Enhancing Data Security through Implementation of a Hybrid Cryptosystem with Emphasis on Levels of Entropy.

MSc Research Project
MSc in Cybersecurity

Lee Kearns
Student ID: x15728099

School of Computing
National College of Ireland

Supervisor: Mr. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Lee Kearns

Student ID: x15728099

Programme: Master of Science in Cybersecurity **Year:** 1

Module: MSc Research Project / Internship

Supervisor: Mr. Vikas Sahni

Submission Due Date: September 6th 2021

Project Title: Enhancing Data Security through Implementation of a Hybrid Cryptosystem with Emphasis on Levels of Entropy.

Word Count: 6160 **Page Count:** 18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Lee Kearns

Date: 01/09/2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Data Security through Implementation of a Hybrid Cryptosystem with Emphasis on Levels of Entropy.

Lee Kearns
x15728099

Abstract

As the technology world we live in today continues to rapidly develop and we see more and more people sharing data across the internet, new and advanced ways of securing this data must be implemented. This paper proposes a method where the implementation of a hybrid cryptosystem is introduced to provide an algorithm that portrays higher entropy levels, making it more secure against attacks such as brute force, man-in-the-middle attacks, stream cipher attacks, or ciphertext frequency analysis. The paper proposes a system that combines the two-industry standard symmetric and asymmetric algorithms AES and RSA. The encryption process is implemented through OpenSSL and GPG scripts for efficiency, while entropy levels are calculated using the Shannon Index Formula. The hybrid system has been evaluated with alternative encryption algorithms and is found to have higher entropy levels in comparison, with levels cumulating to an average of 4.02649, thus enhancing data security.

1 Introduction

Cybercrimes are becoming increasingly common and harder to prevent due to the continuous and rapid advancement in technology. It is becoming more challenging to bring the perpetrators to justice who are responsible for these cybercrimes. With the advances in technology, sending data across a network is becoming more popular, leaving this data vulnerable to various attacks. Data breaches and interceptions occur daily, exposing billions of sensitive information. In recent years, a major man-in-the-middle (MiTM) attack occurred when cybercriminals designed a spoofing campaign to portray as a Chinese VC firm. They intercepted a wire transfer to an Israeli start-up that contained $1 million. [1]. The two legitimate companies were exchanging emails to set up a “secure” communication channel, but an interceptor was sniffing the emails and created a forwarder to receive all communication between the two parties. The attacker then created a fake domain, adding one extra letter to the domain of the Israeli start-up making it difficult for the Chinese firm to recognise. Finally, once the wire transfer was sent, the cybercriminal intercepted the email and obtained the $1 million. This attack may have been avoided with the help from cryptography. Cryptography is the process of converting plaintext data into an unreadable format through mathematical functions. There are several approaches to securing data in cryptography, including the use of encryption algorithms. Encryption consists of converting plain text data into ciphertext and the decryption process converts ciphertext back into plain text. This is achieved using an encryption key, symmetric encryption uses the same key for encryption and decryption, while asymmetric encryption uses a public key for encryption and only the corresponding private key can decrypt the data. Examples of symmetric algorithms include AES, DES, 3DES, and Blowfish, and asymmetric algorithms include RSA and El

Gamal. This paper focuses on the combination of AES and RSA, forming a hybrid cryptosystem, to enhance data entropy levels to better secure encrypted data against attacks such as brute force, MiTM attacks, stream cipher attacks, and ciphertext frequency analysis.

1.1 Research Question

This paper focuses on addressing the following research question: ***Can data security, against popular cyber-attacks, be enhanced by implementing a hybrid cryptosystem combining AES and RSA algorithms?***

1.2 Research Motivation & Objective

Organisations share billions of sensitive information between one another daily. Many of these organisations may not use a secure way of sharing such information. For instance, some companies may use products such as Microsoft SharePoint to send sensitive data externally to clients. These clients may not use any Microsoft products, resulting in the company sending this sensitive data in plain text via email. The primary motive behind this research is to implement a hybrid cryptosystem containing AES & RSA algorithms to enhance the entropy levels of the encrypted data when sharing it across the internet to clients. Enhancing the entropy levels will increase the randomness of the data, making it difficult for attackers to make sense of the data. The following objectives are considered to ensure the previously mentioned criteria is met:

- Performing symmetric (AES) and asymmetric (RSA) encryption to various sizes of data so levels of entropy can be calculated.
- Implementing OpenSSL and GPG encryption scripts to ensure the efficiency of the encryption process.
- Perform comparative analysis to evaluate the proposed hybrid system.
- Shannon Index Formula is used to calculate the levels of entropy of the proposed hybrid system.

1.3 Paper Structure

This research paper is structured as follows; *Section 1: Introduction* will introduce the chosen area of research, while determining the motivation and objectives of the research. *Section 2: Related Work* portrays relevant state of the art research that have already been conducted for data security. *Section 3: Research Methodology* outlines the method that was employed in this paper. *Section 4: Design Specification* highlights the flow of the algorithm, detailing each step of the hybrid encryption approach. *Section 5: Implementation* illustrates how each of the encryption algorithms were implemented to perform the encryption process. *Section 6: Evaluation* portrays the results of the comparative analysis section and conveys the evaluation of the proposed system. Finally, the paper concludes with *Section 7: Conclusion and Future Work* which briefly discusses the research conducted and outlines possible future work.

2 Related Work

The subsections that follow provide an academic literature review related to previous approaches to securing data. The areas that are covered are image, plaintext, and audio encryption, novel data security techniques, and a comparative analysis of encryption techniques.

The rapid development of digital technology has established new ways for people and organisations to share sensitive information with one another, so the need for securing this data is of the utmost importance. The process of data encryption entails converting data that is in a readable plaintext format to an unreadable format, also known as ciphertext. The recipients of this data can only access or read it through decryption. To encrypt such data, the sender will use symmetric or asymmetric algorithms or a hybrid approach that will contain a combination of both. Nowadays, users tend to use open or standard ciphers for cryptology. There are three main reasons for this:

1. *To encourage the implementation of interoperability* (allowing computer systems to exchange information between each other): If these computer systems are using standard ciphers, it makes interoperability easier.
2. *Testing*: If standard ciphers are used, the experts can primarily focus on analysing and testing these ciphers. This will lead to higher confidence in the ciphers ability to secure data.
3. *To comply with Kerckhoff's principle*: This principle states that a cryptosystem's security must be dependant only on the keys chosen for encryption. All other information can be deemed public knowledge.

2.1 Image Encryption

Sending images across the internet has become a popular trend in recent years but the users may not be aware that sensitive information is attached in the metadata of these images, such as geo-location. Considering this, image security must be a high priority for internet users. Authors [2] propose a hybrid approach towards securing images. They combine the use of dynamic keys and static S-Box. The time function is used to randomly generate the dynamic key, depending on what time the user is connected to the system. The key is used for encryption on the static S-Box, converting it to a dynamic S-Box. Using this hybrid approach enables high-level security when transferring data. In addition, it heightens the complexity of AES in general as it provides extra characteristics for diffusion and substitution. Furthermore, it provides strong security against several attacks including algebraic, brute force, linear, and differential attacks. The research conducted by [3] proposes a system that makes use of 2D logistic maps and AES encryption algorithms to enhance image security. These algorithms are independent of one another, meaning that the image is firstly encrypted with a 2D logistic map and then re-encrypted with AES. The system is sensitive to the change in key values after the encryption process is complete, meaning to decrypt the image the exact key values must be entered. The proposed system makes the image robust against differential attacks, thus enhancing security when sharing the data across a network.

The proposed model found in [4] focuses on implementing a Java program that adopts a hybrid approach for encrypting and decrypting multimedia by combining AES and Elliptic Curve Cryptography (ECC) algorithms respectively. AES algorithm is used to encrypt the data first and then the user uses the ECC public key to encrypt the data further. In addition, the program stores the encrypted data on the receiver's directory. Furthermore, the receiver will use their ECC private key to decrypt the file and gain access to the original data. To conclude, using a hybrid approach will increase the encryption time since two encryption algorithms are being used but it will significantly increase the encryption strength as opposed to using the algorithms individually, making it an effective way to enhance the security surrounding the transfer of data across a network. Moreover, the research conducted by [5] highlights a proposed cipher that was created to enhance the performance of AES algorithm and the security of image encryption. This new variant of AES uses chaotic mapping and Exclusive OR operation to replace the MixColumns transformation, resulting in computation time being reduced. In addition, the values that are withdrawn from the encryption key will shift the S-Box rows in a circular motion. The end goal for doing this is to transform the S-

Box into a dynamic entity and simultaneously create an additional layer of obscurity for the cipher that can aid in the defence against attackers. As mentioned previously, this new variant of AES was designed to enhance image encryption. Nevertheless, a strong cipher should have the ability to enhance the security of all data types.

The next section discusses the state-of-the-art approaches to encrypt plaintext and audio files, combining encryption techniques with audio steganography.

2.2 Plaintext & Audio Encryption

The system proposed in [6] describes an attempt to address a substitution issue found in audio steganography. The system comprises of two separate levels of security. The first level consists of strong asymmetric algorithm RSA, which the system uses to encrypt the message. The second level encodes the encrypted message into an audio file. to encode the data, the authors implemented a genetic algorithm-based substitution method. The primary focus of this system is to enhance the security of the message it is encrypting and to enhance existing methods of audio steganography. In [7] the authors propose a novel approach the implements dual encryption. The first level of encryption consists of a pattern matching algorithm which is used to encrypt a plaintext message, depending on the positional value of the text. The second level uses the Least Significant Bit (LSB) technique to embed the encrypted text in a cover image. This dual encryption system ensures an efficient approach to data encryption.

The authors in [8] propose a system for hiding data through a combination of audio encryption, text encryption, and audio steganography. The first step of the proposed system uses the Vigenère cipher algorithm to encrypt the text message. Moreover, the system uses LSB encoding in the second step to embed the encrypted message inside a cover audio file. Finally, the system implements Blum Blum Shub, which is a pseudorandom number generator, to transpose the audio file containing the encrypted message. A downfall to this proposed system is the use of Vigenère cipher algorithm used to encrypt the text message. With the use of advanced technology, this algorithm is not considered strong against cipher attacks, meaning intruders can easily decode the message. A recommendation to use an industry standard encryption algorithm is highlighted by the authors in the paper.

The above sections discuss the existing research conducted for image, plaintext, and audio encryption individually. The section that follows discusses literature that explores novel approaches and modifications to existing encryption techniques which can be applied to enhance data security.

2.3 Novel Data Security Techniques

In 2001, the Rijndael algorithm was appointed the Advance Encryption Standard (AES). Since then, there have been various research papers published that implement an enhancement or modification to the existing AES algorithm. An example of this can be found in [9] where the authors highlight that several diplomatic and military applications consist of small modifications to AES algorithm. The primary focus of applying these small changes is to create a new secret cipher while inheriting the strength of the existing AES algorithm. The authors in [9] have proven that such modifications can be achieved relatively easy, while facing at least one conflict regarding Kerckhoff’s principle [10].

The above research outlines small modifications made to AES algorithm, while there are various papers that propose radical modifications. For instance, the authors [11] propose a system that will increase the algorithms key length to 320-bits. In addition, they propose an increase in the number of rounds to 16. Furthermore, the authors propose an efficient way of generating keys through implementing Polybius square, which allows the user to acquire the encryption key from a password. This proposed system consists of two main issues. Firstly, retrieving an encryption key is more difficult than retrieving a password. Retrieving a password is easier as they are selected by the user meaning they will have little entropy, leaving them vulnerable to social engineering techniques. [12]. Secondly, the authors are proposing a considerable number of changes to the algorithm. Software developers may be reluctant to implement such changes as they may be expensive. The changes may lead to rewriting the cipher code, which can simultaneously cause unnecessary problems to underlying systems. Contrastingly, minimal changes that can easily be implemented and amalgamated with the existing AES algorithm have a higher chance of acceptance.

Various researchers explored the likelihood of creating dynamic ciphers. For example, a dynamic cipher was proposed in [13]. The authors designed a polymorphic cipher that incorporates a semi-random approach that chooses a separate cryptographic suite each time it encrypts date (i.e., a different key length, cipher, and mode of operation). The cryptographic suite selected by the model is dynamically chosen based off values that have been extracted from the encryption key. There are sixty possibilities of cryptographic suites that can be chosen. Only legitimate users can identify the cryptographic suite that has been chosen. Nevertheless, this proposed system requires the implementation of sixty separate cryptographic suites. For this reason, the proposed system is questionable in terms of practicality. In addition, the overall performance of the model is slow.

Again, a dynamic encryption model is proposed in [14] which includes the implementation of symmetric algorithm DES and matrices multiplication. The user inserts plaintext $\boldsymbol{x}$ into the model, which firstly multiplies it using a binary invertible matrix $\boldsymbol{k_a}$. Network Coding concepts is responsible for generating the binary invertible matrix. Following the multiplication, plaintext $\boldsymbol{x}$ becomes $\boldsymbol{z_1}$. Therefore, the DES algorithm is responsible for encrypting $\boldsymbol{z_1}$ which will result in the model outputting $\boldsymbol{z_2}$. In the paper, the authors portray their reason for choosing DES algorithm for encryption: “to bring non-linearity”. Succeeding the encryption process is the generation of a second binary invertible matrix $\boldsymbol{k_c}$ which is used to multiply $\boldsymbol{z_2}$ to produce the ciphertext $\boldsymbol{y}$. The paper exhaustively elaborates the process for generating $\boldsymbol{k_a}$ and $\boldsymbol{k_c}$ alongside their reasons for updating $\boldsymbol{k_c}$.

The above-mentioned model entails an essential step, which is updating the matrix $\boldsymbol{k_c}$ before a new message is sent. This allows a user to send the same message twice knowing that the outcome will be different both times, even without the assistance of the block cipher mode of operation. This step allows the cipher to qualify as a dynamic cipher. Updating the matrix can be seen as a partial key update as $\boldsymbol{k_c}$, $\boldsymbol{k_a}$ and the 64-bit DES key are used in conjunction as the new cipher key. The authors state that the new dynamic cipher has similar performance levels to the existing 3-DES algorithm. However, the performance of 3-DES was never deemed acceptable. Evidently, the main goal of hosting the AES competition was to overcome the poor performance levels of the existing 3-DES cipher. [15]. In addition, it is hard to grasp why the authors chose DES algorithm for encryption in the intermediate layer, particularly when there are alternatives that are more secure and efficient. Finally, the paper portrays that further analysis of the security of the proposed cipher needs to be conducted, which is outlined in the future work section. Consequently, it is hard to determine the strength of the proposed cipher.

The following section discusses a comparative analysis of existing symmetric and asymmetric encryption techniques. The purpose of this will justify the reason behind selecting the encryption algorithms for the proposed system in this paper.

2.4 Comparative Analysis of Encryption Techniques

Cryptography is the art of securing sensitive data and information from becoming hacked or intercepted whilst being shared across a network or the internet [16], which is a very popular trend in recent years and it is only going to increase. For example, in an image that is captured on a device, sensitive information is produced which is known as metadata. The information that makes up this metadata includes image colour, or texture, but also includes sensitive information, for instance, geo-location or make and model of the device the image was captured on. The researchers [17] performed cryptographic techniques on image Exchangeable Image File Format (EXIF) metadata to encrypt the information to enhance its security. EXIF was established by a Japanese company known as Japan Electronic Industries Development Association (JEIDA). EXIF was the standard format of all camera images, and it was designed to adhere to ISO Standard 12234-1. The authors further discuss the importance of image security when sharing images across a network or internet and propose that in future studies they will apply several encryption techniques to image metadata to enhance its security when sharing the images.

Cryptography aims to maintain the security of the data's confidentiality, integrity, and availability (CIA). [16]. When considering encryption techniques, it is split into two separate categories. The number of keys the encryption algorithm uses predicts what category it falls under. The encryption categories include symmetric and asymmetric algorithms. Symmetric algorithms encrypt and decrypt data using the same encryption key, while asymmetric algorithms generate a public and a private key. The public key is used for encryption, while the private key, which is kept secure by the user, will decrypt the data that was encrypted with the corresponding public key. [18]. Symmetric algorithms have a weakness, considering it uses the same key for encryption and decryption. The biggest challenge we face when using symmetric algorithms is finding a secure way of sharing the key, so the decryption process is possible. When sharing this key, we leave ourselves vulnerable to man-in-the-middle attacks. If the key is intercepted when shared, the intruder can decrypt the data and obtain the contents inside. A weakness in asymmetric algorithms is the encryption speed, a symmetric algorithm is considerably faster. This is because asymmetric algorithms make use of more processing power [18].

Common symmetric algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard, Blowfish, and TwoFish. The National Institute of Technology Standards (NIST) suggested that DES was considered the industry standard for symmetric encryption. This encryption algorithm was designed by IBM in 1974, but it was not recognised as a standard until 1997. Moreover, DES uses a 64-bit block size and has a key length of 56 bits. [19] [20]. DES algorithm is vulnerable to various attacks, including key attacks. This is the reason for industries opting to use a more advanced algorithm with higher security features such as 3DES or AES. [19]. The 3DES algorithm was developed in 1998. The name "3DES" was assigned to the algorithm as the data blocks are ciphered 3 times, providing extra security against known attacks, including brute force attacks. Considering the data blocks are ciphered 3 times, it makes the algorithm considerably slow when comparing it to DES. [16]. The study conducted by [16], outlines that the symmetric algorithm Blowfish was developed in 1993 by Bruce Schneier. In addition, this algorithm can use a key length between 32 to 448 bits, with 128 bits being the default key size, and uses a cipher block size of 64 bits. The existing DES algorithm was considering insecure and outdated, so Blowfish was designed to replace it. Finally, the AES symmetric algorithm is round-based allowing it to perform both a cipher and decipher on data blocks. There are numerous variants of this algorithm, including AES-128, AES-192, and AES-256, alongside several modes such as Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR). The key length chosen for encryption, by the user, will determine which variant of AES is used. [21]. AES has never been cracked and is used by intelligence agencies such as the CIA and is considered industry standard by NIST. [22].

Performance analysis of symmetric algorithms AES, DES, 3DES, TwoFish, and Blowfish, and asymmetric algorithm RSA was conducted by [20] [23]. The studies focused on parameters such as memory usage, encryption and decryption times, entropy levels, and algorithm strength. The analysis performed by authors [20], [23] highlights that the symmetric algorithms Blowfish and Twofish consumed the least memory usage and acquired the fastest encryption and decryption times. The analysis conducted in [20] outlines that if data confidentiality and integrity are paramount when encrypting, AES scored the highest so it should be used. Furthermore, the algorithm that scored the highest levels of entropy was Blowfish, suggesting this algorithm is strongest against brute force attacks. Each cryptographic algorithm has its advantages and disadvantages, meaning an educated understanding of the efficiency, weaknesses, and strengths of the algorithms is crucial when deciding which cryptographic algorithm will be implemented with the proposed system. Considering the research conducted in [20] the algorithm with the highest entropy level was Blowfish, with AES and RSA coming second and third respectively. Knowing that AES and RSA are the recommended standard by NIST, and the primary focus of this research is levels of entropy, the two algorithms that have been considered for the hybrid cryptosystem proposed in the study are AES and RSA. An alternative hybrid cryptosystem is used for comparative analysis with the proposed system. It consists of Blowfish and RSA algorithms, considering Blowfish recorded the highest level of entropy between the three in [20].

3 Research Methodology

The research methodology section portrays an overview of the applied methods that make up the proposed system for securing data against common cipher attacks such as brute force, MiTM attacks, stream cipher attacks, or ciphertext frequency analysis. The purpose of the model is to enhance data security through creating a hybrid cryptosystem by combining symmetric and asymmetric encryption algorithms. The reason for combining the algorithms is to benefit from both their advantages such as the encryption throughput and efficiency of symmetric encryption alongside increasing the security and entropy levels of the data through asymmetric encryption. The proposed model consists of three main stages, which include Asymmetric Key Generation, Symmetric & Asymmetric Encryption, and Calculating Entropy Levels.

3.1 Asymmetric Key Generation

To generate both public and private keys, GPG software is used. The user creates an account with the software and chooses which asymmetric encryption algorithm they wish to use; in this paper it is RSA algorithm. They then choose the size of the encryption keys they wish to generate; this research focuses on 2048-bit which is the industry standard. Once this process is complete, the system generates the RSA public and private keys which are mathematically connected. Now, any time the user needs to encrypt data, they must include the username they provided when creating an account, with the encryption script, which will allow the GPG software encrypt the data using the corresponding keys to that account.

3.2 Symmetric & Asymmetric Encryption

Firstly, the user uses AES-256 (industry standard) in CBC mode to encrypt the data. OpenSSL software is used to make the encryption process efficient. The user will enter the encryption script which includes the name of the file they wish to encrypt, the algorithm name, size, and mode, and the name of the outputted encrypted file. After entering the script, the user will be prompted to enter a password which can then be used in the future for decryption, as the encryption key is unique to the password provided. Finally, GPG software is used to make the encryption process efficient. The user takes the encrypted file produced from the symmetric encryption process and encrypts it again using asymmetric algorithm RSA-2048. The user will enter the encryption script which includes the name of the file they wish to encrypt, the username they provided when generating the asymmetric encryption keys, and the name of the outputted encrypted file. The username provided will correspond to the public key that was generated and will use it to encrypt the file. In the future, if the user wishes to decrypt the file, they will need to enter the password provided when creating the account with the GPG software as it corresponds to the private key that was generated.

3.3 Calculating Entropy Levels of the Proposed Hybrid System

Calculating entropy levels will highlight the randomness of the encrypted data. This will determine the strength of the data against various attacks including brute force and cipher frequency analysis. To calculate the levels of entropy, the Shannon Index Formula was followed, which is:

$$H = -n\sum\ i=1\ p_i\ \log 2\ p_i.$$

4 Design Specification

This section outlines the flow of the proposed system which highlights the design of the aspects that make up the system. As mentioned in the previous section and can be seen in Figure 1, the proposed model comprises three major sections. These are Symmetric & Asymmetric Key Generation, Symmetric & Asymmetric Encryption, and calculating the levels of Entropy after Hybrid encryption has been applied to the data.

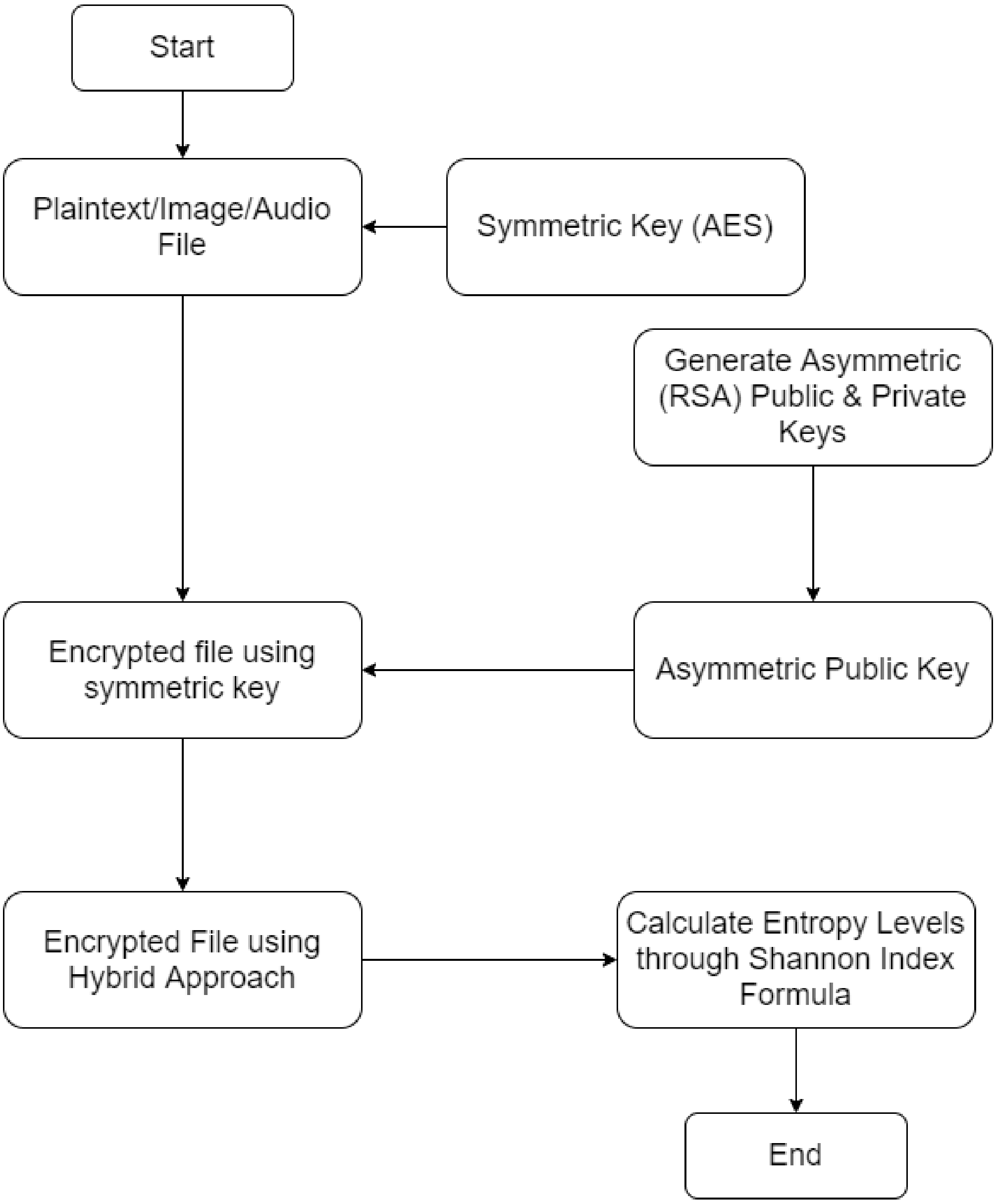

Start
Plaintext/Image/Audio File
Symmetric Key (AES)
Generate Asymmetric (RSA) Public & Private Keys
Encrypted file using symmetric key
Asymmetric Public Key
Encrypted File using Hybrid Approach
Calculate Entropy Levels through Shannon Index Formula
End

Figure 1: Flow Diagram of Proposed System

4.1 Proposed System Algorithm

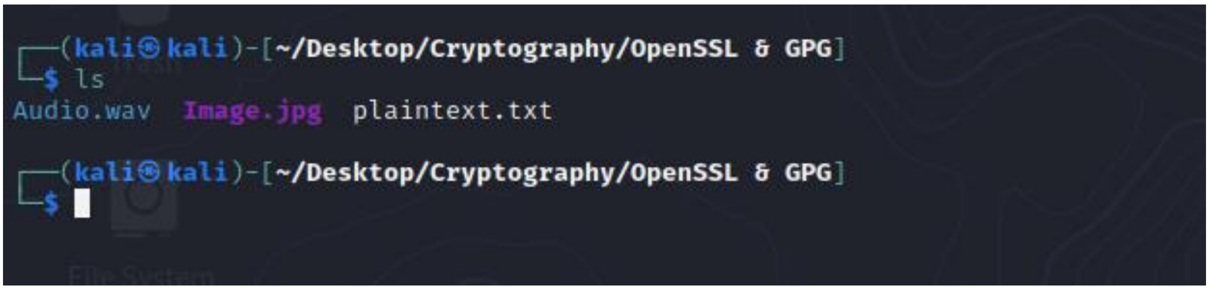
Step 0: The process starts.
Step 1: The user chooses the file they need to be encrypted (Plaintext/Image/Audio).
Step 2: The system generates a symmetric key which the user uses to encrypt the file chosen in the previous step.
Step 3: The user generates their asymmetric keys (Public & Private) for public-key encryption.
Step 4: The user utilises the public key generated in **Step 3** to encrypt the symmetrically encrypted file from **Step 2**. If the system does not recognise the public key, then EXIT the process. Otherwise, continue.
Step 5: The user calculates the level of entropy of the file through the Shannon Index formula which highlights the randomness of the data after the Hybrid encryption process.
Step 6: The process ends.

5 Implementation

This paper proposes a hybrid cryptosystem, which is implemented below by combining the AES-256-bit symmetric algorithm and RSA-2048 bit asymmetric algorithm to encrypt data to enhance its security. The proposed system utilises encryption scripts through OpenSSL [24] and GPG [25].

5.1 Initial Encryption using AES-256-CBC

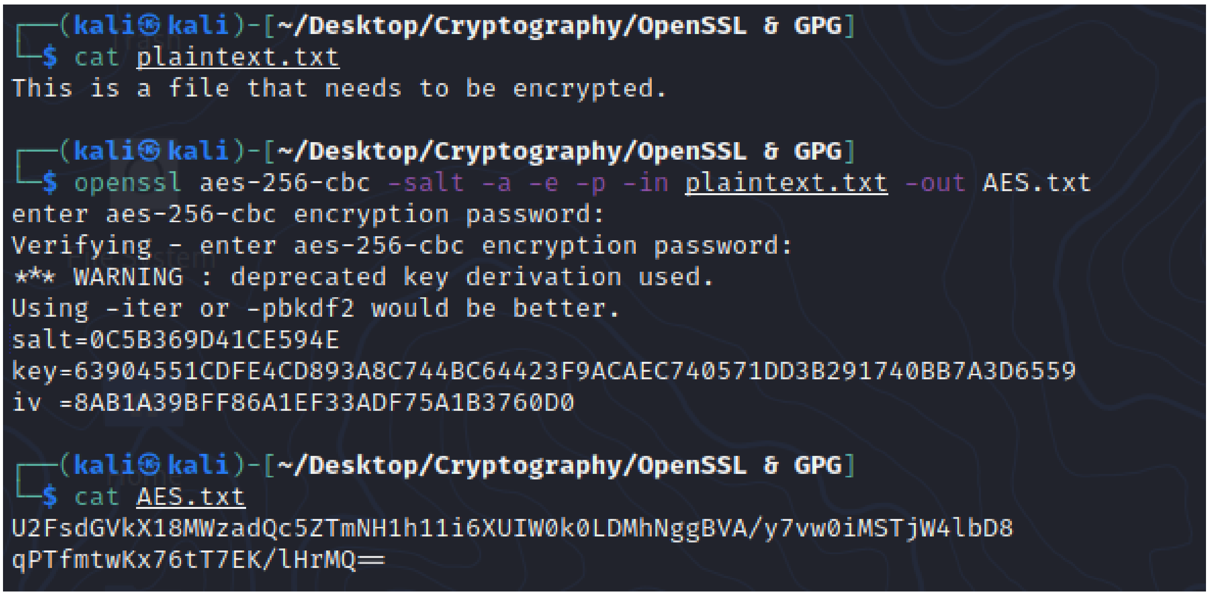
The initial step is to encrypt the data using symmetric algorithm AES-256 bit in Cipher Blocker Chaining (CBC) mode. The user must first choose which file they want to encrypt (plaintext, image, or audio).



```
┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ ls
Audio.wav  Image.jpg  plaintext.txt

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ █
```

Figure 2: Choosing a file for Encryption

Once the file is chosen, the AES scripts are used to encrypt the data. As mentioned previously, the symmetric encryption scripts are run through OpenSSL software, allowing for an efficient encryption process.



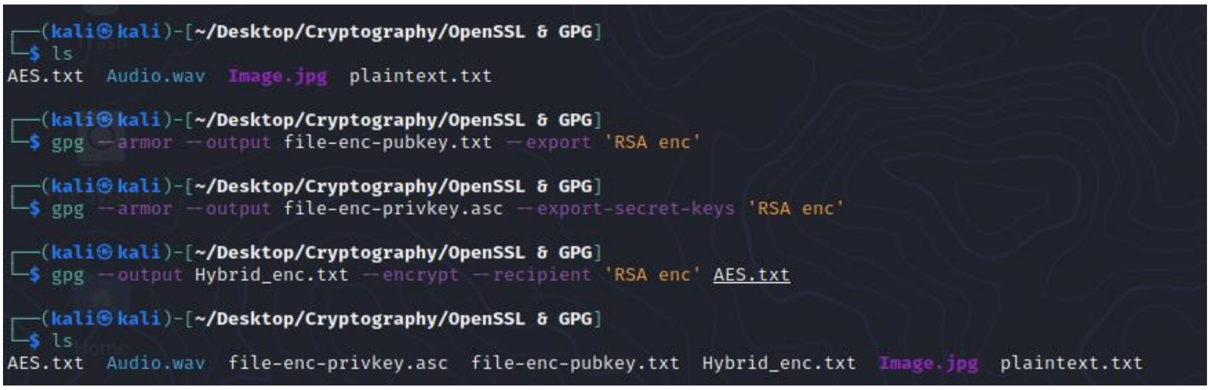
```
┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ cat plaintext.txt
This is a file that needs to be encrypted.

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ openssl aes-256-cbc -salt -a -e -p -in plaintext.txt -out AES.txt
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=0C5B369D41CE594E
key=63904551CDFE4CD893A8C744BC64423F9ACAEC740571DD3B291740BB7A3D6559
iv =8AB1A39BFF86A1EF33ADF75A1B3760D0

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ cat AES.txt
U2FsdGVkX18MWzadQc5ZTmNH1h11i6XUIW0k0LDMhNggBVA/y7vw0iMSTjW4lbD8
qPTfmtwKx76tT7EK/lHrMQ==
```

Figure 3: AES-256-CBC Encryption Process

Figure 3 highlights that the file chosen for encryption, in this example it was the plaintext file. The AES encryption command performs AES encryption on the chosen file and produces the encrypted file “AES.txt”. Furthermore, when encrypting the file through OpenSSL, the user must enter a password. This password is stored on the system which can then be used to decrypt the file in the future, ensuring the same key used for encryption is used in the decryption process. If the password doesn’t correspond to the password used for encryption, the decryption process will fail. In addition, the password is established through user input, while the salt, symmetric key, and IV are randomly assigned through the OpenSSL software.

5.2 Implementing the Hybrid Approach

Now that the initial encryption process is complete, the user must implement asymmetric encryption to benefit from the hybrid approach. The “AES.txt” file generated from the symmetric encryption process previously will now be encrypted again using the asymmetric public key.



```
┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ ls
AES.txt  Audio.wav  Image.jpg  plaintext.txt

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ gpg --armor --output file-enc-pubkey.txt --export 'RSA enc'

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ gpg --armor --output file-enc-privkey.asc --export-secret-keys 'RSA enc'

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ gpg --output Hybrid_enc.txt --encrypt --recipient 'RSA enc' AES.txt

┌──(kali㉿kali)-[~/Desktop/Cryptography/OpenSSL & GPG]
└─$ ls
AES.txt  Audio.wav  file-enc-privkey.asc  file-enc-pubkey.txt  Hybrid_enc.txt  Image.jpg  plaintext.txt
```

Figure 4: Hybrid Encryption Process

Figure 4 demonstrates the hybrid encryption process being implemented by the user. The user combines symmetric and asymmetric encryption to enhance the entropy levels of the data they want to secure. Moreover, asymmetric public and private keys are generated when creating a user with the GPG software. The username chosen is “RSA enc”, so anytime that username is inputted into the command line, the system knows to encrypt the data with the corresponding key generated when creating the user. Finally, with asymmetric encryption, the public key is used to encrypt the chosen data, while the private key is used only for decryption.

6 Evaluation

The evaluation section of this paper portrays comparative analysis experiments conducted to highlight performance and speed of AES, Blowfish, the proposed hybrid cryptosystem implemented for this research and an alternative hybrid cryptosystem, alongside analysis of the entropy levels of both systems. The proposed system comprises of AES and RSA algorithm, while the alternative system comprises of Blowfish and RSA algorithms. The reason behind the selection of Blowfish and RSA is that previous research shows Blowfish to have the highest levels of entropy compared to AES, DES, 3DES, and RSA, and RSA is industry standard appointed by NIST. If the proposed system has higher entropy levels than the alternative algorithms, it will illustrate an enhancement in data security. The evaluation is based on ten different file sizes ranging from 32kB – 6144kB that look to calculate performance metrics including encryption throughput, encryption times, and entropy levels.

The encryption throughput can determine the performance of an algorithm. This can be measured by dividing the size of the plaintext file by the time taken for encryption. [26].

Considering the formula for calculating throughput, the faster the encryption time the higher the performance levels of the algorithm.

Contrastingly, encryption time is the total time the algorithm takes to encrypt the plaintext (i.e., how long together AES & RSA take to encrypt the data). The efficiency of an algorithm can be determined by calculating the encryption time. [26]. Considering this, the least time taken for encryption, the higher the efficiency of the algorithm.

In cryptography, randomness is an essential part for encryption algorithms as information should not be easily guessed by intruders. Entropy levels represent the randomness of the data that has been encrypted. In addition, it highlights uncertainty in the data. In data security, encryption algorithms should portray high randomness when encryption has been performed, so there is little need to depend on keys and ciphertext. Moreover, when an algorithm acquires high entropy levels, the relationship between the ciphertext and key may become complex, also known as confusion. Greater levels of confusion are an essential role in making it difficult for intruders to crack the ciphertext. Furthermore, entropy is another way to measure the performance of an algorithm. Finally, Shannon entropy index formula is used for calculating entropy levels of the proposed hybrid cryptosystem and alternative encryption algorithms. This formula calculates the number of times a character appears in data, meaning the higher the randomness of the data, the harder it is for attackers to predict the content.

6.1 Case Study 1: Comparative Analysis of Proposed Hybrid Cryptosystem and Alternative Hybrid Cryptosystem

6.1.1 Encryption Times of Proposed Hybrid Cryptosystem & Alternative Hybrid Cryptosystem

File Size (KB)	AES + RSA Encryption Time (Seconds)	Blowfish + RSA Encryption Time (Seconds)
32	0.372459621	0.004564872
64	0.477603056	0.008935483
128	0.501921935	0.015716502
256	0.529911194	0.030510758
512	0.570362261	0.049852471
1024	0.571026941	0.113631458
2048	0.588299138	0.226334057
4096	0.686185029	0.405616037
5120	0.816835306	0.555357515
6144	0.824170286	0.722015485

Table 1: Encryption Times of Proposed Hybrid Model & Alternative Hybrid Model

6.1.2 Comparison of AES & Proposed Hybrid Cryptosystem Encryption Times

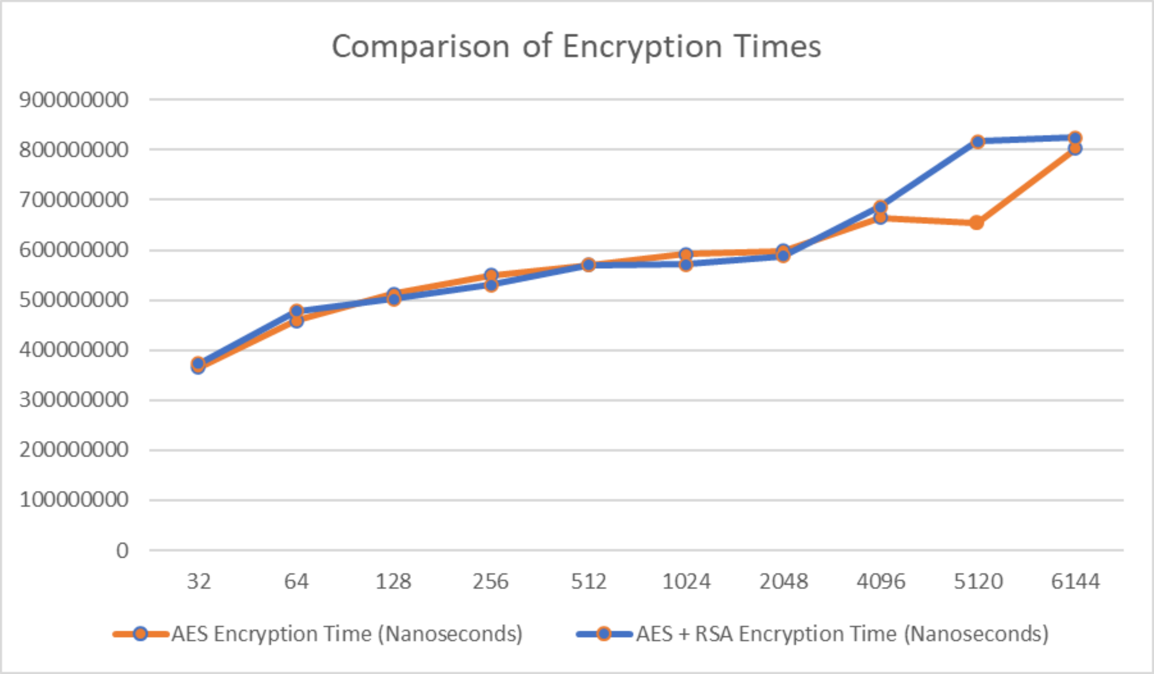


Figure 5: Comparison of Encryption Times for Proposed System

6.1.3 Comparison of Blowfish & Alternative Hybrid Cryptosystem Encryption Times

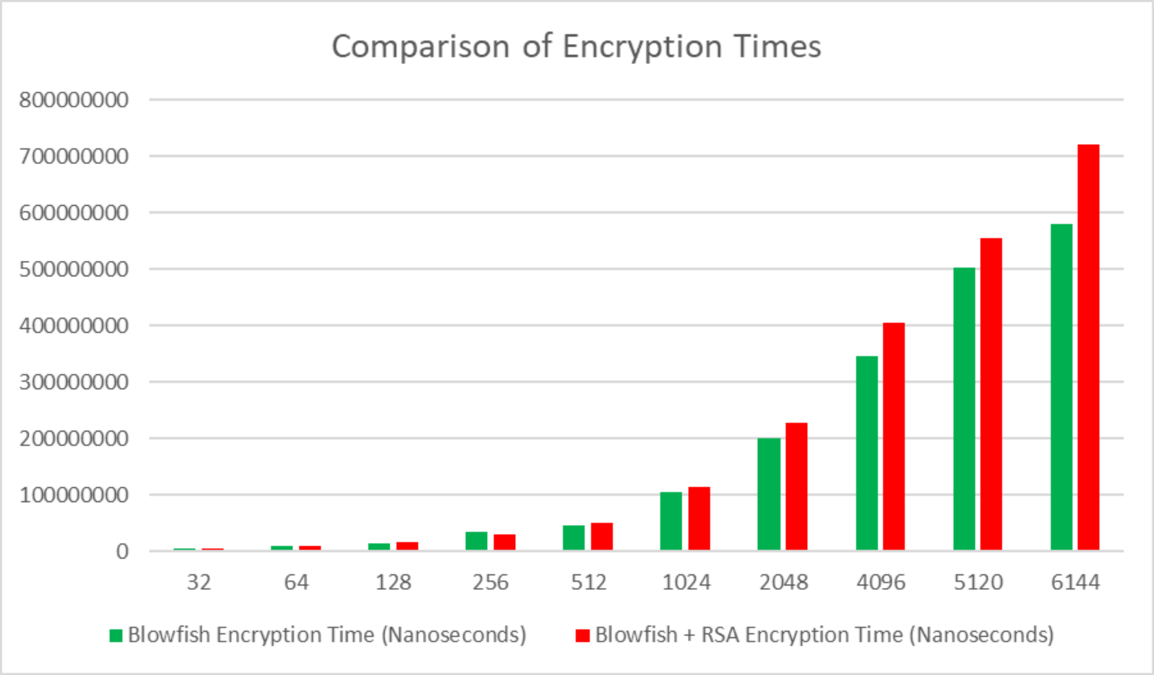


Figure 6: Comparison of Encryption Times of Alternative System

6.1.4 Comparison of Proposed Hybrid Cryptosystem & Alternative Hybrid Cryptosystem Encryption Times

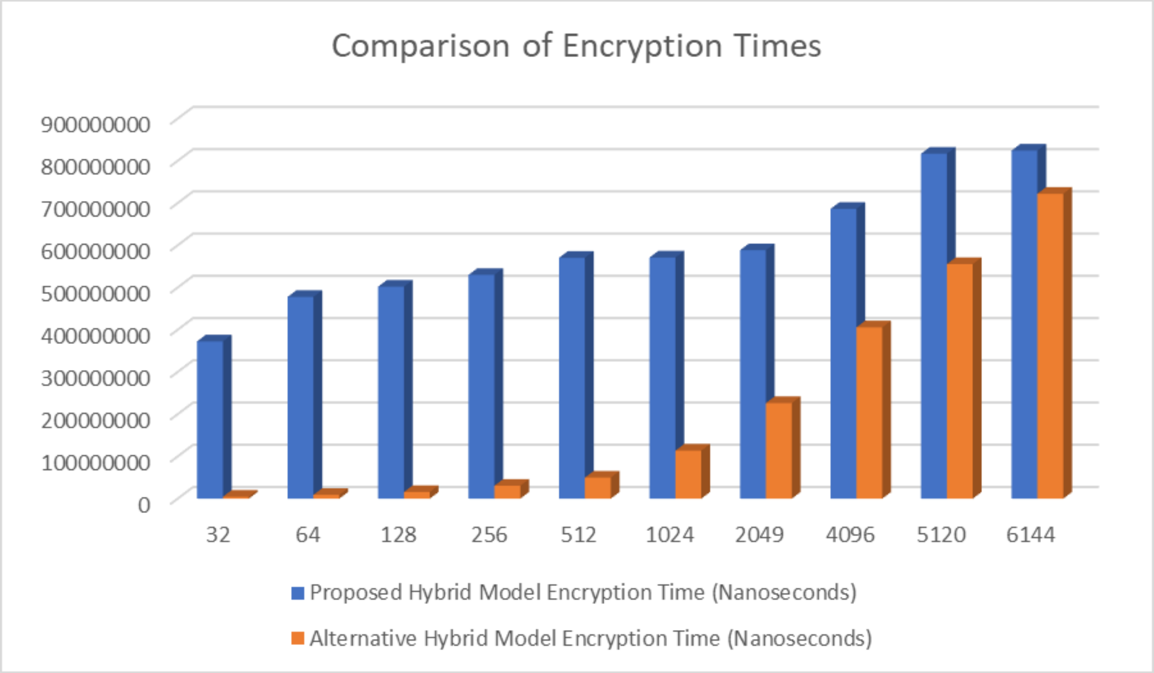


Figure 7: Comparison of Encrypted Times of Proposed System and Alternative System

6.1.5 Comparison of Encryption Throughput between Proposed Hybrid Cryptosystem & Alternative Hybrid Cryptosystem

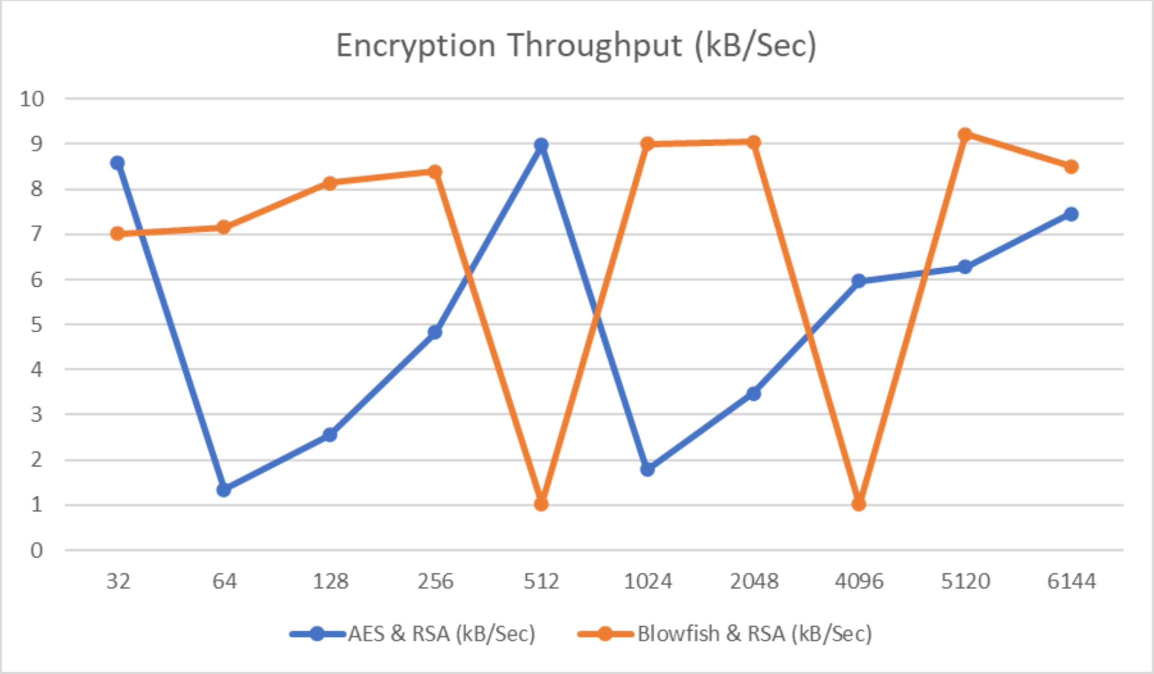


Figure 8: Encryption Throughput (kB/Sec)

6.2 Case Study 2: Analysis of Entropy Levels Between Proposed Hybrid Cryptosystem & Alternative Hybrid Cryptosystem

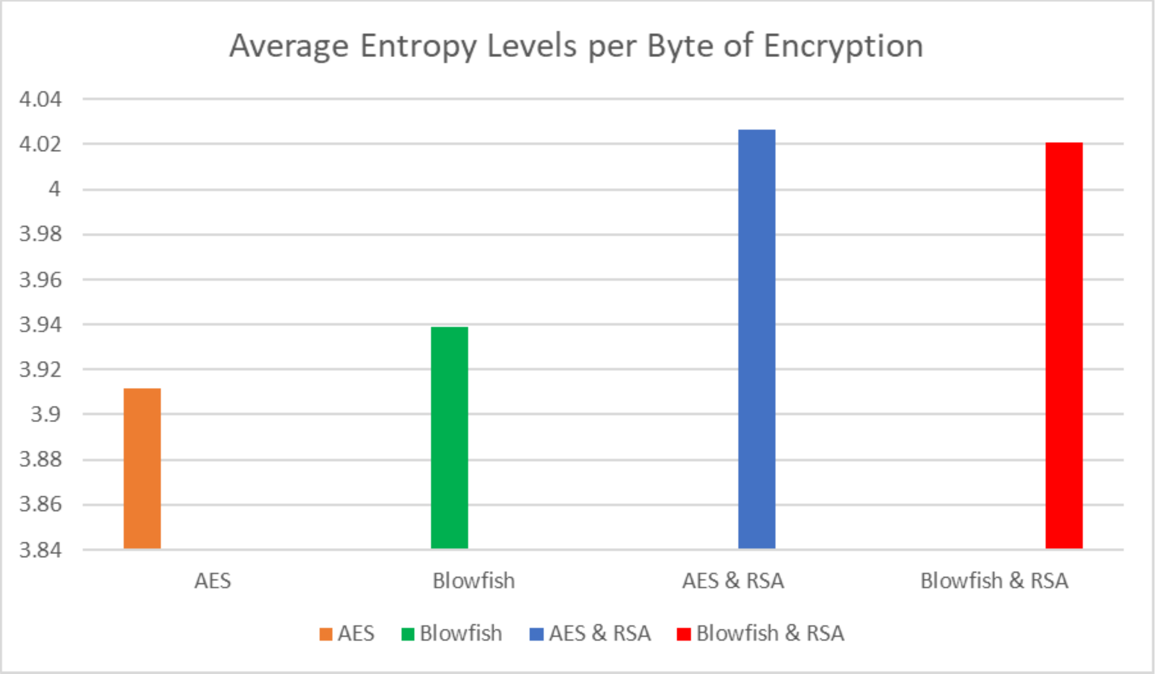


Figure 9: Entropy Levels of Proposed System & Alternative System

6.3 Discussion

The proposed hybrid cryptosystem was compared to AES, Blowfish, and Blowfish & RSA in the previous section. Metrics such as encryption times, encryption throughput, and entropy levels were analysed. As previously mentioned in the literature review, Blowfish, AES, and RSA recorded the highest levels of entropy respectively in [20]. However, AES and RSA are both industry standard algorithms appointed by NIST, hence the reason for selecting them for the proposed hybrid cryptosystem. In addition, the combination of these two algorithms has already been researched in [23] but the primary focus of their research was the algorithms efficiency and speed. The authors outlined in their future work that metrics such as entropy levels can be examined, hence the decision to primarily focus on entropy levels in this paper.

Results of encryption times taken by AES, AES & RSA, Blowfish, and Blowfish & RSA are compared in figures 5 and 6. They highlight that Blowfish takes the least time for encryption compared to the other mentioned algorithms. Evidently, the slowest encryption time is recorded by the proposed hybrid system outlined in this paper. In addition, results of encryption times taken and encryption throughput by proposed hybrid system and alternative hybrid system are compared in figures 7 and 8. It can be observed that the alternative hybrid system has much faster encryption times and the performance of the system is more efficient when compared to the proposed hybrid system. Considering the results mentioned thus far, it can be observed that AES, Blowfish, and the alternative hybrid system portray faster encryption times and are more efficient than the proposed hybrid system, meaning if the primary focus of this research was speed and efficiency, one of the mentioned algorithms should be considered. However, the primary focus of this research paper is entropy levels.

The results of the entropy levels of AES, Blowfish, proposed hybrid system and alternative hybrid system are outlined in figure 9. AES algorithm is industry standard appointed by NIST. Considering this, AES entropy levels (3.9118) were used as a baseline for this research, highlighting that the proposed hybrid cryptosystem recorded the highest levels of entropy (4.02649) when compared to the alternative algorithms. Therefore, for this research, the proposed hybrid cryptosystem consisting of AES & RSA algorithms is proved to have more randomness and confusion than alternative hybrid cryptosystem, meaning it is more secure against attacks such as brute force, MiTM attacks, stream cipher attacks, or ciphertext frequency analysis.

7 Conclusion and Future Work

The main objective behind this research paper was to determine whether the implementation of a hybrid cryptosystem containing AES and RSA algorithms would enhance data security against popular cyber-attacks such as brute force, man-in-the-middle attacks, stream cipher attacks, and cipher frequency analysis. AES and RSA have both been appointed as industry standard algorithms by NIST. A hybrid cryptosystem was created which firstly encrypts data using AES and then encrypts that data again with RSA. The results of the proposed hybrid cryptosystem prove that combining these algorithms produces a higher level of entropy (4.02649) than alternative methods. This provides a higher level of randomness to the encrypted data, making it more secure against the above-mentioned attacks, thus making it difficult for attackers to make sense of the data. This research concludes that the proposed hybrid cryptosystem containing AES and RSA algorithms successfully enhances data security against attacks such as brute force, man-in-the-middle attacks, stream cipher attacks, and frequency analysis.

The motivation behind this research was mentioned in *Section 1* of this paper. Considering the evaluated results of this research, a Python application consisting of AES and RSA algorithms can be implemented for future work. The future scope of this research will be to implement a secure Python system for data transfer between two parties, using AES and RSA algorithms for encrypting and decrypting the data.

8 Acknowledgements

I would like to personally thank my project supervisor, Mr. Vikas Sahni, and the entire team at SecuriCentrix for their continued support and guidance. Mr. Vikas Sahni and SecuriCentrix colleagues showed constant support and encouragement throughout the duration of the research dissertation. I would also like to thank my girlfriend, family, and my peers enrolled in the cybersecurity master’s programme who guided me through any rough phases encountered throughout the year.

References

[1] '"Ultimate" MiTM Attack Steals $1M from Israeli Startup'. https://threatpost.com/ultimate-mitm-attack-steals-1m-from-israeli-startup/150840/ (accessed Sep. 01, 2021).

[2] F. J. D'souza and D. Panchal, 'Advanced encryption standard (AES) security enhancement using hybrid approach', in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, May 2017, pp. 647–652. doi: 10.1109/CCAA.2017.8229881.

[3] Y. Jha, K. Kaur, and C. Pradhan, 'Improving image encryption using two-dimensional logistic map and AES', in *2016 International Conference on Communication and Signal Processing (ICCSP)*, Apr. 2016, pp. 0177–0180. doi: 10.1109/ICCSP.2016.7754116.

[4] S. C. Iyer, R. R. Sedamkar, and S. Gupta, 'A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach', *Procedia Comput. Sci.*, vol. 79, pp. 293–298, Jan. 2016, doi: 10.1016/j.procs.2016.03.038.

[5] A. Abdulgader, M. Ismail, N. Zainal, and T. Idbeaa, 'ENHANCEMENT OF AES ALGORITHM BASED ON CHAOTIC MAPS AND SHIFT OPERATION FOR IMAGE ENCRYPTION', . *Vol.*, p. 12, 2005.

[6] G. Singh, K. Tiwari, and S. Singh, 'Audio Steganography using RSA Algorithm and Genetic based Substitution method to Enhance Security'. https://www.ijser.org/paper/Audio-Steganography-using-RSA-Algorithm-and-Genetic-based-Substitution.html (accessed Aug. 30, 2021).

[7] R. Chowdhury, D. Bhattacharyya, S. K. Bandyopadhyay, and T. Kim, 'A View on LSB Based Audio Steganography', *Int. J. Secur. Its Appl.*, vol. 10, no. 2, pp. 51–62, Feb. 2016, doi: 10.14257/ijsia.2016.10.2.05.

[8] N. Sinha, A. Bhowmick, and B. Kishore, 'Encrypted Information Hiding using Audio Steganography and Audio Cryptography', *Int. J. Comput. Appl.*, vol. 112, no. 5, p. 5.

[9] C. Clavier, Q. Isorez, D. Marion, and A. Wurcker, 'Complete reverse-engineering of AES-like block ciphers by SCARE and FIRE attacks', *Cryptogr. Commun.*, vol. 7, no. 1, pp. 121–162, Mar. 2015, doi: 10.1007/s12095-014-0112-7.

[10] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, 'Combination of Steganography and Cryptography: A short Survey', *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 518, p. 052003, Jun. 2019, doi: 10.1088/1757-899X/518/5/052003.

[11] P. Kumar and S. B. Rana, 'Development of modified AES algorithm for data security', *Optik*, vol. 127, no. 4, pp. 2341–2345, Feb. 2016, doi: 10.1016/j.ijleo.2015.11.188.

[12] J. Saleem and M. Hammoudeh, 'Defense Methods Against Social Engineering Attacks', in *Computer and Network Security Essentials*, K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 603–618. doi: 10.1007/978-3-319-58424-9_35.

[13] A. Altigani, S. Hasan, S. M. Shamsuddin, and B. Barry, 'A multi-shape hybrid symmetric encryption algorithm to thwart attacks based on the knowledge of the used cryptographic suite', *J. Inf. Secur. Appl.*, vol. 46, pp. 210–221, Jun. 2019, doi: 10.1016/j.jisa.2019.03.013.

[14] H. Tang, Q. T. Sun, X. Yang, and K. Long, 'A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense', *IEEE Access*, vol. 6, pp. 26059–26068, 2018, doi: 10.1109/ACCESS.2018.2832854.

[15] N. Sklavos, 'Book Review: Stallings, W. Cryptography and Network Security: Principles and Practice', *Inf. Secur. J. Glob. Perspect.*, vol. 23, no. 1–2, pp. 49–50, Jan. 2014, doi: 10.1080/19393555.2014.900834.

[16] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, ‘Comprehensive study of symmetric key and asymmetric key encryption algorithms’, in *2017 International Conference on Engineering and Technology (ICET)*, Aug. 2017, pp. 1–7. doi: 10.1109/ICEngTechnol.2017.8308215.

[17] H. Wijayanto, I. Riadi, and Y. Prayudi, ‘Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy’, vol. 5, pp. 2320–5156, May 2016.

[18] P. Kumar, S. Rawat, T. Choudhury, and S. Pradhan, ‘A performance based comparison of various symmetric cryptographic algorithms in run-time scenario’, in *2016 International Conference System Modeling Advancement in Research Trends (SMART)*, Nov. 2016, pp. 37–41. doi: 10.1109/SYSMART.2016.7894485.

[19] M. Panda, ‘Performance analysis of encryption algorithms for security’, in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Oct. 2016, pp. 278–284. doi: 10.1109/SCOPES.2016.7955835.

[20] P. Patil, P. Narayankar, Narayan D.G., and Meena S.M., ‘A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish’, *Procedia Comput. Sci.*, vol. 78, pp. 617–624, Jan. 2016, doi: 10.1016/j.procs.2016.02.108.

[21] M. Biglari, E. Qasemi, and B. Pourmohseni, ‘Maestro: A high performance AES encryption/decryption system’, in *The 17th CSI International Symposium on Computer Architecture Digital Systems (CADS 2013)*, Oct. 2013, pp. 145–148. doi: 10.1109/CADS.2013.6714255.

[22] I. T. L. Computer Security Division, ‘AES Development - Cryptographic Standards and Guidelines | CSRC | CSRC’, *CSRC | NIST*, Dec. 29, 2016. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development (accessed Aug. 25, 2021).

[23] E. Jintcharadze and M. Iavich, ‘Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems’, in *2020 IEEE East-West Design Test Symposium (EWDTS)*, Sep. 2020, pp. 1–5. doi: 10.1109/EWDTS50664.2020.9224901.

[24] Kekayan, ‘Encrypt files using AES with OPENSSL’, *Medium*, Jul. 07, 2018. https://kekayan.medium.com/encrypt-files-using-aes-with-openssl-dabb86d5b748 (accessed Sep. 01, 2021).

[25] ‘Getting started with commandline encryption tools on Linux’, *HowtoForge*. https://www.howtoforge.com/tutorial/linux-commandline-encryption-tools/ (accessed Sep. 01, 2021).

[26] M. Arora, S. Sharma, and D. Engles, ‘Parametric comparison of EMDS algorithm with some symmetric cryptosystems’, *Egypt. Inform. J.*, vol. 18, no. 2, pp. 141–149, Jul. 2017, doi: 10.1016/j.eij.2016.11.004.

9 Appendix

Monthly Internship Activity Report

Student Name: Lee Kearns		Student number:	x15728099
Company:	SecuriCentrix	Month Commencing:	June 2021

Week 1: During the first week of employment at SecuriCentrix, I was given an alarm (Potentially Unwanted Program) to analyse to determine whether it was a false positive or true positive. After analysing the appropriate sections of the log, the DNS RR name was related to a third party vendor that you can get free driver updates. Analysis highlighted that to follow security best practices, only official websites should be used to download software and updates. This alarm was flagged as a true positive. This task enhanced my analysis skills and highlighted the essential places to focus on when analysing alarms. The rest of this week was spent becoming familiar with the company's SIEM tool AlienVault, focusing on how everything is laid out and how it functions.

Week 2: First task of the second week was to carry out a malware analysis of a Pcap file for Suhas, my Team Leader. The task consisted of 15 questions related to the piece of malware and it was split into three categories: Initial analysis, static analysis, and dynamic analysis. Some questions that were asked was to find the hash of the 2 files, the magic header, file size, the malware family and so on. Malware analysis has always been an interest of mine, so to have the chance to gain hands on experience has had a huge benefit. Tools such as WireShark, Autopsy, PE Viewer were used to complete this task. During this week I was exposed to my first client call. This call was with Client 1, and Adrian, a consultant for SecuriCentrix, was carrying out a security audit. I was asked to observe the tasks involved and become familiar with how to engage with clients. This call highlighted how to appropriately engage with clients and to know your audience. I obtained some theoretical knowledge also. Next, I was tasked with analysing a potential phishing email for David, the managing director of SecuriCentrix. David was receiving multiple occurrences of the same email and wanted an investigation to be carried out to determine whether it was a phishing attempt. The email was in Arabic, so the first step was to convert it to English. The sender's email was then searched on Google, no results matched it. But a similar email was found with one letter changed. It was linked to an Egyptian professor from Cairo, and his mobile number matched a mobile number provided in the email. This led us to believe it was a possible impersonation, so further analysis was conducted. The domain of the sender's email was scanned through VirusTotal - 1/88 vendors categorised it as suspicious and phishing. The source code of the email was inspected. This was to highlight where the URLs inside the email were being redirected to. It is bad practice to just hover over the link itself. The website name was searched on Google, highlighting that it was an insecure website with no SSL cert. The conclusion derived from the analysis was that this email is in fact a phishing attempt. Following this, I was tasked with creating new Linux assets group for Client 2.

Week 3: I experienced more exposure to analysing alarms during the third week of employment. The alarm's name was "Bitcoin Minor". The Bitcoin Minor alarm consisted of a Monero Trojan malware and a DNS RR name pool.minexmr.com. This DNS RR name was ran through VirusTotal and other vendors and it was flagged as malicious. An incident report was raised with the client and they informed us that the DNS RR name had since been blocked on their antivirus and perimeter firewall. Another alarm was analysed "Multiple AWS IAM Access Denied" which occurred on Client 3. User Michael.Clark, was attempting to access resources he did not have access for. Raised a query with the client and they responded that it was a legitimate user on their system. The user is busy accessing new portal pages to generate certain reports requested from him. Very often those pages references resources that are not allowed for the logged in user and the errors will then be handled by the console backend. The final task of the week was assigned to me by Sanga, a SOC analyst at SecuriCentrix. Sanga tasked me to compare 2 alarms from the event Azure Security Centre and identify if they are true/false positives. It was determined that the event "Adaptive application control policy violation was audited" was the true positive, Sanga sent query to the client previously in relation to it. The other event in relation to SQL was a false positive. An internal resource was running an SQL query which triggered the alarm. This week strongly enhanced my analysis skills with alarms that are triggered on the SIEM tool.

Week 4: Sanga tasked me with analysing an alarm for client Client 4. The alarm name was "Zmap Scanning". I created an incident report and Sanga raised it with the client and still awaiting their response. Next task was creating Incident report for Sanga for client Client 5 regarding DNS Query to Suspicious Domain alarm. The DNS RR Name fget.guangbom.com was analysed through threat detection tools, highlighting that it was safe. Through further analysis on the DNS RR name on US Anywhere, there were several related IP addresses found that were all flagged as suspicious. Searched for DNS RR Name on Google, several documentations highlight that is is related to a HummingBad malware which acts as a rootkit malware. An Incident Query has been raised with the client and a list of CNC URLs that must be blocked have been sent to the client, alongside a list of the associated IP addresses. Client responded that the DNS RR name has since been blocked on their antivirus and perimeter firewall.

Employer comments

Lee has settled well and appears to learn quickly. He has made some good progress on his thesis too.

Student Signature: Lee Kearns Date: 28/06/2021

Industry Supervisor Signature: _David Steele_______________06/07/2021________

Monthly Internship Activity Report

Student Name: Lee Kearns Student number: x15728099

Company: SecuriCentrix Month Commencing: July 2021

The beginning of this month ran as well as expected. I have acquired several daily tasks as well as handling other ones. These daily tasks include completing a daily security checklist, monitoring a client's environment and checking for malicious IP addresses relating to Bad Robot, Scan on Non-Standard Ports, and Zmap Scanning events, and monitoring alarms. The daily security checklist entails of monitoring our clients' environments for the previous 24 hours and inserting the data (alarm names, details, Source/Destination IP’s, status of the sensors and systems) into an excel workbook. Carrying out this task is a great way to simultaneously monitor alarms while carrying out the checklist which allowed me to work more efficiently and raise queries/incidents with clients if needed.

After I was shown how to raise queries and incidents with clients, I was able to raise several throughout the month. A query report is only used for events with lower priority or if we need the client to provide more information regarding the event. An incident report is for events with higher priority, and we attach strategies that the client should follow for mitigation purposes.

I was shown how we create alarms in the SIEM tool used in the company. After I was comfortable with the fundamentals behind creating an alarm, I was tasked with creating several for our clients. These alarms needed to be reviewed and are now implemented in the corresponding client’s environments.

Finally, I was exposed to several penetration tests towards the end of the month for a few clients. The clients authorise us to perform a penetration test on their environment and systems to test and check for vulnerabilities in their security. If any are found, they must be documented in a report and sent out to the client with recommendations on how to mitigate and patch the vulnerabilities in order for the client to become PCI certified. I was involved in both the penetration testing and report writing which I found to be very beneficial as I see myself becoming a pen tester for my long-term career path.

Employer comments

Lee is adapting well to the environment and tasks he is working on.

Student Signature: Lee Kearns Date: 31/07/2021

Industry Supervisor Signature: __David Steele 24/08/2021

Monthly Internship Activity Report

Student Name: Lee Kearns Student number: x15728099

Company: SecuriCentrix Month Commencing: August 2021

The final month of the Internship program was equally enjoyable as the previous two months. I still carried out my daily tasks while much of my time was consumed with continuing some penetration tests. I continued creating more alarms and raising incidents and queries with clients as they appeared through monitoring the client’s environments.

Employer comments

Student Signature: Lee Kearns Date: 20/08/2021

Industry Supervisor Signature: David Steele 24/08/2021