**会议审稿模板**

\***Overall recommendation(总评) ：**

3 (Strong Accept)  (only for best paper candidate)

2 (Accept)  (support to accept)

1 (Weak Accept) (inclined to accept)

0 (Borderline/Neutral)  (either accept or not accept is fine)

-1 (Weak Reject)  (has some weaknesses, not fatal)

-2 (Reject) (fundamental error, not recommend to publish)

-3 (Strong Reject) (only for Plagiarism or faked paper)

\***Strong Points （优点）：**

请分条列出论文的优点。包括论文选题是否实际、论文贡献是否突出、是否有足够的创新点、所提出的技术的应用性如何、论文写作水平如何、实验做的是否扎实等方面的考量。

1. 本文解决了存储卷烟销售数据云平台不可信时，面临的数据血缘关系篡改问题，通过代理重签名，还可以使得用户的认证信息不直接暴露在云平台之下，具有实际意义。
2. 贡献较为突出，综述方面都没有人兼顾在外包云数据服务中心场景下数据血缘分析的高效性和安全性。
3. 创新点在加密算法方面表现充足，但对于细粒度还缺乏解释。
4. 可以实际运用于有关系统，实验的对照方法缺乏介绍。

\***Weak Points（缺点）：**

请分条列出至少5个缺点。

1. 在3.1和3.2中分别对比了两种方法Hybrid Attribute和CloudSafetyNet这两种方法均没有在之前的相关工作中介绍，此前可以详细介绍。
2. 在3.1中CloudSafetyNet的实验结果与本文的方法特别接近，本文却没有分析原因。
3. 本文的内容主要描述了“基于代理重签名的算法血缘安全分析”，并没有明显体现“细粒度”。
4. 本文的综述部分缺乏逻辑，且关联性较弱。
5. 图五在数据达到300时有更高的斜率，在更高的数据量时可能算法的复杂度有剧烈变化。

\***Detailed Comments ：**

请对论文进行总结，包括选题是否结合实际是否先进？解决方案是怎么样的，解决方案是否有一定创新性？实验结论如何？

本文解决了存储卷烟销售数据云平台不可信时，面临的数据血缘关系篡改问题，并提出了两种使用血缘关系信息进行代理重签名的算法，使用户的认证信息不必暴露在云平台之下。

从综述看，本文是首次关注卷烟销售领域分析数据血缘关系的问题，具有创新性。

实验参照对比方法具有更好地效率，证明了优越性。