Future Work and Improvements:

1. Using our own servers to protect the server-side encryption algorithm will significantly reduce the risk of server-side code leakage. It will also allow us to be a trusted entity for signing signatures. Additionally, we can mitigate Man-in-the-Middle (MIM) attacks by implementing our own secure connections.

2. Adding expiry dates to licenses can greatly enhance business utility.

3. Blacklisting certain PC IDs ensures that PCs with untrusted software (as described in security context 3.2) will be blocked in future versions. This ensures that only paying users can access new versions of protected software.

4. Encrypting other sections: Sometimes critical information resides in the data or rdata section of the exe file. Encrypting these sections can play a crucial role in safeguarding software properties.

5. Other OS compatibility: Currently, our system supports only Windows 10 operating systems.

6. Processor support: Our system currently supports only Intel x86/64 architectures.

7. Supporting multithreaded programs.

8. Enhancing performance.