



## (12)发明专利申请

(10)申请公布号 CN 110866233 A

(43)申请公布日 2020.03.06

(21)申请号 201910896068.5

(22)申请日 2019.09.22

(71)申请人 苏州浪潮智能科技有限公司

地址 215100 江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢

(72)发明人 李哲

(74)专利代理机构 济南舜源专利事务所有限公司 37205

代理人 张亮

(51)Int.Cl.

G06F 21/32(2013.01)

G06F 21/88(2013.01)

G08B 13/22(2006.01)

G08B 25/08(2006.01)

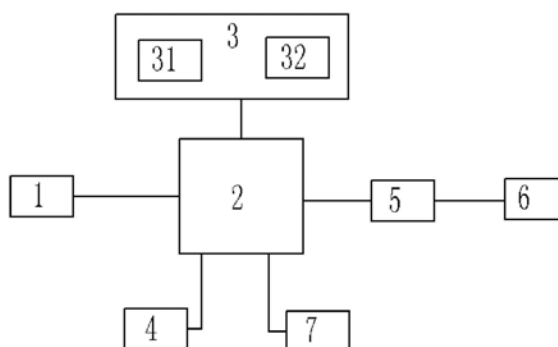
权利要求书1页 说明书3页 附图1页

### (54)发明名称

一种服务器硬盘防盗报警系统及方法

### (57)摘要

本发明涉及一种服务器硬盘防盗报警系统及方法,包括:用于监测防盗挡板在位状态信息的在位检测电路;所述的在位检测电路连接到微控制器;在位检测电路实时将防盗挡板的在位信息传送到微控制器;微控制器连接有供电模块;通过供电模块对微控制器进行供电;微控制器还连接有指纹识别模块和GMS模块,指纹识别模块将识别到的指纹信息传送到微控制器,GMS模块将微控制器产生的报警信号传送到后台监控中心;微控制器还连接有存储器。



1. 一种服务器硬盘防盗报警系统,其特征在于,包括:  
用于监测防盗挡板在位状态信息的在位检测电路;  
所述的在位检测电路连接到微控制器;在位检测电路实时将防盗挡板的在位信息传送至微控制器;  
微控制器连接有供电模块;通过供电模块对微控制器进行供电;  
微控制器还连接有指纹识别模块和GMS模块,指纹识别模块将识别到的指纹信息传送至微控制器,GMS模块将微控制器产生的报警信号传送至后台监控中心;  
微控制器还连接有存储器。
2. 根据权利要求1所述的一种服务器硬盘防盗报警系统,其特征在于,所述的供电模块包括板载供电单元和蓄电池供电单元。
3. 根据权利要求2所述的一种服务器硬盘防盗报警系统,其特征在于,所述的在位检测电路设置有多组,分布在防盗挡板的周边,检测防盗挡板的在位信息。
4. 根据权利要求3所述的一种服务器硬盘防盗报警系统,其特征在于,所述的微控制器采用51系列单片机控制器。
5. 一种服务器硬盘防盗报警方法,其特征在于,包括以下步骤:  
S 1:对防盗挡板的在位状态信息进行采集;  
S2:对采集到的在位状态信息进行处理,如果在位状态信息正常,则不进行任何操作,如果在位状态信息异常,则转到步骤S3;  
S3:判断在位状态信息异常是否属于服务器例行检查的情况,如果是则不进行报警操作,否则向远程控制中心发送报警信号;  
所述步骤S3中通过指纹识别模块识别操作人员指纹,如果指纹识别正确,则认定属于服务器例行检查。
6. 根据权利要求5所述的一种服务器硬盘防盗报警方法,其特征在于,所述步骤S1中,通过多路在位检测电路对防盗挡板的在位状态信息进行监测。
7. 根据权利要求6所述的一种服务器硬盘防盗报警方法,其特征在于,所述步骤S3中,通过短信发送方式向远程控制中心发送报警信号。

## 一种服务器硬盘防盗报警系统及方法

### 技术领域

[0001] 本发明属于服务器安全保护技术领域,具体涉及一种服务器硬盘防盗报警系统及方法。

### 背景技术

[0002] 服务器已经成为企业中不可缺少的器件之一,在企业办公中起到不可替代的作用,硬盘是服务器非常重要的一种硬件,是服务器的一个主要存储空间,存储着服务器中的所有数据它的安全性直接决定着企业数据安全。

[0003] 随着科技的快速发展,服务器硬盘的作用会越来越大,但是目前的服务器硬盘防盗性能较差,若出现硬盘被盗的情况,将会对企业信息和资产造成严重的损失。

[0004] 现有技术中,通过在服务器前置挂耳中间位置增加防盗挡板的方式实现安全保护,但是这种方式,当硬盘被盗窃时,无法及时通知远程监控中心采取措施,导致硬盘数据丢失;此为现有技术中存在的缺陷和不足。

[0005] 有鉴于此,本申请提供一种服务器硬盘防盗报警系统及方法;以解决现有技术中存在的缺陷和不足;是非常有必要的。

### 发明内容

[0006] 针对现有技术中存在的硬盘被盗窃时,无法及时通知远程监控中心采取措施,导致硬盘数据丢失的不足,本发明提供一种服务器硬盘防盗报警系统及方法,以解决上述技术问题。

[0007] 为实现上述目的,本发明给出以下技术方案:

[0008] 第一方面,本发明提供一种服务器硬盘防盗报警系统,包括:

[0009] 用于监测防盗挡板在位状态信息的在位检测电路;

[0010] 所述的在位检测电路连接到微控制器;在位检测电路实时将防盗挡板的在位信息传送至微控制器;

[0011] 微控制器连接有供电模块;通过供电模块对微控制器进行供电;

[0012] 微控制器还连接有指纹识别模块和GMS模块,指纹识别模块将识别到的指纹信息传送至微控制器,GMS模块将微控制器产生的报警信号传送至后台监控中心;

[0013] 微控制器还连接有存储器。

[0014] 作为优选,所述的供电模块包括板载供电单元和蓄电池供电单元;通过提供两种供电方式,避免出现供电异常断路的情况;可用于服务器断电后此系统正常工作。

[0015] 作为优选,所述的在位检测电路设置有多个,分布在防盗挡板的周边,检测防盗挡板的在位信息;多个在位检测电路能够更加全面的监测防盗挡板的在位信息。

[0016] 作为优选,所述的微控制器采用51系列单片机控制器;开发成本低。

[0017] 第二方面,本发明提供一种服务器硬盘防盗报警方法,包括以下步骤:

[0018] S1:对防盗挡板的在位状态信息进行采集;

[0019] S2:对采集到的在位状态信息进行处理,如果在位状态信息正常,则不进行任何操作,如果在位状态信息异常,则转到步骤S3;

[0020] S3:判断在位状态信息异常是否属于服务器例行检查的情况,如果是则不进行报警操作,否则向远程控制中心发送报警信号;

[0021] 所述步骤S3中通过指纹识别模块识别操作人员指纹,如果指纹识别正确,则认定属于服务器例行检查。

[0022] 作为优选,所述步骤S1中,通过多路在位检测电路对防盗挡板的在位状态信息进行监测;多个在位检测电路能够更加全面的监测防盗挡板的在位信息。

[0023] 作为优选,所述步骤S3中,通过短信发送方式向远程控制中心发送报警信号;数据传输安全及时。

[0024] 本发明的有益效果在于,对硬盘状态进行实时监控,当发生盗窃事件时,可及时通知远程用户,为追回数据提供宝贵时间。此外,本发明设计原理可靠,结构简单,具有非常广泛的应用前景。

## 附图说明

[0025] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,对于本领域普通技术人员而言,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0026] 图1是本发明提供了一种服务器硬盘防盗报警系统的结构原理图。

[0027] 图2是本发明提供了一种服务器硬盘防盗报警方法的流程图。

[0028] 其中,1-在位检测电路,2-微控制器,3-供电模块,4-指纹识别模块,5-GMS模块,6-台监控中心,7-存储器,31-板载供电单元,32-蓄电池供电单元。

## 具体实施方式

[0029] 为了使本技术领域的人员更好地理解本发明中的技术方案,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都应当属于本发明保护的范围。

[0030] 实施例1:

[0031] 如图1所示,本实施例提供了一种服务器硬盘防盗报警系统,包括:

[0032] 用于监测防盗挡板在位状态信息的在位检测电路1;所述的在位检测电路1设置有多,分布在防盗挡板的周边,检测防盗挡板的在位信息;多个在位检测电路能够更加全面的监测防盗挡板的在位信息。

[0033] 所述的在位检测电路连接到微控制器2;所述的微控制器22采用51系列单片机控制器;开发成本低。在位检测电路实时将防盗挡板的在位信息传送至微控制器;

[0034] 微控制器2连接有供电模块3;通过供电模块3对微控制器2进行供电;所述的供电模块3包括板载供电单元31和蓄电池供电单元32;通过提供两种供电方式,避免出现供电异常断路的情况;可用于服务器断电后此系统正常工作。

[0035] 微控制器2还连接有指纹识别模块4和GMS模块5,指纹识别模块4将识别到的指纹信息传送至微控制器2,GMS模块5将微控制器2产生的报警信号传送至后台监控中心6;

[0036] 微控制器2还连接有存储器7。存储器7中存储有预存指纹数据信息,指纹识别模块读取到指纹后,传送至微控制器;微控制器调取存储器中预存指纹数据信息进行比对,如果与存储器中的指纹数据信息吻合,则认为属于服务器例行检查;不进行报警操作。

[0037] 如图2所示,本实施例提供一种服务器硬盘防盗报警方法,包括以下步骤:

[0038] S1:对防盗挡板的在位状态信息进行采集;通过多路在位检测电路对防盗挡板的在位状态信息进行监测;多个在位检测电路能够更加全面的监测防盗挡板的在位信息。

[0039] S2:对采集到的在位状态信息进行处理,如果在位状态信息正常,则不进行任何操作,如果在位状态信息异常,则转到步骤S3;

[0040] S3:判断在位状态信息异常是否属于服务器例行检查的情况,如果是则不进行报警操作,否则向远程控制中心发送报警信号;通过短信发送方式向远程控制中心发送报警信号;数据传输安全及时。

[0041] 所述步骤S3中通过指纹识别模块识别操作人员指纹,如果指纹识别正确,则认定属于服务器例行检查。

[0042] 尽管通过参考附图并结合优选实施例的方式对本发明进行了详细描述,但本发明并不限于此。在不脱离本发明的精神和实质的前提下,本领域普通技术人员可以对本发明的实施例进行各种等效的修改或替换,而这些修改或替换都应在本发明的涵盖范围内/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。

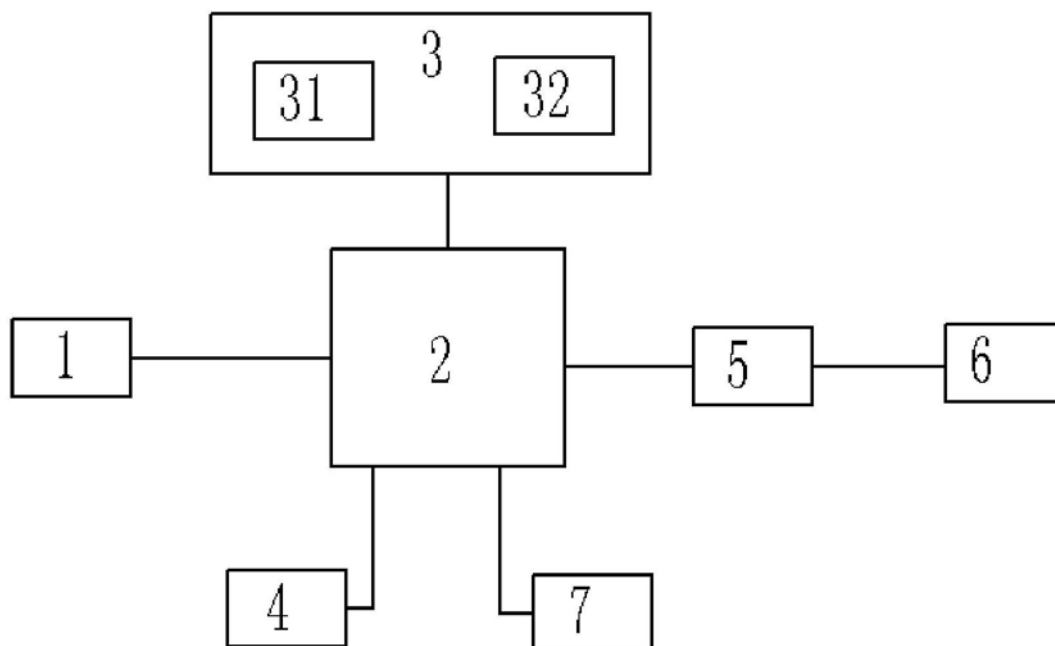


图1

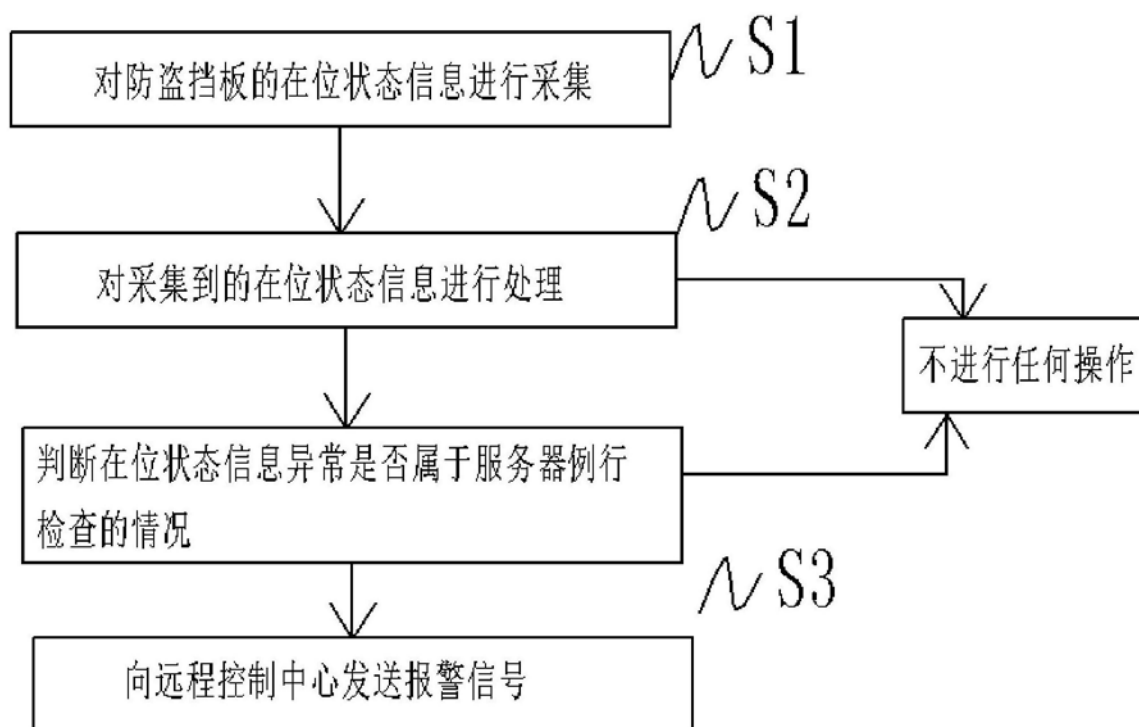


图2