

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2024/208194 A1

(43) 国际公布日
2024 年 10 月 10 日 (10.10.2024)

(51) 国际专利分类号:

G06F 21/56 (2013.01)

G06F 21/62 (2013.01)

G06F 40/151 (2020.01)

(74) 代理人:北京同钧律师事务所(**BEIJING TONGJUN LAW FIRM**); 中国北京市海淀区西直门北大街32号院1号楼7层808室, Beijing 100082 (CN)。

(21) 国际申请号: PCT/CN2024/085521

(22) 国际申请日: 2024 年 4 月 2 日 (02.04.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:

202310352365.X 2023年4月4日 (04.04.2023) CN

(71) 申请人: 云智能资产控股(新加坡)私人股份有限公司(**CLOUD INTELLIGENCE ASSETS HOLDING (SINGAPORE) PRIVATE LIMITED**) [SG/SG]; 新加坡新加坡市勿拉士峇沙路51号来赞达一号大厦#03-06, Singapore 189554 (SG)。

(72) 发明人: 朴君 (**PIAO, Jun**); 中国浙江省杭州市西湖区三墩镇灯彩街1008号云谷园区, Zhejiang 310030 (CN)。

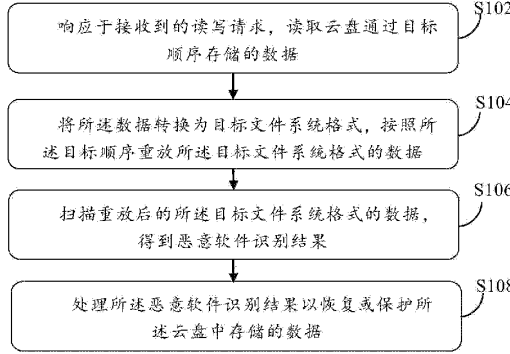
(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,

(54) **Title:** DATA PROTECTION METHOD AND SYSTEM, STORAGE SERVER, AND CLIENT

(54) 发明名称: 数据保护方法及系统、存储服务器和客户端

[图1]



S102 In response to a received read-write request, read data stored in a target order in a cloud disk

S104 Convert the data to a target file system format, and re-arrange the data in the target file system format in the target order

S106 Scan the re-arranged data in the target file system format to obtain a malicious software identification result

S108 Process the malicious software identification result to recover or protect the data stored in the cloud disk

(57) **Abstract:** The present application relates to the technical field of cloud computing, and discloses a data protection method and system, a storage server, and a client. The data protection method comprises: in response to a received read-write request, reading data stored in a target order in a cloud disk; converting the data to a target file system format, and re-arranging the data in the target file system format in the target order, wherein the target file system format is compatible with a file system of a client; scanning the re-arranged data in the target file system format to obtain a malicious software identification result; and processing the malicious software identification result to recover or protect the data stored in the cloud disk. The present application achieves the real-time performance of malicious software identification, reduces the data security risk to the maximum extent, and reduces the storage cost because there is no need to plan a separate storage space for a scanning task.

[见续页]

PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请公开了一种数据保护方法及系统、存储服务器和客户端, 涉及云计算技术领域, 该数据保护方法包括: 响应于接收到的读写请求, 读取云盘通过目标顺序存储的数据; 将所述数据转换为目标文件系统格式, 按照所述目标顺序重放所述目标文件系统格式的数据; 其中, 所述目标文件系统格式与所述客户端的文件系统适配; 扫描重放后的所述目标文件系统格式的数据, 得到恶意软件识别结果; 处理所述恶意软件识别结果以恢复或保护所述云盘中存储的数据。本申请实现了恶意软件识别的实时性, 最大限度降低数据安全风险, 无需单独为扫描任务规划存储空间, 降低存储成本。