(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 105119917 B
(45)授权公告日 2018.03.06

(21)申请号 201510516458.7

(22)申请日 2015.08.21

(65)同一申请的已公布的文献号
申请公布号 CN 105119917 A

(43)申请公布日 2015.12.02

(73)专利权人 福建天晴数码有限公司
地址 350000 福建省福州市开发区星发路8号

(72)发明人 陈丛亮 刘德建 毛新生

(74)专利代理机构 福州市博深专利事务所(普通合伙) 35214
代理人 林志峥

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 102129469 A,2011.07.20,
CN 102882974 A,2013.01.16,
CN 102737119 A,2012.10.17,
US 2014181517 A1,2014.06.26,

审查员 马欣

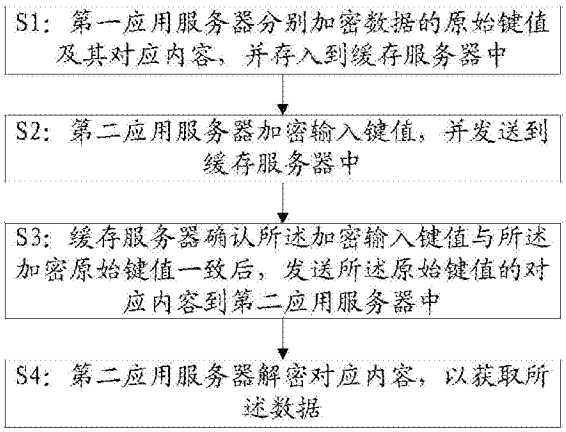
权利要求书1页 说明书4页 附图3页

(54)发明名称

增强数据安全性的方法及系统

(57)摘要

本发明公开了一种增强数据安全性的方法及系统,其中方法包括:S1:第一应用服务器分别加密数据的原始键值及其对应内容,并存入到缓存服务器中;S2:第二应用服务器加密输入键值,并发送到缓存服务器中;S3:缓存服务器确认所述加密输入键值与所述加密原始键值一致后,发送所述原始键值的对应内容到第二应用服务器中;S4:第二应用服务器解密对应内容,以获取所述数据。通过上述方式,本发明能够加强现有缓存服务器数据的安全性,避免数据缓存时被泄露。



CN 105119917 B

1.一种增强数据安全性的方法，其特征在于，包括：

S1：第一应用服务器分别加密数据的原始键值及其对应内容，并存入到缓存服务器中；

S2：第二应用服务器加密输入键值，并发送到缓存服务器中；

S3：缓存服务器确认所述加密输入键值与所述加密原始键值一致后，发送所述原始键值的对应内容到第二应用服务器中；

S4：第二应用服务器解密对应内容，以获取所述数据；其中，步骤S1具体为：

S11：根据数据，设置对应的缓存服务器节点；

S12：第一应用服务器通过AES加密算法加密数据的原始键值及其对应内容；

S13：第一应用服务器推送原始键值及其对应内容到对应节点的缓存服务器中存储。

2.根据权利要求1所述增强数据安全性的方法，其特征在于，步骤S13之后，还包括：

S14：修改所述数据；

并根据修改后的数据，执行步骤S11。

3.根据权利要求1所述增强数据安全性的方法，其特征在于，其中步骤S2具体为：

S21：第二应用服务器获取用户输入键值的指令；

S22：第二应用服务器通过AES加密算法加密输入键值，并发送到缓存服务器中。

4.根据权利要求1所述增强数据安全性的方法，其特征在于，步骤S4具体为：

S41：第二应用服务器通过AES解密算法解密对应内容，以获得所述数据。

5.一种增强数据安全性的系统，其特征在于，包括：第一应用服务器、缓存服务器及第二应用服务器；并执行如下步骤：

S1：第一应用服务器分别加密数据的原始键值及其对应内容，并存入到缓存服务器中；

S2：第二应用服务器加密输入键值，并发送到缓存服务器中；

S3：缓存服务器确认所述输入键值与所述原始键值一致后，发送所述原始键值的对应内容到第二应用服务器中；

S4：第二应用服务器解密对应内容，以获取所述数据；其中，步骤S1具体为：

S11：根据数据，设置对应的缓存服务器节点；

S12：第一应用服务器通过AES加密算法加密数据的原始键值及其对应内容；

S13：第一应用服务器推送原始键值及其对应内容到对应节点的缓存服务器中存储。

6.根据权利要求5所述增强数据安全性的系统，其特征在于，步骤S13之后，还包括：

S14：修改所述数据；

并根据修改后的数据，执行步骤S11。

7.根据权利要求5所述增强数据安全性的系统，其特征在于，其中步骤S2具体为：

S21：第二应用服务器获取用户输入键值的指令；

S22：第二应用服务器通过AES加密算法加密输入键值，并发送到缓存服务器中。

8.根据权利要求5所述增强数据安全性的系统，其特征在于，步骤S4具体为：

S41：第二应用服务器通过AES解密算法解密对应内容，以获得所述数据。

增强数据安全性的方法及系统

技术领域

[0001] 本发明涉及计算机缓存技术领域，尤其是涉及一种增强数据安全性的方法及系统。

背景技术

[0002] 目前，计算机技术人员使用分布式缓存是为了提高多台应用服务器的响应速度。但是，在内存没有加密的情况下，将会导致系统其他进程可以容易获取到内存内的敏感数据。

[0003] 现有专利(申请号：201310746988.1)公开了一种分布式缓存的方法和系统，该方法包括：分布式缓存系统获取业务应用的数据操作请求，并根据该数据操作请求指示操作数据的键值通过哈希运算得到对应该数据的虚拟队列vBucket的标识信息；获取该vBucket标识信息与缓存服务节点的对应关系，并根据该对应关系确定该vBucket标识信息对应的第一缓存服务节点，将该数据操作请求分配到该第一缓存服务节点进行相应的数据操作。该专利可以提高缓存访问数据的速度，但是没有对数据进行加密。

发明内容

[0004] 本发明所要解决的技术问题是：加强现有缓存服务器数据的安全性，避免数据缓存时被泄露。

[0005] 为了解决上述技术问题，本发明采用的技术方案为：提供一种增强数据安全性的方法，包括如下步骤：

[0006] S1：第一应用服务器分别加密数据的原始键值及其对应内容，并存入到缓存服务器中；

[0007] S2：第二应用服务器加密输入键值，并发送到缓存服务器中；

[0008] S3：缓存服务器确认所述加密输入键值与所述加密原始键值一致后，发送所述原始键值的对应内容到第二应用服务器中；

[0009] S4：第二应用服务器解密对应内容，以获取所述数据。

[0010] 为解决上述问题，本发明还提供一种增强数据安全性的系统，包括：第一应用服务器、缓存服务器及第二应用服务器；并执行上述步骤。

[0011] 本发明的有益效果在于：区别于现有技术，本发明分别加密数据的键值及其对应内容，并存入缓存服务器中，在读取时，加密输入键值，并比对一致后，将内容解密以获取数据。通过上述方式，本发明可以加强现有缓存服务器数据的安全性，避免数据缓存时被泄露。

附图说明

[0012] 图1为本发明方法实施例一的流程示意图；

[0013] 图2为本发明方法实施例二的流程示意图；

[0014] 图3为本发明系统实施例三的结构框图。

具体实施方式

[0015] 为详细说明本发明的技术内容、所实现目的及效果，以下结合实施方式并配合附图予以说明。

[0016] 本发明最关键的构思在于：分别加密数据的键值及其对应内容，并与加密输入键值比对一致后，进行解密以获取数据。

[0017] 请参照图1，本发明实施例一提供一种增强数据安全性的方法，包括如下步骤：

[0018] S1：第一应用服务器分别加密数据的原始键值及其对应内容，并存入到缓存服务器中；

[0019] S2：第二应用服务器加密输入键值，并发送到缓存服务器中；

[0020] S3：缓存服务器确认所述加密输入键值与所述加密原始键值一致后，发送所述原始键值的对应内容到第二应用服务器中；

[0021] S4：第二应用服务器解密对应内容，以获取所述数据。

[0022] 区别于现有技术，本发明分别加密数据的键值及其对应内容，并存入缓存服务器中，在读取时，加密输入键值，并比对一致后，将内容解密以获取数据。通过上述方式，本发明可以加强现有缓存服务器数据的安全性，避免数据缓存时被泄露。

[0023] 如图2所示，在实施例一的基础上，本发明实施例二在执行步骤S1时，具体为：

[0024] S11：根据数据，设置对应的缓存服务器节点；

[0025] S12：第一应用服务器通过AES加密算法加密数据的原始键值及其对应内容；

[0026] S13：第一应用服务器推送加密原始键值及其加密对应内容到对应节点的缓存服务器中，以存储。

[0027] 其中，步骤S13之后，还包括：

[0028] S14：修改所述数据；并根据修改后的数据，执行步骤S11。

[0029] 其中在执行步骤S2时，具体为：

[0030] S21：第二应用服务器获取用户输入键值的指令；

[0031] S22：第二应用服务器通过AES加密算法加密输入键值，并发送到缓存服务器中。

[0032] 其中在执行步骤S4时，具体为：

[0033] S41：第二应用服务器通过AES解密算法解密对应内容，以获得所述数据。

[0034] 区别于现有技术，本发明根据数据特性，设置对应的缓存服务器节点，以方便后续读取操作，在加密数据的键值及其对应内容后，对应存入各自节点；并使用AES算法进行加解密。使得操作便捷，并加强现有缓存服务器数据的安全性，避免数据缓存时被泄露。

[0035] 具体地，本发明所述的缓存服务器可以是分布式缓存服务器。分布式缓存服务器中的每台服务器均视为节点，而且可根据实际情况，进行区分、编号等。如需要存储联系人的手机号码，可以根据联系人的姓氏首字母进行归类，即可以A字母开头的姓氏，归类存储到缓存服务器的第一节点；以B字母开头的姓氏，归类存储到缓存服务器的第二节点，以此类推。

[0036] 本发明在对数据的键值及其对应内容加密或解密时，可采取现有技术已知的加解密算法，如AES算法等。本领域技术人员可根据实际情况、自身偏好选择适合的算法，只要可

实现上述功能即可，此处不再赘述。

[0037] 为方便在分布式缓存服务器中调用数据，在根据数据设置对应节点后，第一应用服务器推送加密后的键值及其对应内容到各自的节点上，以存储。表1是本发明存储结果的其中一种表现形式。

[0038] 表1：键值-内容存储示意表。

[0039]

键值	内容
加密键值1(解密后为key_12)	加密内容1(解密后为abc)
加密键值2(key_15)	加密内容2(abc2)
加密键值3(key_30)	加密内容3(abc3)

[0040] 本发明分别对键值及其对应内容加密，是根据缓存的特性，利用hash算法可以快速定位到数据，不会因为加密后导致定位熟读下降，进而影响读取速度。

[0041] 目前，分布式缓存服务器一般都已经实现此功能，通过键值快速查询内容，从而避免遍历所有数据，只需要对键值进行hash后，找到相同hash的若干个键值，然后逐一比较键值即可。

[0042] 在读取数据时，需要输入键值，这里输入的键值也需要加密，加密算法同上。缓存服务器比对输入键值与原始键值，若一致，则直接发送数据给用于读取的第二应用服务器使用，第二应用服务器可以是不同于存储时的第一应用服务器，也可以是同一服务器的两个服务端口，或者是同一应用服务器。

[0043] 如：用户访问应用服务器获取key_12对应内容，则先使用AES加密算法，对key_12加密，得到加密键值1，放入缓存服务器获取到加密内容1，然后解密后输出返回给用户。

[0044] 若第二应用服务器出现修改数据时，第二服务器访问分布式缓存服务器时，需对应修改加密后的键值及其加密后的内容为修改后的最新键值及其内容，该操作类似计算机操作时，对文档的覆盖或替换。

[0045] 如：在数据有改动时，应用服务器加密键值key_12生成加密键值1，通过加密键值1修改分布式缓存服务器上所有节点的内容为加密后的内容2(abc2)给之后所有应用服务器访问。

[0046] 如图3所示，本发明实施例三还对应提供一种增强数据安全性的系统100，包括：第一应用服务器110、缓存服务器120及第二应用服务器130；并执行如下步骤：

[0047] S1：第一应用服务器110分别加密数据的原始键值及其对应内容，并存入到缓存服务器120中；

[0048] S2：第二应用服务器130加密输入键值，并发送到缓存服务器120中；

[0049] S3：缓存服务器120确认所述输入键值与所述原始键值一致后，发送所述原始键值的对应内容到第二应用服务器130中；

[0050] S4：第二应用服务器130解密对应内容，以获取所述数据。

[0051] 其中，步骤S1具体为：

[0052] S11：根据数据，设置对应的缓存服务器节点；

[0053] S12：第一应用服务器110通过AES加密算法加密数据的原始键值及其对应内容；

[0054] S13：第一应用服务器110推送原始键值及其对应内容到对应节点的缓存服务器

120中，以存储。

[0055] 其中，步骤S13之后，还包括：

[0056] S14：修改所述数据；

[0057] 并根据修改后的数据，执行步骤S11。

[0058] 其中，步骤S2具体为：

[0059] S21：第二应用服务器130获取用户输入键值的指令；

[0060] S22：第二应用服务器130通过AES加密算法加密输入键值，并发送到缓存服务器中。

[0061] 其中，步骤S4具体为：

[0062] S41：第二应用服务器130通过AES解密算法解密对应内容，以获得所述数据。

[0063] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等同变换，或直接或间接运用在相关的技术领域，均同理包括在本发明的专利保护范围内。

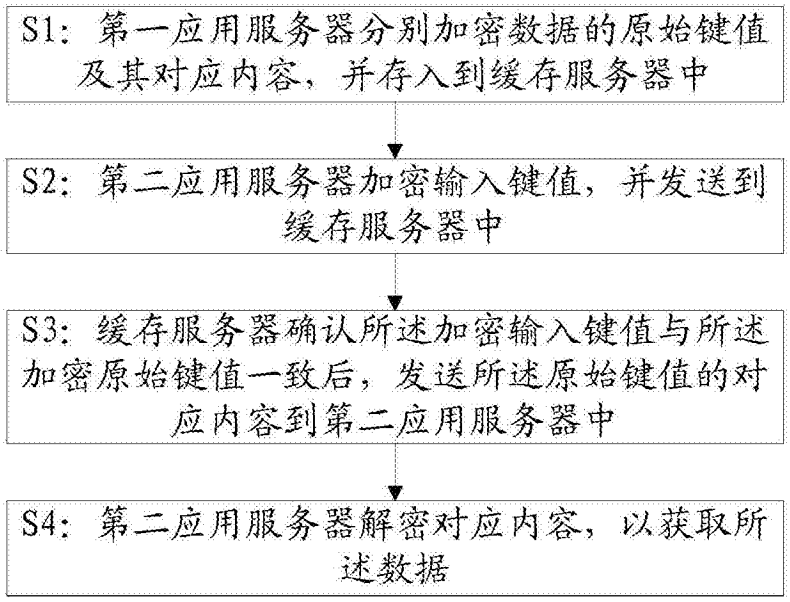

S1：第一应用服务器分别加密数据的原始键值及其对应内容，并存入到缓存服务器中
S2：第二应用服务器加密输入键值，并发送到缓存服务器中
S3：缓存服务器确认所述加密输入键值与所述加密原始键值一致后，发送所述原始键值的对应内容到第二应用服务器中
S4：第二应用服务器解密对应内容，以获取所述数据

图1

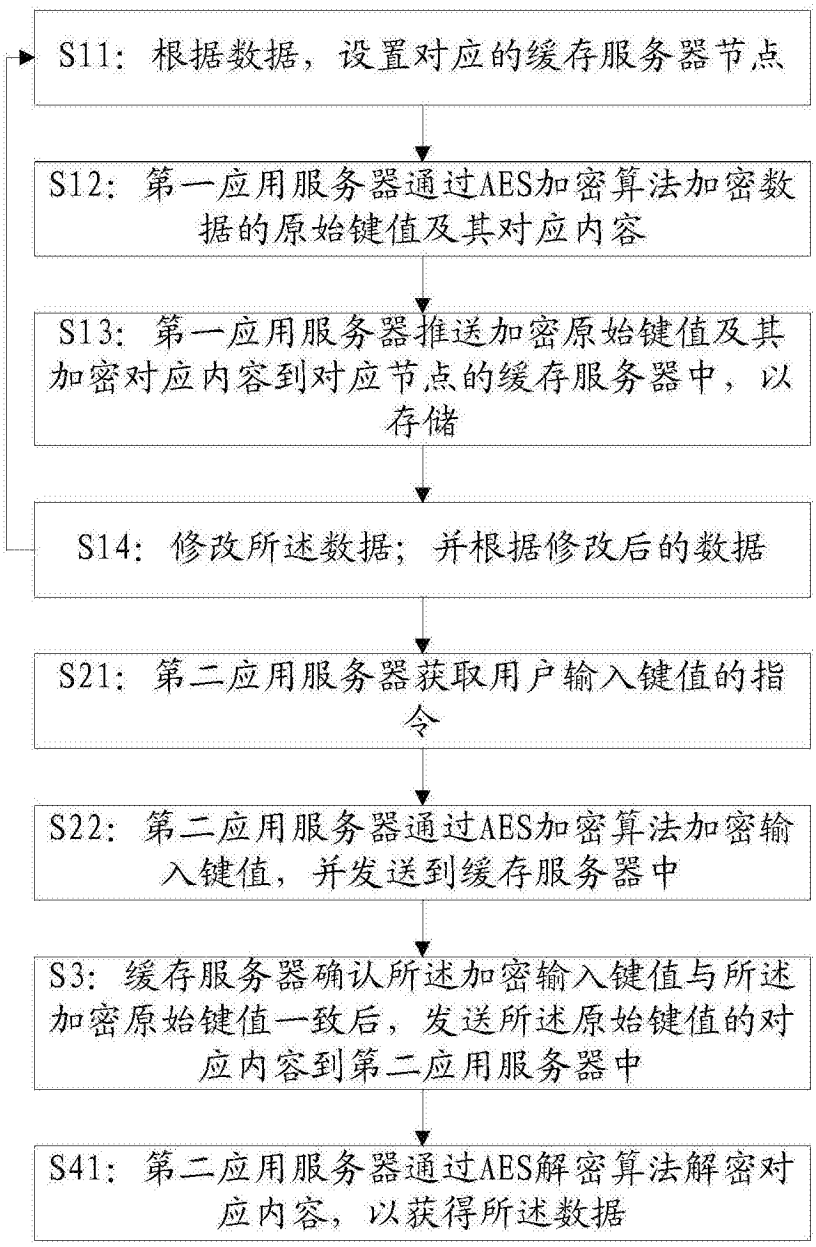

S11：根据数据，设置对应的缓存服务器节点
S12：第一应用服务器通过AES加密算法加密数据的原始键值及其对应内容
S13：第一应用服务器推送加密原始键值及其加密对应内容到对应节点的缓存服务器中，以存储
S14：修改所述数据；并根据修改后的数据
S21：第二应用服务器获取用户输入键值的指令
S22：第二应用服务器通过AES加密算法加密输入键值，并发送到缓存服务器中
S3：缓存服务器确认所述加密输入键值与所述加密原始键值一致后，发送所述原始键值的对应内容到第二应用服务器中
S41：第二应用服务器通过AES解密算法解密对应内容，以获得所述数据

图2

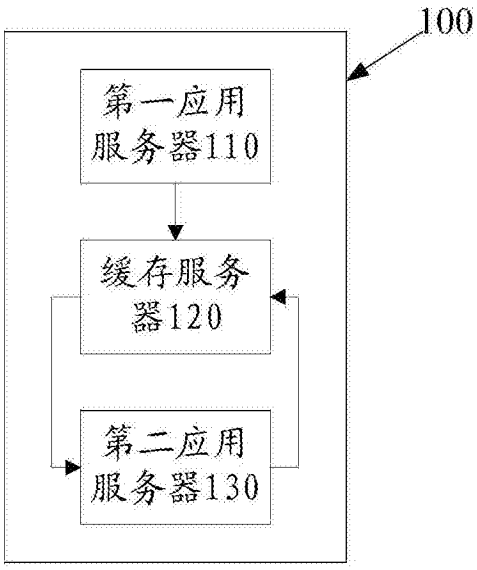


图3