On the security of a variant of Elgamal Encryption scheme

Abstract:

Now a days huge amounts of personal data are generated and collected everywhere due to the rapid advancement of technologies. The use of machine learning techniques makes it possible to extract useful knowledge from these data. However, because of their sensitivity, it is critical that such data be strongly protected by using encryption.

Existing system:

In the existing systems they are comparatively more efficient protocols for distributed key generation and distributed decryption for the cryptosystem than previous approaches. They have proved the security of their protocols using the simulation-based proofs based on appropriate assumptions. Their approach for distributed key generation is fairly complex and the cost of distributed decryption is still at least three times higher than that of centralized decryption in that the shares of the private key have to be long enough to properly hide the private key from those participants.

1. Application performance complexity is there
2. Cost is very high when compared with other methods.

Proposed system:

The ElGamal encryption scheme is a public-key cryptosystem with homomorphic properties. It is composed of three algorithms for key generation, encryption, and decryption, respectively.

Any adversary having access to the prime order of the underlying group in the ElGamal encryption scheme would be able to mount such an attack, which results in the total exposure of the secret key in the distributed cryptosystem.

Advantages:

1. It provides security for the data and capable of restricting the data attacks.
2. Application performance has been improved.

SYSTEM REQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –III
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X
- Front End : HTML, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.
- Database : MySQL 5.0
- Database Connectivity : JDBC