达成处理数以千万计甚至亿计的信息，达到和“超级计算机”同样强大效能的网络服务。

[0003] 正因为分布式计算的上述优点，如何保证各个分布式单元之间以及与中央单元的安全稳定的通信和数据管理显得越来越关键，以及目前分布式计算机系统经常面临的海量节点攻击服务器导致整个系统崩溃的情形。但是现有的分布式计算系统大多是通过简单验证和多机备份的方式进行安全保护，效率低，成本高，不利于分布式计算系统的未来发展。

发明内容

[0004] 本发明的目的是通过以下技术方案实现的。

[0005] 根据本发明的实施方式，提出一种信息系统安全监控及访问控制方法，所述信息系统包括中央处理器、多个分布式计算机集群、多个集群网间连接器、可靠因子运算器、交互数据安全管理单元、高资源损耗攻击防范单元、运行于所述分布式计算机上的模拟机、以及可靠因子存储单元，所示信息系统安全监控及访问控制方法具体包括：

[0006] S1、通过集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信；

[0007] S2、通过可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证；

[0008] S3、通过交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理；以及

[0009] S4、通过高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击。

[0010] 根据本发明的实施方式，所述集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信具体包括：

[0011] A1、一个分布式计算机集群中的一个第一模拟机向另一个分布式计算机集群中的一个第二模拟机发起数据通信请求；

[0012] A2、所述第一模拟机所在分布式计算机集群的集群网间连接器根据所述数据通信请求中所包含的所述第一模拟机的安全识别码判定是否要做风险处理，当需要做风险处理时，执行下一步，否则进一步判断是直接接受该请求消息还是拒绝，若为直接接受，则转入步骤A4，若为拒绝，则抛弃该请求消息的数据包；

[0013] A3、所述第一模拟机所在分布式计算机集群的集群网间连接器根据所述第一模拟

机与所述第二模拟机的安全识别码查找是否存在相应的预定安全链路，若不存在，创建新的预定安全链路，然后执行下一步，否则，直接执行下一步；

[0014] A4、将所述第一模拟机的安全识别码中的信息写入所述数据通信请求的数据包的地址字段，然后将数据包通过所述预定安全链路转发到所述第二模拟机所在的分布式计算机集群，由所述第二模拟机所在分布式计算机集群的集群网间连接器经由所述预定安全链路接收所述数据包；

[0015] A5、由所述第二模拟机的安全识别码与所述第一模拟机的安全识别码得到安全方案，将所述安全方案与所述第一模拟机所在分布式计算机集群的集群网间连接器的安全方案进行比较，在比较结果一致的前提下放行所述数据包，否则抛弃所述数据包；

[0016] A6、所述第二模拟机接收到数据包后，根据所述第一模拟机的安全识别码、所述第二模拟机的安全识别码以及数据通信控制方案判断所述第一模拟机对所述第二模拟机的操作类别，根据所述操作类别实现所述第一模拟机对所述第二模拟机的查询或拷贝。

[0017] 根据本发明的实施方式，所述第一模拟机所在分布式计算机集群的集群网间连接器与所述第二模拟机所在分布式计算机集群的集群网间连接器各自对所发送的消息进行加密，对所接收的消息进行解密。

[0018] 根据本发明的实施方式，所述的数据通信控制方案包括：根据模拟机预设的安全级别判断双方进行通信的操作权限，包括查询权限、拷贝权限、禁止访问。

[0019] 根据本发明的实施方式，所述可靠因子运算器执行多个分布式计算机集群的模拟机与云中央处理器之间的安全通信具体包括：

[0020] B1、模拟机通过可靠因子运算器与云中央处理器之间提出建立通信策略并使用存储于可靠因子存储单元的密码进行身份验证；

[0021] B2、模拟机通过可靠因子运算器与中央处理器进行会话密码协商；

[0022] B3、执行从模拟机到中央处理器的数据传输。

[0023] 根据本发明的实施方式，所述高资源损耗攻击防范单元包括监测单元、防范进程启动单元、攻击防范实施单元；所述高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击具体包括：

[0024] C1、监测单元监测分布式系统的中央处理器、资源利用率、网络吞吐量性能与经验值进行对比分析；

[0025] C2、当系统性能门限值高于最高门限值时由防范进程启动单元启动防范进程；

[0026] C3、攻击防范实施单元在分布式计算机与中央处理器建立传输控制协议连接后，截获集群网间连接器向中央处理器发起的获取请求；其中，传输控制协议连接对中央处理器发送的统一资源定位符所对应的集群网间连接器；

[0027] C4、攻击防范实施单元通过中央处理器向这个分布式计算机返回一个包含会话跟踪数据的重定位到统一资源定位符的数据包，该会话跟踪数据是由中央处理器生成的，同时定义重定位次数N＝0；

[0028] C5、在重定位次数N＜3的情况下，如果分布式计算机是一个有效主机，则会根据超文本传送协议的规则对这个重定位数据包进行响应，如果分布式计算机是一个肉鸡主机，则不能对这个重定位数据包进行响应或者响应错误，重定位次数N+1，当重定位次数N＞＝3的时候，将此非法用户加入限制名单，禁止访问中央处理器；

[0029] C6、攻击防范实施单元根据上述响应对返回正确响应的分布式计算机的定义为有效，允许进行访问，进入C7；如果不能对重定位数据包进行响应或响应错误，则进入C5，再次进行会话跟踪数据的重定位；

[0030] C7、对当前系统的性能再次进行分析，当中央处理器、资源利用率、网络吞吐量接近系统最高门限时，对系统资源进行动态增加，同时增加模拟机数量帮助中央处理器接受超文本传送协议请求，对增加的模拟机进行记录，进入C8；当中央处理器、资源利用率、网络吞吐量为系统正常状态时，防范结束，继续监测中央处理器动态；

[0031] C8、再次对当前系统性能进行分析，当中央处理器、资源利用率、网络吞吐量恢复到系统正常状态时，恢复原始系统资源，同时移除增加的模拟机，恢复到原始系统，防范结束，继续监测中央处理器动态；当中央处理器、资源利用率、网络吞吐量仍然接近系统最高门限时，返回到C7。

[0032] 本发明的信息系统安全监控及访问控制方法通过集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信；通过可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证；通过交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理；以及通过高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击，大大提高了整个信息系统的可靠性和安全性。

附图说明

[0033] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0034] 附图1示出了根据本发明实施方式的信息系统结构示意图；

[0035] 附图2示出了根据本发明实施方式的信息系统安全监控及访问控制方法流程图；

[0036] 附图3示出了根据本发明实施方式的通过集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信流程图；

[0037] 附图4示出了根据本发明实施方式的通过可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证流程图；

[0038] 附图5示出了根据本发明实施方式的通过交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理流程图；

[0039] 附图6示出了根据本发明实施方式的通过高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击。

具体实施方式

[0040] 下面将参照附图更详细地描述本公开的示例性实施方式。虽然附图中显示了本公开的示例性实施方式，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0041] 根据本发明的实施方式，提出一种信息系统安全监控及访问控制方法，如附图1所示，所述信息系统包括中央处理器、多个分布式计算机集群(附图中示出了一个详细的集

群)、多个集群网间连接器、可靠因子运算器、交互数据安全管理单元、高资源损耗攻击防范单元、运行于所述分布式计算机上的模拟机、以及可靠因子存储单元，所述可靠因子存储单元存储用以进行模拟机身份识别的密码，每个分布式计算机集群包括一个集群网间连接器，所述分布式计算机集群依次通过集群网间连接器、可靠因子运算器、以及交互数据安全管理单元连接中央处理器，所述中央处理器还连接高资源损耗攻击防范单元，所述分布式计算机上运行模拟机和可靠因子存储单元。

[0042] 如附图2所示，所示信息系统安全监控及访问控制方法具体包括：

[0043] S1、通过集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信；

[0044] S2、通过可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证；

[0045] S3、通过交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理；以及

[0046] S4、通过高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击。

[0047] 根据本发明的实施方式，如附图3所示，所述集群网间连接器执行多个分布式计算机集群的多个模拟机之间的安全通信具体包括：

[0048] A1、一个分布式计算机集群中的一个第一模拟机向另一个分布式计算机集群中的一个第二模拟机发起数据通信请求；

[0049] A2、所述第一模拟机所在分布式计算机集群的集群网间连接器根据所述数据通信请求中所包含的所述第一模拟机的安全识别码判定是否要做风险处理，当需要做风险处理时，执行下一步，否则进一步判断是直接接受该请求消息还是拒绝，若为直接接受，则转入步骤A4，若为拒绝，则抛弃该请求消息的数据包；其中，

[0050] 所述安全识别码包括码头部分与安全ID集合，所述安全ID集合包括有至少一个安全ID，一个所述的安全ID描述了至少一种安全识别码实施策略；所述安全ID包含安全ID类别，所述安全ID类别为机密性、完整性与可用性中的一种；

[0051] A3、所述第一模拟机所在分布式计算机集群的集群网间连接器根据所述第一模拟机与所述第二模拟机的安全识别码查找是否存在相应的预定安全链路，若不存在，创建新的预定安全链路，然后执行下一步，否则，直接执行下一步；

[0052] A4、将所述第一模拟机的安全识别码中的信息写入所述数据通信请求的数据包的地址字段，然后将数据包通过所述预定安全链路转发到所述第二模拟机所在的分布式计算机集群，由所述第二模拟机所在分布式计算机集群的集群网间连接器经由所述预定安全链路接收所述数据包；

[0053] A5、由所述第二模拟机的安全识别码与所述第一模拟机的安全识别码得到安全方案，将所述安全方案与所述第一模拟机所在分布式计算机集群的集群网间连接器的安全方案进行比较，在比较结果一致的前提下放行所述数据包，否则抛弃所述数据包；

[0054] A6、所述第二模拟机接收到数据包后，根据所述第一模拟机的安全识别码、所述第二模拟机的安全识别码以及数据通信控制方案判断所述第一模拟机对所述第二模拟机的操作类别，根据所述操作类别实现所述第一模拟机对所述第二模拟机的查询或拷贝。

[0055] 在所述的步骤A1与步骤A2之间，还包括：

[0056] A11、所述第一模拟机所在分布式计算机集群的集群网间连接器对所述数据通信请求消息的数据包做路径追踪处理，查找链路状态表，得到反馈值，若其反馈值表示已经绑定到某一路径且符合链路状态，则直接执行步骤A4，若其反馈值为新建状态，那么查找第一模拟机安全识别码，然后执行步骤A2，若其反馈值表示已绑定到某一路径，但不符合该路径状态，则释放此数据包；

[0057] 在所述的步骤A2中，还包括：当该请求消息被拒绝时，将安全识别码动态绑定到通信连接，建立链路状态表；

[0058] 在所述的步骤A4与步骤A5之间，还包括：

[0059] 步骤A41、对所述数据包进行路径追踪处理，得到反馈值，若所述反馈值表示为已经绑定到某一路径且符合链路状态，直接将数据包按照链路状态中的处理方式进行处理；若反馈值为新建状态，执行步骤A5；若反馈值为已经绑定到某一路径且不符合链路状态，则抛弃数据包；

[0060] 在所述步骤A5中还包括：在抛弃所述数据包后，将安全识别码动态绑定到通信连接，建立链路状态表。

[0061] 在所述的步骤A3中，所述的创建新的预定安全链路包括：

[0062] A31、所述第一模拟机所在分布式计算机集群的集群网间连接器发送建立预定安全链路的请求消息到所述第二模拟机所在分布式计算机集群的集群网间连接器；该请求消息包括所述第一模拟机的安全识别码信息，所述第二模拟机的识别信息；

[0063] A32、所述第二模拟机所在分布式计算机集群的集群网间连接器查找所述第二模拟机的安全识别码，结合所述第一模拟机的安全识别码决定是否允许建立所述预定安全链路，若允许，发送响应消息给所述第一模拟机所在分布式计算机集群的集群网间连接器；所述响应消息包括所述预定安全链路的级别、算法在内的预定安全链路参数；

[0064] A33、所述第一模拟机所在分布式计算机集群的集群网间连接器获得预定安全链路参数后，向所述第二模拟机所在分布式计算机集群的集群网间连接器返回确认消息，建立所述的预定安全链路。

[0065] 根据本发明的实施方式，所述第一模拟机所在分布式计算机集群的集群网间连接器与所述第二模拟机所在分布式计算机集群的集群网间连接器各自对所发送的消息进行加密，对所接收的消息进行解密。

[0066] 在所述的步骤A4中，在将所述第一模拟机的安全识别码中的信息写入所述数据通信请求的数据包的地址字段后，还包括对所述数据包进行加密、验证、封装的操作，然后再将数据包通过所述预定安全链路转发到所述第二模拟机所在的分布式计算机集群；

[0067] 在所述步骤A4中，所述第二模拟机所在分布式计算机集群的集群网间连接器经由所述预定安全链路接收所述数据包时，还要对所述数据包做解密、验证、解封装的操作。

[0068] 所述的数据通信控制方案包括：

[0069] 根据模拟机预设的安全级别判断双方进行通信的操作权限，包括查询权限、拷贝权限、禁止访问等。

[0070] 根据本发明的实施方式，如附图4所示，所述可靠因子运算器执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证具体包括：

[0071] B1、模拟机通过可靠因子运算器与中央处理器之间提出建立通信策略并使用存储于可靠因子存储单元的密码进行身份验证，包括：

[0072] B11、可靠因子运算器获取对应模拟机的可靠因子存储单元的用于身份验证的密码电子身份证，并且向中央处理器发送所述密码电子身份证；

[0073] B12、中央处理器验证所述电子身份证是否过期，通过验证后，向可靠因子运算器发送自身的用于身份验证的密码电子身份证，同时产生验证码N1(32位)，使用模拟机的身份验证密码密钥加密N1，并发送给可靠因子运算器，只有模拟机的身份验证密码对称密钥才能正确解密得到这个验证码；

[0074] B13、可靠因子运算器验证中央处理器身份验证密码电子身份证是否过期，验证通过后，使用对应模拟机的身份验证密码对称密钥解密得到验证码N1，可靠因子运算器也产生一个验证码N2，使用中央处理器身份验证密码密钥加密N2和N1，然后用模拟机的身份验证密码对称密钥签名，发送给中央处理器；

[0075] B14、中央处理器验证收到的N1是否为自己发出的，如果是则使用模拟机身份验证密码密钥加密N2，然后用自己的身份验证密码对称密钥签名，发送给可靠因子运算器；

[0076] B15、可靠因子运算器验证收到的N2是否为自己发出的，如果是则双方身份验证完成；

[0077] B2、模拟机通过可靠因子运算器与中央处理器进行会话密码协商，包括：

[0078] B21、可靠因子运算器和中央处理器协商两个系统公开参数a和q，其中a是整数，q是素数，a是q的素根；

[0079] B22、可靠因子运算器选择一个验证码s，计算出一个密钥A，$A=a^s \bmod q$，发送给中央处理器；

[0080] B23、中央处理器选择一个验证码d，计算出一个密钥B，$B=a^d \bmod q$，发送给可靠因子运算器；

[0081] B24、可靠因子运算器根据B计算共享密码K1，$K1=B^s \bmod q$，并对共享密码K1进行散列运算，发送给中央处理器，中央处理器根据A计算出共享密码K2，$K2=A^d \bmod q$，并对共享密码K2进行散列运算，比较与收到的散列值是否相同，如果相同则会话密码有效；

[0082] B3、执行从模拟机到中央处理器的数据传输，包括：

[0083] B31、模拟机使用可靠因子运算器计算的共享密码对数据进行加密，同时产生一个验证码，加密结果与验证码构成一个数据包，对数据包进行散列计算，散列值与数据包一起发送给中央处理器；

[0084] B32、中央处理器接收到消息后，进行完整性验证，如果验证成功则通知中央处理器，数据接收正常。

[0085] 根据本发明的实施方式，所述交互数据安全管理单元包括：加密单元、数据分割单元、数据存储分配单元、权限判断单元、数据读取单元、纠错单元以及解密单元，如附图5所示，所述交互数据安全管理单元进行分布式计算机与中央处理器之间交互数据的安全管理具体包括：数据上载进程和数据下载进程；其中

[0086] 所述数据上载进程包括：

[0087] D11、通过加密单元将所述待上载文件二次加密；

[0088] D12、通过数据分割单元根据事先配置的冗余纠错码将待上载文件密文切分成若

干个数据块，并分配相应的块识别码；

[0089] D13、数据存储分配单元采用数据分布存储算法将这些数据块分发到中央处理器的存储节点中存储，同时存储相应的中继数据信息，所述中继数据信息包括：文件的访问权限、数据块的路由信息、及文件和数据块的对应关系；

[0090] 所述数据下载进程包括：

[0091] D21、权限判断单元判断分布式计算机是否具有下载数据的权限；

[0092] D22、若有，则通过数据读取单元查询文件和数据块的对应关系信息得到相应块识别码，并通过这些块识别码查询数据块的路由信息，读取数据块；

[0093] D23、将读取的数据块缓存，进行文件纠错解码，恢复文件的完整密文；

[0094] D24、将文件密文进行解密，并传给分布式计算机。

[0095] 根据本发明的实施方式，所述高资源损耗攻击防范单元包括监测单元、防范进程启动单元、攻击防范实施单元；如附图6所示，所述高资源损耗攻击防范单元检测并防范对整个分布式系统进行的高资源损耗攻击具体包括：

[0096] C1、监测单元监测分布式系统的中央处理器、资源利用率、网络吞吐量性能与经验值进行对比分析；

[0097] C2、当系统性能门限值高于最高门限值时由防范进程启动单元启动防范进程；

[0098] C3、攻击防范实施单元在分布式计算机与中央处理器建立传输控制协议连接后，截获集群网间连接器向中央处理器发起的获取请求；其中，传输控制协议连接对中央处理器发送的统一资源定位符所对应的集群网间连接器；

[0099] C4、攻击防范实施单元通过中央处理器向这个分布式计算机返回一个包含会话跟踪数据的重定位到统一资源定位符的数据包，该会话跟踪数据是由中央处理器生成的，同时定义重定位次数N＝0；

[0100] C5、在重定位次数N＜3的情况下，如果分布式计算机是一个有效主机，则会根据超文本传送协议的规则对这个重定位数据包进行响应，如果分布式计算机是一个肉鸡主机，则不能对这个重定位数据包进行响应或者响应错误，重定位次数N+1，当重定位次数N＞＝3的时候，将此非法用户加入限制名单，禁止访问中央处理器；

[0101] C6、攻击防范实施单元根据上述响应对返回正确响应的分布式计算机的定义为有效，允许进行访问，进入C7；如果不能对重定位数据包进行响应或响应错误，则进入C5，再次进行会话跟踪数据的重定位；

[0102] C7、对当前系统的性能再次进行分析，当中央处理器、资源利用率、网络吞吐量接近系统最高门限时，对系统资源进行动态增加，同时增加模拟机数量帮助中央处理器接受超文本传送协议请求，对增加的模拟机进行记录，进入C8；当中央处理器、资源利用率、网络吞吐量为系统正常状态时，防范结束，继续监测中央处理器动态；

[0103] C8、再次对当前系统性能进行分析，当中央处理器、资源利用率、网络吞吐量恢复到系统正常状态时，恢复原始系统资源，同时移除增加的模拟机，恢复到原始系统，防范结束，继续监测中央处理器动态；当中央处理器、资源利用率、网络吞吐量仍然接近系统最高门限时，返回到C7。

[0104] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，

都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

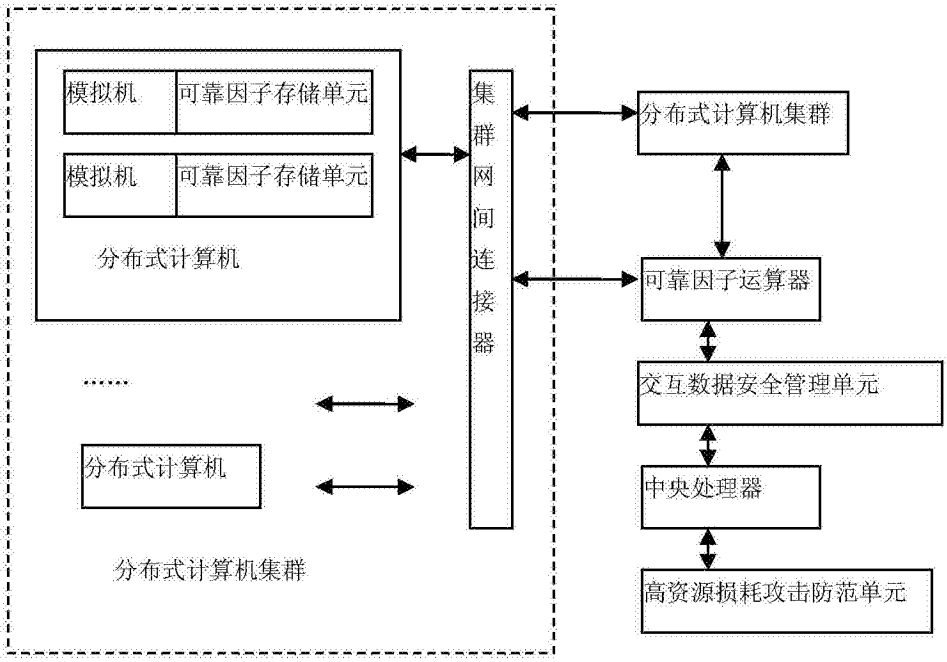

模拟机
可靠因子存储单元
模拟机
可靠因子存储单元
分布式计算机
.....
分布式计算机
分布式计算机集群
集群网间连接器
分布式计算机集群
可靠因子运算器
交互数据安全管理单元
中央处理器
高资源损耗攻击防范单元

图1

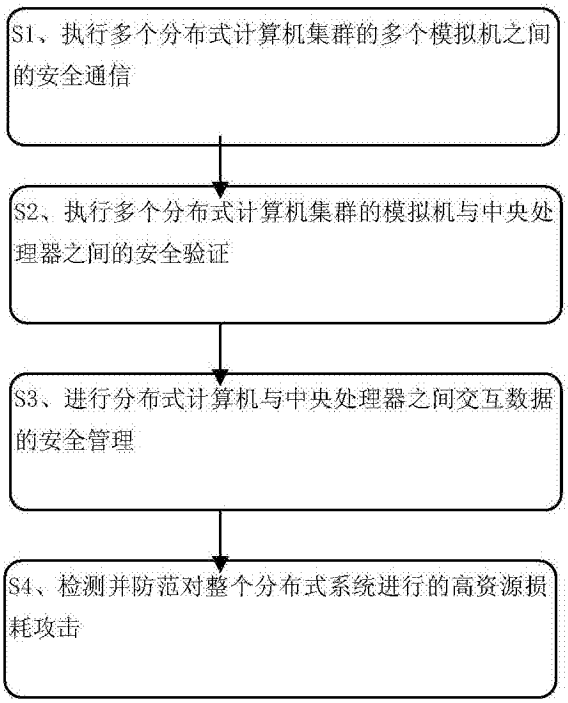

S1、执行多个分布式计算机集群的多个模拟机之间的安全通信
S2、执行多个分布式计算机集群的模拟机与中央处理器之间的安全验证
S3、进行分布式计算机与中央处理器之间交互数据的安全管理
S4、检测并防范对整个分布式系统进行的高资源损耗攻击

图2

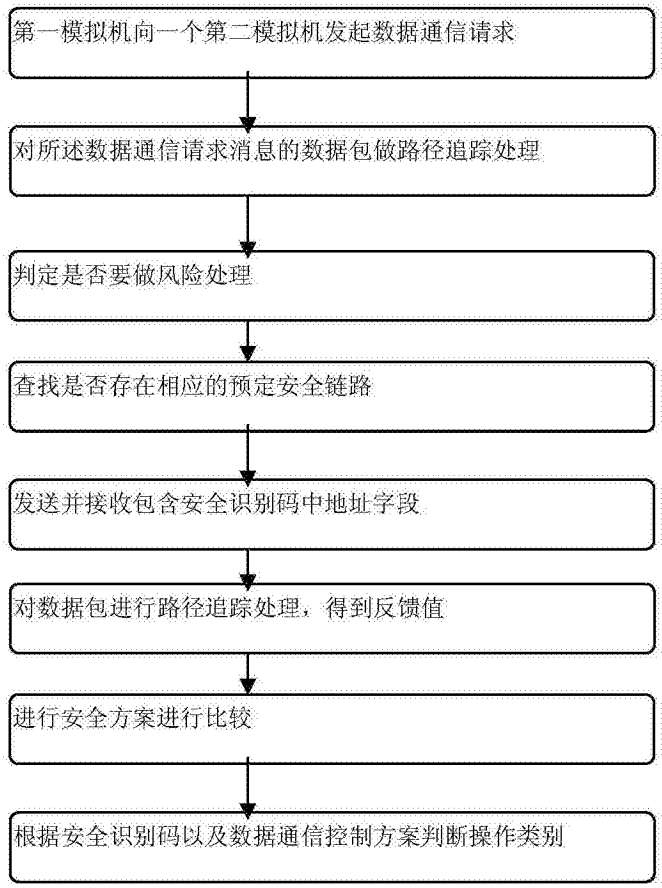

第一模拟机向一个第二模拟机发起数据通信请求
对所述数据通信请求消息的数据包做路径追踪处理
判定是否要做风险处理
查找是否存在相应的预定安全链路
发送并接收包含安全识别码中地址字段
对数据包进行路径追踪处理，得到反馈值
进行安全方案进行比较
根据安全识别码以及数据通信控制方案判断操作类别

图3

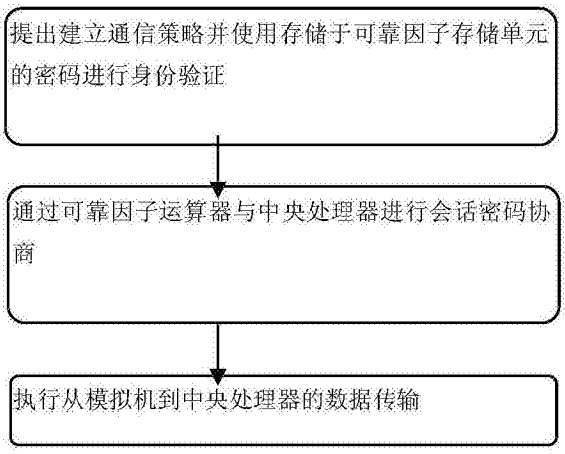

提出建立通信策略并使用存储于可靠因子存储单元的密码进行身份验证
通过可靠因子运算器与中央处理器进行会话密码协商
执行从模拟机到中央处理器的数据传输

图4

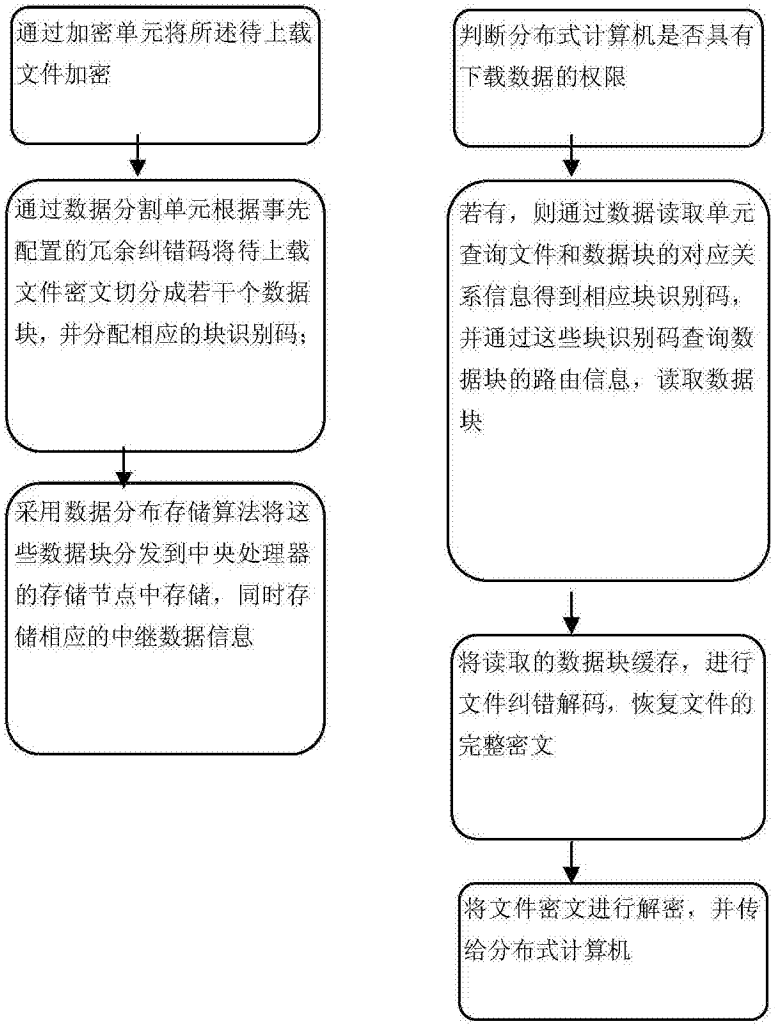

通过加密单元将所述待上载文件加密
通过数据分割单元根据事先配置的冗余纠错码将待上载文件密文切分成若干个数据块，并分配相应的块识别码；
采用数据分布存储算法将这些数据块分发到中央处理器的存储节点中存储，同时存储相应的中继数据信息
判断分布式计算机是否具有下载数据的权限
若有，则通过数据读取单元查询文件和数据块的对应关系信息得到相应块识别码，并通过这些块识别码查询数据块的路由信息，读取数据块
将读取的数据块缓存，进行文件纠错解码，恢复文件的完整密文
将文件密文进行解密，并传给分布式计算机

图5

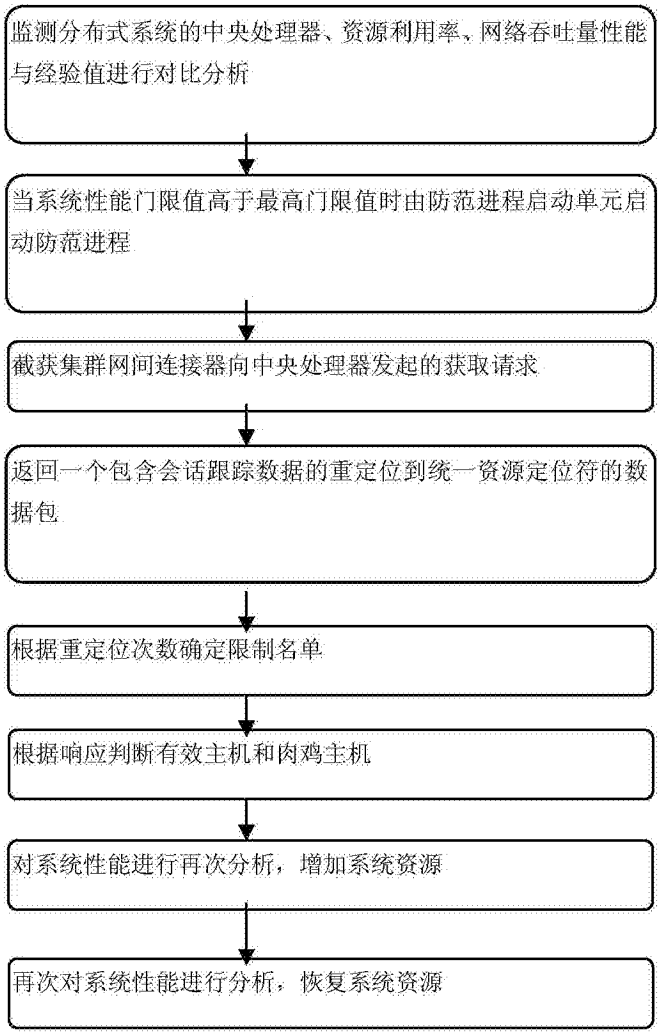

监测分布式系统的中央处理器、资源利用率、网络吞吐量性能与经验值进行对比分析
当系统性能门限值高于最高门限值时由防范进程启动单元启动防范进程
截获集群网间连接器向中央处理器发起的获取请求
返回一个包含会话跟踪数据的重定位到统一资源定位符的数据包
根据重定位次数确定限制名单
根据响应判断有效主机和肉鸡主机
对系统性能进行再次分析，增加系统资源
再次对系统性能进行分析，恢复系统资源

图6