RMI Security Recommendations

- Follow Secure Coding Guidelines for Java SE.

Add missing check permissions

More related to internet application especially when there is exposure to SQL injection or brute force attack.

- Always run a security manager when using RMI, either on a client or server. See The Security Manager in The Java Tutorials.

  Need to make a custom policy file to grant permission to a specific location in the project. The activation of the security manager needs to configure the socketPermission by advance. It means adding a network configuration for each installation (server or client)

Establish a reasonable security policy. For example, grant SocketPermission and allow listen, accept, connect, and resolve actions only among hosts communicating with RMI. Do not have the security policy grant AllPermission. See Permissions in the JDK and Default Policy Implementation and Policy File Syntax.

Need to do a port configuration on both client and server application to securise the data transfert. Will be difficult to implement without adding complexity to the application installation and configuration

- If RMI is being used only for communication among JVMs on the local host, restrict communications to be local only. Accomplish this by specifying the appropriate socket permissions in the security policy file as described previously. Alternatively, you can use RMI APIs directly to restrict connections only to the local host. See an example of this in the documentation for the RMISocketFactory class.

Only for localhost application

- Ensure that the value of the java.rmi.server.useCodebaseOnly property is true (which is the default value). Setting this property to false enables remote code loading, which increases the level of security risk to the system. See java.rmi Properties.

Done

- Run RMI over SSL/TLS, and require authentication for both server and client. For further information, see the following:
  - The SslRMIClientSocketFactory class
  - The SslRMIServerSocketFactory class
  - Using Java RMI with SSL

- Java Secure Socket Extension (JSSE) Reference Guide
- JSSE Sample Code

Too complicate need to generate an SSL certificate for each new user using internet. Will be difficult to implement without adding complexity to the application installation and configuration