跨域多节点云平台安全访问通道加密技术研究

黄 翔 莫剑锋 黄信信 孙宇宁 刘慧航

（南方电网数字平台科技（广东）有限公司）

摘要：基于云端计算信息操作机制的转型调整，很多企业将应用领域的环境实施全方位的转化升级和系统管理，同时依托于云端共享平台的工作联动，让不同应用域之间的工作访问联动，可以在必要的情况下完成跨域访问操作。当前主流的应对方案就是综合跨域多节点云平台安全访问通道加密技术，从云平台的安全访问环境，构建出系统全面的保密沟通体系，要力争工作效果符合现代工作的需求。为此本文结合跨域多节点云平台安全访问通道加密技术的特点，从其实现的方式和应对的作业点实际情况的角度进行分析，提出专项的服务工作措施和市场发展的前景，以推动数据信息的安全存储，提升管理合力，保证在现有工作机制下跨域多节点云平台安全访问通道加密技术适应工作基础调节，保证网络安全。

关键词：跨域；多节点；安全访问

互联网产业的高速发展，为人们高效的通信交流以及资源访问得到了便利保障，但是实际的信息网络安全问题也变得尤为严峻，在对网络环境中如何有效控制非法的访问以及敏感信息的控制本身就是一个较为严重的个人安全风险问题。当前在网络环境的支持下，网络建设安全问题已经成为人们在进行网络管理的过程中所面临的核心问题。随着云计算的高度发展，跨域多节点云平台安全访问通道加密技术的应用逐渐地广泛，为了有效地加快访问的控制管理，就需要现有的管理人员在现有的应用管理环境下，加快访问资源的判断，分析何种访问资源可以实现访问工作的落实。而跨域多节点云平台安全访问通道加密技术的提出，则能直观的反映出云端处理工作的有效性，加快技术的产业分析，保证最佳的服务工作效果。

一、关键技术分析

1、跨域单点登录

现阶段的技术手段可以在当前的管理机制下，将跨域单点登录的操作机制划分为两种不同的操作机制。一是以经纪人为基础的核心单点登录机制，这种方式的出现主要是需要依托于一个中央的能够控制操作和安全管理信息用户，作为集中地用户认证体系以及账号信息管理工作模式，在这种操作机制下所实现的中央认证的安全管理操作模式，有效的减少了原有的管理工作任务负担，多数都是将其作为一个单独与市场管理门户，实现直接登录的第三方操作机制，也就是我们在安全操作管理任务中所提及的经纪人。

为了保证安全登录的效果，此方式下完成的单点登录机制，首先在现有的资源访问管理机制前期，客户端首先要有效的分析判断服务器工作机制，做好身份信息的确认和判断，为了保证安全管理工作任务的推进，可以在客户端的选择以及服务器的任务落实的基础上做好内部通道的分析和判断。其次用户在实际的认证工作完成之后，会在通路的安全管理基础上，发送代表用户身份的安全信息指标信号。最后在实际的工作中用户在明确安全身份信息之后，做好访问数据的传送，就能达到单点登录的目标要求。

当客户端的服务设备向服务器终端之间进行请求，请求数据必然会直接被定向到认证服务端端口，当认证服务器在完成用户数据分析后，会通过安全通道，将数据信息传输到客户端信号之中，通过认证后，服务器的工作模式会重新的被定向到服务器之中。其次用户方位其他的服务器过程中，也会被重新认证到服务器的终端上，只要使用者在使用工作的前期已经在服务器端口完成安全信号的传输，在完成认证的过程中就可以被直接重新的定地到整个应用的服务端之中。

2、非对称加密技术

为保证跨域多节点云平台安全访问通道加密技术的工作效果，达到最佳的安全工作效率，就需要在现有的工作机制中，对于相关的信息数据进行管理分析和工作模式的创新，完成数据的统筹规划和工作模式的协调。依托于公共钥匙密码的运行操作体系，讲述信息的加密操作能力与通道环境下的数据解密能力之间进行拆分，形成不同的工作体系和操作管理机制。这种密钥的工作方式的特点就是自爱加密算法的基础上以及加密秘钥的实际操作之中，进一步的判断整个访问通道环境是否安全合理。

现阶段我们所提及的跨域多节点云平台安全访问通道加密技术，就是在当前的工作环境下，基于结构特征形成单向的陷门函数，而不是在普通的加密算法基础上，综合通道环境特征构建出一种特殊的非对称加密技术。单向陷门函数简约来说就是在一个环境中集合与集合之间的映射，这种形式出现的表达状态是非对称性的，可以适应不同环境下的安全访问的渠道环境特点和工作机制。跨域多节点云平台安全访问通道加密技术操作机制本身的工作机密性较强，可以有效地防止敏感信息出现

泄露的情况，在这种机制下可以通过数字签名的方式确保相关的数据信息来源的精准性。

二、跨域多节点云平台安全访问通道加密技术背景分析

跨域多节点云平台安全访问通道加密技术是现行我国网络环境通路结构上的一种基础的工作管理标准技术，而跨域多节点云平台安全访问通道加密技术手段主要是在现有的工作机制下，将各种原有的数字信号数据与文本信息资料的进一步调节，形成不同管理操作机制下，就要传输成为不同的信号过程，在网络通路之间的连接加密操作机制，消息传输和网络流转的过程中保证加密管理。将信息数据从节点加密管理以及技术的转换之后，形成特定加密算法的信息管理，就是要加快用户之间的交换数据传输转型。多数来说就是要在通路结构上做好路径的选择分析和描述规划。

安全访问通道的加密处理就是要在物理管控条件下实现数据连接，做好数据的加密管理工作落实，接收管理人员就是要在传输路径之中，对于不同的节点及其进行传输分析，其以此解密的每一个节点操作的计算机管理信息数据，然后传达到目的地位置之中。加密操作管理的方式必须要完成高效的加密处理才能实现，这种操作下的加密操作方式的实现高效性可以满足服务需求，在不同的节点传输之间的线路间，需要安装相关的跨域多节点云平台安全访问通道加密技术支撑设备，依托于相同的秘钥信息，保证加密设备以及加密功能的实现，以保证线路上可以完成加密处理，保证网络的安全性效果。

跨域多节点云平台安全访问通道加密技术对于用户来说是高效公开的，换言之网络可以实现自行执行操作的，同时用户不会影响加密工作的有效开展。这种加密方式的实现就是要在物理工作机制下进行执行的，主要的操作就是在硬件设备中实现操作的，其本身可以保证通道的安全性。

三、跨域多节点云平台安全访问通道加密技术实施

1、链路加密

在现有的网络环境中的一个节点上的通信链路结构，工作有效性较高，而链路的加密只要保证网络传输结构主体安全运作，就能确保方位的质量。在跨域多节点云平台安全访问通道加密技术操作的过程中，所有的消息都是需要在传输的前期完成加密处理，在每一个网络节点环境下，对不同的信息数据进行解密处理，之后在使用下一阶段的联系后完成加密调节，再实现传输操作。在到达既定的目的之后，一个信息数据需要通过多链路之间的传输操作。

由于不同的中间传输介质的信息数据在解密之后需要被重新的加密处理，所有的信息数据都要在现有的链路结构主体上将所有的数据的密文形式进行展现。这种形式下链路的加密机制最终限制了传输的信息来源，因为填充技术的使用以及字符的出现不需要在数据传输的方式下就可以完成加密，这就导致信号的频率得到延时，可以有效的防止通信业务信息的出现。

虽然链路结构加密模式在计算机网络工作中的使用广泛性较高，因此本身并未形成任何矛盾问题。在链路结构的加密限制影响下，要求链路内的加密设备进行协同操作，之后利用一种链路模式对链路的传输数据进行加密管控。这种机制下就为链路结构主体上集中进行协调和传输产生影响，继而导致信息数据的丢失。另外即使一小部分的数据需要进行加密，也会让所被传输的信号数据出现加密反应。

在一个网络节点环境下，链路的加密只是为了给通信的链路结构提供安全保证，让信息数据以明文的方式呈现。但是在现有的工作机制下，需要保证现有每一个节点环境下的安全性的工作费用较高，因此就需要在跨域多节点云平台安全访问通道加密技术推进执行的基础上，加快硬件设施管理以及安全物理环境的综合协调。为保证安全策略的推进执行，既需要做好数据观察，以防止因为安全问题导致保险的费用增加。在传统的加密算法中。所属需要使用秘钥的操作，以保证通路的安全性，但随着跨域多节点云平台安全访问通道加密技术的有效使用，解决了现行链路加密工作中所出现的访问困难的情况，因为每一项的安全管理工作机制都不许在不同的节点存储一定的加密措施信号，这样既需要对秘钥进行物理的传输，也要保证有具体的网络环境保证跨域多节点云平台安全访问通道加密技术的应用，以更好实现秘钥的连续分配工作效果。

2、节点加密处理

虽然在跨域多节点云平台安全访问通道加密技术的应用过程中，对于节点有了较为精细化的管理，也能为网络数据提供一定的安全保障，但是在具体的操作管理机制上，其本身的安全管控与链路加密机制相类似，其本身都需要在通信链路上位传输的信息数据提供安全支撑，在不同的中间接电线对消息进行解密操作，在通过跨域多节点云平台安全访问通道加密技术对于数据进行加密。因为 IE 要对所有的数据信息完成加密处理，因此数据的加密过程都是公开的。但是与链路加密操作有所差异的是，在跨域多节点云平台安全访问通道加密技术操作中，节点的加密不允许消息数据在节点操作中以明文的表现方式所存在，它更多地就是将受到的信息进行解密处理。这一过程就是在节点操作的安全模块环境下进行执行。节点加密要求报头以及路由信息数据以一种明文的表现方式进行传输，这一过程就是在现有节点环境下依托于安全模块机制进行工作任务的落实。这种方式对于防止攻击业务本身的有效性相对较高。

3、端口到端口间的加密

端口到端口之间的加密操作就是要保证数据信息在起点到终点的传输中都是以加密的文字形式存在，通过使用这种方式消息的传输本身在到达终点之前是不能完成解密操作的，因为信息在传输的全过程都是以被保护的方式存在的，因此即使有节点出现损坏也并不会出现信息泄露。

端口到端口的加密主要是数据从一个端点到另一个端点之间的加密管理工作，在这种解密工作机制中所有的中间节点位置都是以非明文的表现方式所呈现，因此工作过程中除却报头以外的各项数据节点都是以密文的方式呈现在整个通道环境中的，只是在发送端以及接收端才会安装解密的社诶。但是在中间的流转渠道都不会进行解密处理。为此就需要有一定密码数据信息设备，与链路结构进行相比，可以有效地减少密码的实际数量。另外信息主要是通过报头以及报文的方式呈现的，报头要以通路为主体进行选择分析，因为传输过程中需要实现路径的选择分析，在链路支架加密处理过程中，报文以及报头都需要进行加密处理操作，但是在端口到端口之间的加密管理，因为通道环境的每一个节点进行不正确的报文解密操作，但是为更好地做好报文传输操作目的，就需要做好道路环境的信息数据选择分析和传输管理。为此只能进行加密报文的处理调控，但是在实际的工作中并不可以对报头进行加密处理。这种就很容易被一些通信分析问题所发现，从而获取一些敏感的信息数据。

在现有的工作机制下为更好地发挥跨域多节点云平台安全访问通道加密技术的工作效果，就需要对道路环境进行综合分析，判断在不同的环境机制下的访问管理工作存在的多种问题，从现有的环境状态出发，对于端口与端口之间的道路位置进行综合的分析和严格的管控，提出专项的分析工作措施和管理工作机制，以跨域多节点云平台安全访问通道加密技术我 IE 支撑加快技术优化，在保证现行各项数据精准高效传输的同时，确保信息的安全性和有效性。

总结：基于云计算工作机制的发展，新兴的跨域多节点云平台安全访问通道加密技术的综合应用，而区块链网络环境下所构建的加密技术手段，实现了数据存储、点对点传输、共享机制、加密算法等不同计算机技术的新型应用模式探索，在各领域中都得到了全面的应用，其本身的分布式数据存储都需要综合当前的安全管理工作机制对其进行影响分析，让其可以在点对点的通道环境内保证数据的高效联动流通模式，公式机制的出现导致节点之间的工作量可以快速校验，而加密算法的出现，也保证了数据存储的安全性。因此这些特点让区块链可以在现有的信息安全保密管理机制下，支撑跨域多节点云平台安全访问通道加密技术的推进，保证信息数据的安全性。

参考文献：

[1]袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报.2016,(4).DOI:10.16383/j.aas.2016.c160158.

[2]李凤华,苏锟,史国振,等.访问控制模型研究进展及发展趋势[J].电子学报.2012,(4).DOI:10.3969/j.issn.0372-2112.2012.04.030.

[3]林利,石文昌.构建云计算平台的开源软件综述[J].计算机科学.2012,(11).DOI:10.3969/j.issn.1002-137X.2012.11.001.

[4]倪力舜.基于联邦的跨域身份认证平台的研究[J].电脑知识与技术.2011,(1).53-55.

[5]邓昀,程小辉.移动跨域单点登录系统设计[J].计算机工程与设计.2010,(8).