计算机网络通信安全中数据加密技术分析

丁 然*
南京机电职业技术学院，江苏 211135

摘 要：在社会经济不断发展的过程中，我国的科技研发水平，也在不断地提高。当前计算机网络技术的应用范围，变得越来越广，对居民的日常生产生活，产生了巨大的影响。但是计算机网络技术在发展时，因为网络的过度开放等问题。导致居民在获取大量的数据信息资源时，会遭受信息数据的窃听和盗取等问题。导致网络环境的安全问题，变得更加严重，而且引起了社会各界人士的广泛关注。所以，在进行计算机网络通信技术应用时，必须保证技术的应用安全，通过数据加密等技术的应用，营造一个更加安全的网络环境。本文就计算机网络和通信安全中的数据加密技术应用进行相关的分析和探讨。

关键词：计算机网络；通信安全；数据加密技术；分析探讨

一、前言

现阶段计算机网络技术，已经渗透到我国居民生产生活的各个方面。但是相关技术在应用时。面临较多的安全性问题。当前在进行技术研发时，数据加密技术的应用属于保护计算机网络和通信安全的重要方式。所以这项技术的应用价值，非常的高，可以对网络环境中的安全性问题，进行有效地解决。数据加密技术在应用时。加密方式比较特殊，而且技术的应用，存在不同的形式。所以，相关人员在进行这项技术研究时，必须对技术的特点，进行深入的了解。才能准确地把握技术的应用形式，确保技术在应用时，能够发挥更大的作用，提高计算机网络通信技术应用的安全性[1]。

二、数据加密技术应用特点

当前在进行数据加密型技术应用时，存在对称性的加密方法。这种技术可以应用到明文的转换过程中，只需要借助相关的公式和算法内容，就可以完成数据信息的加密储存。在进行数据信息的加密和解密时，所应用的公式和算法是一样的，这种数据加密技术在应用时，存在一定的安全隐患问题。因为一旦公式和算法被泄露，那么这项技术就会被破解，在应用时会出现更多的问题。在进行这种加密技术应用时，可以将原文按照一定的算法，转换为没有具体规律的数据和信息组。在加入密钥内容之前，就要将这些数据和信息分为两组。所有的数据、信息组和密钥内容，都要在函数公式的计算下结合到一起，最终的原文会以加密的形式重现出来。所以这项技术在应用时，存在一定的安全性，但是只要公式被泄露出去，那么这种技术在应用时，会存在更多的危险性[2]。

图1 数据加密技术

如图1所示，在进行数据加密技术应用时，还存在非对称性的加密技术，这项技术可以应用到数据、信息的传递过程中，可以对加密的数据、信息进行破解。在破解时，只需要进行公钥内容的解密和私钥内容的解密。这种双重加

* **通讯作者：**丁然，1989 年 9 月，男，汉族，江苏镇江人，现任南京机电职业技术学院教师，中级教师，本科。研究方向：计算机网络技术。

密的传输方式，可以降低数据、信息泄露的概率。而且在进行这种技术应用时，加密数据和解密信息的算法公式，并不是一样的。所以，在进行技术应用时，即使加密的公式和算法泄露，也不会对数据信息的安全性，造成不利的影响。但是在进行这种技术应用时，操作速度比较低，尽管技术的应用安全性比较高，但实际操作时也存在一定的问题。所以，相关的人员在进行技术应用时，一定要提高技术的应用速度[3]。

三、计算机网络通信安全中数据加密技术的具体应用

（一）链路加密技术的具体应用

在进行这种技术应用时，主要是在某链路上，通过报文形式。进行数据信息的传递和展示。数据信息在经过某一个节点时，这一个节点的密码装置就会对数据、信息进行解密。在对报文内容进行传递开启之前，会对相关的数据、信息进行二次加密。这些数据信息在经过下一个节点时，同样可以通过密码装置，对密码进行破解。在数据、信息离开之前，也会接受下一个节点的密码加密。所以，这项技术在应用时，就是不断地对信息、数据进行加密和解密。在整个流动过程中，信息数据的总体趋势始终处于加密状态。而且整个操作流程的链路形式比较复杂，加密方式比较繁琐，所以，要对这项技术进行破解，存在一定的困难。这项技术的应用重点，就是保证所有的节点，都能加密成功，才能充分发挥技术的应用效果。一旦在技术应用的过程中，出现加密缺漏问题，就会失去作用。所以，相关人员在进行这项技术研究时，一定要对每个节点的加密方式，进行全面的了解。才能保证每个节点的加密成功，并且为下一个节点的加密操作，奠定良好的基础。在进行实际操作时，还应该对整个流程进行综合控制，才能保证整个流程连接起来。通过各个节点的连接，确保技术的应用效果，能够得到有效的提高，从而为信息技术的应用，创造一个更加安全的环境。在进行技术应用时，相关人员还要对现有的加密方式进行优化，才能保证每个节点的加密效果更佳。避免在技术应用时，出现缺漏的问题，提高技术应用的安全效果。例如某一人员在进行链路加密技术实际应用时，最初所有的链路和节点的加密效果都比较强。但在传输时遭受了外界的攻击，某一个节点的加密失效，而且对报文进行了解密。导致所有数据信息，都处于解密的状态，最终导致这项技术的应用，失去了安全作用[4]。

（二）节点加密技术的具体应用

如图2所示，在进行这项技术应用时，某一个链路中传递的信息数据在经过相应节点之前，报文一般是以明文的方式存在的。在到达这一个节点之后，报文的形式就会立即转化为加密的状态。报文中的所有数据信息首先要在这一个节点区域进行解密，然后将所有的数据信息统一置于安全的模块中，然后进行下一步的加密。信息和数据在所有的节点处，都要进行相应的加密，而且加密的程序都是一致的。相关人员在进行这项技术应用时，必须保证解密和加密，所使用的密钥存在一定的差异。要保证各个节点之间，接收到的报文数据信息，结构和设备都是一样的，才能提高数据信息传递的安全性。这项技术在具体应用时，对每个节点的管理，存在较高的要求，所以，实际应用效果并不显著。一些黑客或者病毒，都可以对数据信息，进行相应的操作，所以，这项技术应用的安全性并不高[5]。

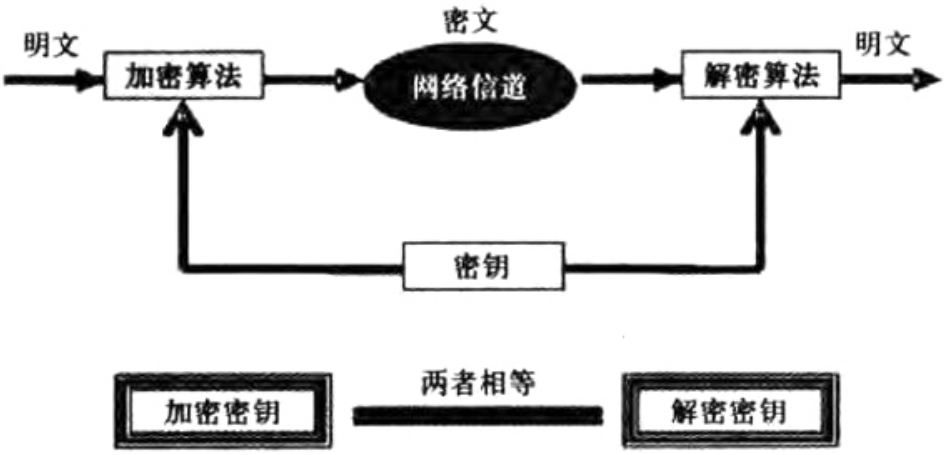

图2 明文加密

相关人员在进行技术具体应用时，应该对现有的加密方式进行改进，才能保证每个节点的管理水平，能够得到有效的提高，确保技术的应用效果更强。但是当前很多人员在进行这项技术应用时，没有认识到管理工作开展的重要性。在开展管理工作的过程中，依然存在较多的问题，导致技术的应用安全性，被大大的降低。所以，在进行这项技术应用时，一定要对管理的重点进行明确，而且要对现有的管理方式和内容进行改进，才能保证管理工作在开展时，

能够发挥更大的效用。确保技术的应用安全性，能够得到有效的提高。从而将这项技术应用到，计算机网络通信技术的各个环节中，为相关工作的开展。提供有效的支持。例如某一人员在进行这项技术应用时，虽然对节点进行了管理，但是没有严格地按照管理要求。开展相关的操作。所以，这项技术的实际应用效果，得不到有效的提高。而且在进行信息数据资源传递时，遭受了外在的攻击，一些黑客对数据信息进行了窃取。或者因为病毒的影响，导致信息数据出现了丢失等情况，最终传递出去的信息数据，不符合应用的要求。这种问题的出现，不仅会对技术的加密效果，造成不利的影响，而且无法保证相关技术的应用安全性[6]。

（三）端到端加密技术的具体应用

这项技术主要作用于，明文的加密过程中。在进行技术应用时，首先要根据信息数据接收的地址，对传递的路径进行设计。而且在传递的过程中，要始终保持明文的状态。在将数据、信息转换成加密形式的报文包之后，这个报文包无论在哪条链路和节点区域进行传递，都要始终保持加密的状态，才能提高技术应用的安全性。在传进时，无论是哪一个链路或者节点的密码装置，都不能对这种报文包进行实际解密。在进行实际传递时所经过的节点，都要依靠明文的指示进行相应的操作。才能保证最终的报文包，能够以加密的形式，到达运输的终端。端对端加密技术在应用时，可以将其作用到信息、数据加密的过程中，而且信息、数据不会存在被破解的风险，所以信息数据始终是安全的。即使是在传输的路径中，报文包存在丢失现象，或者节点出现了损坏问题，也不会对数据信息的安全性，产生较大的影响。所以这项技术的应用安全性比较高，相关人员在进行技术应用时，只要保证报文包始终处于加密的状态，就可以保证信息数据的安全[7]。

在进行这项技术应用时，只要对报文包进行严格的管理，就可以提高技术应用的安全性。所以，相关的人员，一定要对这项技术的应用形式，进行准确的把握。才能保证报文包的加密形式不会遭受破坏。例如某一人员在进行这项技术应用时，对相应的文字信息，进行了加密，将接收的地址，设定成了传递的路径。但是在实际操作时，没有将其转化为加密状态的报文包，或者在转换的过程中，出现了安全性的问题。导致报文包在传递时，出现了丢失或者被解密等情况。那么，这项技术在应用时，就存在更多的风险。而且无法保证信息数据在传递的过程中，始终处于安全的状态。如果在实际传递时，出现了信息数据的丢失情况，或者遭受了节点的破坏，就会降低信息数据应用的安全性[8]。

（四）密钥加密技术的具体应用

如图3所示，这种密钥加密技术的应用，与对称性加密技术和非对称性加密技术的应用，存在一定的联系。这项技术在应用时，相关的算法和公式，与上文的两种技术，存在相同之处。这种技术在具体应用时，存在公钥和私钥两种类型。虽然只有两种类型，在实际操作时，都会导致部分信息数据出现泄露的问题。但在实际泄露时，这些信息、数据其实是无关紧要的，大部分隐秘类型的信息、数据安全性还是比较高的。密钥加密技术在实际使用时，首先要对需要进行加密的信息、数据，按照相应的算法和公式内容进行加密的认证。后期在对信息、数据进行传递时，会经过检测系统的监控和扫描。这种操作方式，可以提高信息数据传递的安全性，但是在实际传递时，也会经历病毒木马的攻击。在受到攻击时，密钥的管理系统会制定相应的防护措施，并且对信息数据的访问形式设定严格的权限。接收人员在接收到信息数据之前，必须输入私钥的密码并且保证正确，才能获取相应的数据信息。所以，这项技术的应用，安全性也比较高。但是在实际应用时，相关人员必须保证信息数据在经历病毒的攻击时，不会泄露一些重要的数据信息。而且在进行检测系统建设时，还要对现有的系统功能进行完善，确保系统在应用时，能够发挥更大的作用，能够对一些安全性问题，进行有效的解决，才能提高技术应用的安全性。

图3 密钥加密技术

当前很多人员在进行这项技术应用时，主要对密码进行了有效的管理，必须输入正确的密码，才能获取相应的数据信息资源。例如有些人员在进行这种技术应用时，因为应用的算法和公式，存在一定的缺陷，而且公钥的密码和私钥的密码，在传递时也存在泄漏的风险，导致这项技术的应用并不安全。甚至有些人员没有认识到，密码设计的重要性。在进行密码设计时，设计的比较简单，不符合没有加密技术应用的安全性原则。导致信息数据在传输时，不仅会面临外在的攻击，而且内部的安全性，也得不到有效的提高。尤其是在经过检测系统时，会因为系统的漏洞，出现安全性的问题。管理系统也无法对这些攻击性问题，进行有效的防护。在对信息数据的访问权限进行设计时，也出现了较多的问题，导致接收人员在接收信息数据时，接收到了一些错误的信息数据，或者接收到的信息数据，存在丢失等问题。这些问题的出现，都会降低技术应用的安全效果，而且不利于技术的发展成熟。

（五）数字签名认证加密技术的具体应用

接收人员在获取数据信息之前，要对这些数据信息进行解密，在解密时首先要经历信息的采集和计算等阶段，要保证相关的算法在应用时能够和函数保持一致。在将信息数据的摘要类型计算出之后，通过数字的形式，对数据信息进行获取。在对这些数字信息进行接收时，要发送个人认证，或者用密钥进行签名，才能获取全部的数据信息资源。原有的信息和加密的数据信息，都要经过传递，才能到达接收的地点。接收人员也要按照同样类型的算法和公式，对原有的信息数据进行有效的摘要和提取，然后，将摘要之后的信息数据资源，与发送者已经签名过的信息数据资源进行有效的对比，才能保证技术应用的完整性。在这个过程中，签收的人员要借助发送人员，提供的公钥密码，才能对数据信息，进行有效的获取。如果在进行实际接收时，两者的信息和数据摘要能够保持一致，就证明信息和数据在传递的过程中是比较安全的。如果最终获取到的信息数据存在缺失，或者与发送人员，提供的信息数据不一致。那么就代表这些数据信息，在传递的过程中，遭受了外界的攻击，出现了安全性的问题。

所以相关的人员，在进行这项技术应用时，一定要保证加密的有效性。还要对个人的权限，进行有效的设计，才能提高技术应用的安全效果。确保这项技术在应用时，能够保障信息数据的传递安全。因为当前很多人员在进行这种技术应用时，并没有重视签名和认证，导致加密技术的应用，无法发挥应有的效果，会对数据信息传递的安全性，造成不利的影响。所以，在进行实际信息数据传递时，相关的人员一定要对这项技术的应用重点和难点，进行深入的分析和了解，才能保证技术的应用，更加的安全。提高信息数据传递的安全性，确保所有的信息数据在传递时，不会出现缺失和错误等情况。

例如，相关的人员在进行这项技术应用时，可以首先设计一个复杂的数字签名，并且对个人的认证，进行严格的管理。确保签名和认证在发送时，更加的安全，才能保证所有的信息数据在传递的路径中，不会遭受黑客和病毒的攻击，使得数据信息在传递时，能够保持完全的一致。相关人员在应用这项技术时，还应该提高加密的效果，才能为数据信息的传输，营造一个更加安全的环境。

四、结语

综上所述，当前在进行数据加密技术应用时，可以进行选择的类型比较多。但大部分技术在应用的过程中，都存在一定的问题，无法保证网络环境的绝对安全。要想提高网络和通信技术应用的安全系数，就要将多种类型的加密技术进行联合使用，通过综合技术的应用使得加密效果能够得到进一步的加强。相关人员还应该研发一些新型的技术，在现有的加密技术基础上，对技术的应用形式进行改善和优化，确保加密技术的应用效果和应用价值更高。才能为我国居民创造更加安全稳定的网络运行环境，促进计算机网络通信技术，进行可持续的发展。

参考文献：

[1]宋华茂,谢伟,张润坤.计算机网络通信安全中数据加密技术的应用分析[J].通讯世界, 2019,26(09):150-151.

[2]李红超,田有朋.试论数据加密技术在计算机网络通信安全中的应用[J].数字技术与应用, 2019,37(06):188+190.

[3]杨娟素,梁翠娟.计算机网络通信安全管理工作中数据加密技术的应用[J].数字通信世界, 2019(06):202.

[4]王慧.关于计算机网络通信安全中数据加密技术的运用探析[J].信息与电脑(理论版), 2019(09):148-149.

[5]李玉珍.基于计算机网络通信安全中数据加密技术的运用分析[J].信息与电脑(理论版), 2019(09):184-186.

[6]汤恒,张鹏伟,黄光前.计算机网络信息安全中数据加密技术分析[J].数字技术与应用, 2018,36(11):186-187.

[7]张耀东,张娴静.数据加密技术在计算机网络通信安全中的应用分析[J].赤峰学院学报(自然科学版), 2018,34(05):42-43.

[8]鲍印虎,董鹏,张占美.数据加密技术在计算机网络通信安全中的应用分析[J].科技传播, 2018,10(09):104-105.