5. Security Tech Stack:

- Cryptography(Application):

    The encryption algorithm assigned to the TechScribe.TV company is called Triple DES. The Triple Data Encryption Standard (3DES) is a symmetric-key block cipher encryption algorithm. The 3DES algorithm is based on the original DES algorithm, which was vulnerable to brute-force attacks due to its relatively short key length. It applies the DES algorithm three times to each data block to provide increased security. Triple DES uses three 56-bit keys, resulting in a total length of 168 bits. These three keys are often referred to as Key1, Key2, and Key3. To encrypt data, the algorithm applies Key1 to the plaintext data block, then decrypts it using Key2, and finally encrypts it again using Key3.

    Our company has implemented the Triple DES algorithm to encrypt every line of a text file which contains the emails of every client that has used our platform. The encrypted text is then displayed directly to the console along with the original email for reference. In a C# program, you would apply the algorithm by firstly using the library System.Security.Cryptography. This library houses the CryptoServiceProvider class which contains many useful methods that will be applied in the implementation of the algorithm. Then, each line of the file will be divided into an array of bytes. This array of bytes will go through the ComputeHash, CreateEncryptor, and TransformFinalBlock methods until we have a newly encrypted array of bytes. The new array will be converted back to a string and either stored in a separate file or printed directly onto the console.

- Cryptography(Unique Algorithm):

    To add a layer of security to all of TechScribe.TV's data, we've invented a new encryption algorithm named Rainbow Encryption. It uses a randomized array of capitalized and lowercase letters and numbers as a base alphabet, as well as a key that constantly shifts between 8 identities. This serves as a very simplistic example of what could be evolved into a much more complex algorithm by just expanding the range of the key or by changing the calculations of the key from addition or subtraction to a much more complex formula. The alphabet could also be lengthened to include special

characters or even made to morph into a different arrangement for every use of the encryption. The effectiveness of the encryption in its current state is hindered by the out of bounds exceptions caused by the “alphabet” which were handled by using very basic methods that could potentially expose a pattern in the encrypted data.