Personal Data Security in Recruitment Platforms

Alya'a Bajoudah† and Hatim AlSuwat [1†],
S44380349@st.uqu.edu.sa Hssuwat@uqu.edu.sa
[1] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Summary
Job offers have become more widespread and it has become easier and faster to apply for jobs through electronic recruitment platforms. In order to increase the protection of the data that is attached to the recruitment platforms. In this research, a proposed model was created through the use of hybrid encryption, which is used through the following algorithms: AES,Twofish,. This proposed model proved the effectiveness of using hybrid encryption in protecting personal data.

Keywords:
Personal data ,Hybrid cryptography , AES , Twofish, RSA..

1. Introduction

With the rapid development of technology, particularly in the fields of the Internet and technology, the exchange of information and data has become very easy and fast over the Internet, Increasing people's knowledge and their communication with each other.This spread has resulted in the creation of new platforms that help people display more about their fields and how others can benefit from them. Recently, platforms that assist job seekers in finding job opportunities in their fields have proliferated, by connecting job seekers and employers via platforms in which the job seeker enters his personal information in addition to the CV, and then the job seeker receives job offers that are relevant to his field , "Internet recruiting, or e-Recruitment, is a trend that has resulted in the emergence of a market place in which recruiters and job seekers communicate at an unimaginable scale."[1]

This data contain basic and personal data for job seeker, and this data must be protected during its transmission and reception via the platform. To achieve data protection and privacy from third party , We must employ the strongest and most advanced methods of cryptography encryption." Cryptography primarily concerned with the process of transforming a simple content into a complicated content and vice versa."[2]. The main objective of cryptography science is: "Confidentiality, Allows authentication, Maintains, Integrity, Prevents repudiation"[3]. The cryptography science depend on two-basic operation :encryption and decryption. These two basic operation use the varies types of algorithms. The differences of these algorithms depends on some criteria such as : effectiveness , number of key's, and time.

In cryptography science there are many of algorithms These algorithms are divided into two basic types As shown in figure1:First type, symmetric cryptography.Second type asymmetric cryptography. each of them have the specific properties .

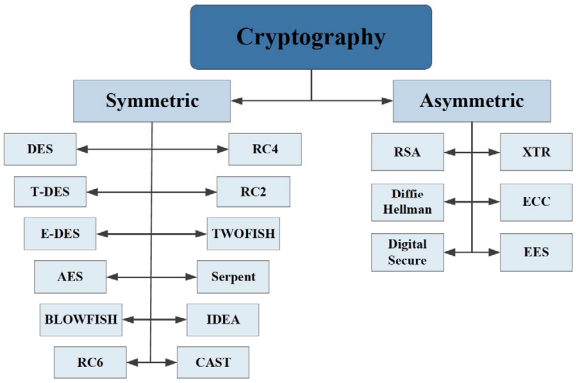

Fig. 1 The Classification of Encryption Algorithms.[4]

Basic type of cryptography

I. Symmetric cryptography

"A symmetric cryptography is an encryption and decryption algorithm that uses a single enigmatic key."[5]. The sender has access to this key. and receiver and it used it in secret way .Both sender and receiver must protect the key, because the key's privacy keeps information private, examples of algorithms used in symmetric encryption are: DES, AES,TWOFISH.

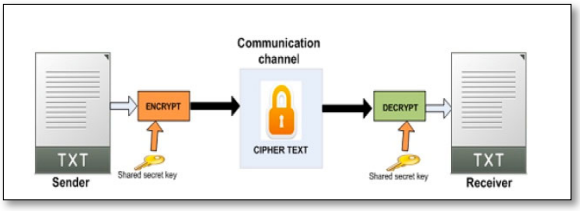

Fig. 2 Symmetric cryptography[6].

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.40

II. Asymmetric cryptography

"Asymmetric encryption is a type of encryption in which one key is being used to encrypt and the other is used it to decrypt."[5]. These key's defined as public and privet keys, the sender will use the different and separate key from receiver . Both of them must keep these key's secret, examples of algorithms used in symmetric encryption are: Diffie Hellman ,RSA,ECC.

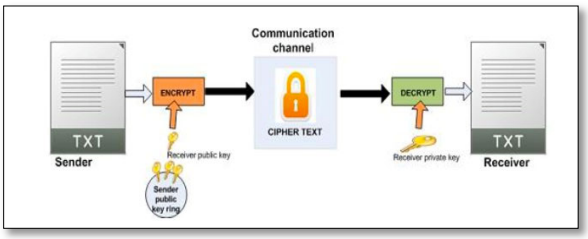

Fig. 3 Asymmetric cryptography[6].

There are new type of cryptography this type is hybrid cryptography

III. Hybrid cryptography

This type combined the previous types in one type by using one of them to encrypt the plain text and another one to encrypt the key , The strength of the two types also combines, and thus the encryption becomes stronger and unauthorized access to data is difficult.

The last type of encryption (hybrid cryptography)it is characterized by its frequent use, which is characterized by its strength, due to its combination of the two basic types of encryption. With the multiplicity of algorithms in each encryption method, it is difficult to identify a specific algorithm for hybrid encryption, each time a hybrid encryption is created from new algorithms. The benefits and drawbacks of hybrid encryption ,asymmetric encryption can slow down the process of encryption, but when combined with symmetric encryption, both types of encryption are improved. As a result, the submitted process is more secure, and overall system performance improves.

A hybrid encryption technique is presented in this paper. based on (AES+ Twofish +RSA) encryption is designed and developed. A hybrid cryptography consists of number of encryption algorithm types, each with a different level of strength. The idea of this research create the key by using AES algorithm ,and encrypt this key by using the Twofish algorithm , then encrypt generated key by using public key in RSA algorithm then, send the encrypted key with cipher text to receiver. To protect the personal data and prevent the external attacker , also increase the level of security in recruitment platforms.

The summarization of contribution of our work as follows:

1. We proposed the new hybrid encryption level by using (AES+ Twofish +RSA) in three level on encryption and decryption.
2. To secure and protect the personal data that store it in the platforms from the unauthorized to access data.
3. Ensuring the recruitment platforms is secure from the attackers.
4. Enhancing the throughput of the cryptography algorithm.
5. Increasing the data security by building hybrid algorithms.
6. Decreasing the processing time for encryption and decryption.

The remainder structured of paper as the following : Section 2: Related works , Proposed method in Section 3 Conclusions and Future works in Section4, and References in Section 5 .

2. Related works

In [7], The researchers proved the possibility of making hybrid encryption using both type of cryptography algorithms (Diffie-Hellman as symmetric type and RSA as asymmetric type), which differ in their strength to protect data while using a public communication channel. The methodology used in this research consists of two main steps: In the first step, using Diffie-Hellman algorithm to published two keys to both parties. In the second step, RSA is used to encrypt and decrypt data by creating a secret key pair (public and private key)at both side (sender, receiver), sender for encryption and the receiver for decryption. This algorithm is proven to be secure and thus reduces the risk of sharing key values on a public communication channel, and is considered a two-level encryption algorithm. One of the downsides is that it is multi-step and therefore takes a long time.

In [8], the researchers proved the protection of cloud computing applications. The methodology used in this research that the data are stored as encrypted form, and when they are retrieved, they are in decrypted form and decrypted of data in two ways, either through the AES

algorithm with Blowfish algorithm or via AES algorithm with Twofish algorithm. The AES algorithm with Twofish algorithm are more efficient in performance and faster in execution.

In [9], The researchers proved that the security of the data that is stored in the cloud computing can be improved through the use of the hybrid encryption feature through use the combined type of cryptography algorithms such as Homographic as symmetric encryption and Blowfish as asymmetric encryption. The encryption process begins with Homographic algorithm this algorithm works on bit therefore, it converts the input text to binary to encrypted after that bits are collected and converted into text. Then in the second step, the ciphertext in the previous step is encrypted again using the Blowfish algorithm. For decryption, reliance is placed on reversing the sequence of the encryption process, starting from the step in which the Blowfish algorithm is used, and the next step for decryption using the Homographic algorithm. The result of this hybrid algorithm proved that by using it on the cloud computing, it provides a security and better storage technology.

In [10],Through this research, the researchers applied a hybrid symmetric cipher via use of two algorithms (AES + Twofish). The encryption process is start by using the algorithm AES to encrypt the plain text, and then using the algorithm Twofish to encrypt the encrypted text again. As for the decryption process, it is completely opposite to the encryption process. The result of this research is proved that this hybrid encryption using these two algorithms (AES ,Twofish) is more secure and easy to implemented .

In [11],In this study, the researchers demonstrated the strength of data protection by using hybrid encryption in areas that require the exchange of data security. In this study, they used a comparison of the RSA and AES algorithms, as well as a hybrid approach that works on use of these two algorithms simultaneously. The methodology used in hybrid encryption in this study is that the plain text is encrypted using the algorithm of AES, and the secret key for AES algorithm is encoded with the RSA algorithm's public key. and then sending the public key and the encrypted text to the recipient to protect the body and key from any external attack, , and the recipient decrypting the RSA private key with the RSA public key, and then using that key to decrypt AES key then, AES key to decrypt the encrypted text. This study showed the result of the effectiveness of the hybrid algorithm in protecting the private key of encryption in addition to data protection and execution faster than other algorithms, is 67.47% faster than RSA algorithm and slower than ASA algorithm 32.39%.

In [12], Through this research, the researchers made a study of symmetric hybrid encryption, which greatly helps in solving encryption problems and increasing its efficiency. One of the most important factors to measure these algorithms used in symmetric encryption 1- Performance 2- Productivity 3- Time spent in the encryption and decryption process. The study is based on several types of algorithms that depend on symmetric cipher, including: (AES - Blowfish) and (AES-Twofish) that perform an experiment for each hybrid type. The study showed that the hybrid cipher used for algorithms (AES-Twofish) is the best in performance and throughput.

The summary of previous researches showed that the hybrid cryptography increase the level of data security in different aspect such as Cloud computing .In addition it's showed the various algorithms used it in hybrid algorithms and with this multiple type combination of algorithms the result of these studies it present the strength of these algorithms.

Proposed Model

The proposed model in this research, to encrypt and protect the personal data of users in electronic recruitment platforms is done through hybrid cryptography model, the hybrid cryptography model consists of three different types of encryption algorithms, which contain of different types of encryption: symmetric encryption, and asymmetric encryption. This section will contain subsections to explain the types of encryption algorithms used in this research and the mechanism of how the hybrid cryptography model work.

1. Algorithms using in the proposed model

1.1 Advance Encryption Standard (AES)

"is an encryption method used by US government agencies to secure sensitive but unclassified information; as a result, it is likely to be the mandated encryption standard for business contracts in the private market." [13]," Joan Daemen and Vincent Rijmen created the algorithm in 1998, which would be a symmetric block cipher."[14].It is symmetric cryptography algorithms, the key size (128,192, 256)bit's , in addition to the block size 128 bit's . As for security, it has a high security rate, in addition to its has high speed of execution. The result of the encryption process using this algorithm is equal to the original text ,

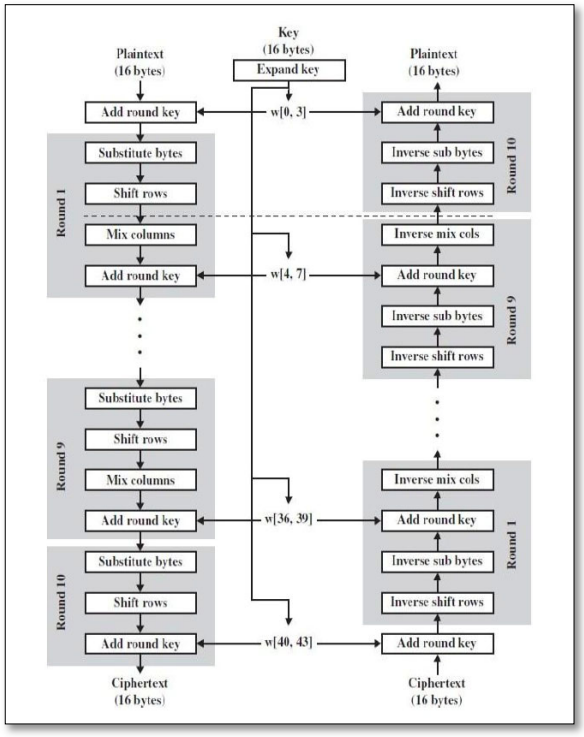

Fig. 4 AES algorithm structure[15].

- Block size: 128bits.
- Key size: 128,192, 256 bit's

Based on what is explained in [15].

As shown in figure 4 AES algorithm it's work depend on built around 12 round of a substitution-permutation network, or SP network. It consists of a sequence of connected processes, including substitutions (replacing inputs with certain outputs) and bit (row)shuffling (permutations). These steps, which contain both substitution and permutation, enhance the encryption's strength process.

1.2 Twofish

Is an encryption algorithm for increase the security for communication and transforming data via internet" Twofish is just a symmetric key algorithm including a the size of block 128 bits as well as a key size of 256 bits that is connected to the previous block cipher Blowfish." [16]. Regarding to symmetric key block cipher Twofish algorithm perform encryption and decryption process with the same key, as well as the size of key from 128,192, until 256 bit's. The calculation of Twofish encryption provides a high level of security[17].

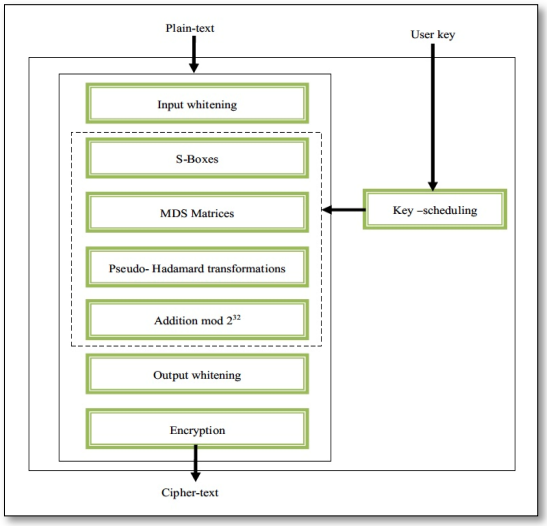

Fig. 5 Twofish algorithm structure[18].

- Block size: 128bits.
- Key size: 128,192, 256 bit's

As shown in figure 5 Twofish algorithm it's work depend on built around 16 round of Feistel network. It consists of a sequence of connected processes, including S-Boxes (replacing inputs with certain outputs) , matrices and transformation bit through using function. Twofish is a highly flexible deign. Start with sub-key generation until encryption of data this is due to wide range of design options, which is one of its main benefits over its competitors. [19].

1.3 Rivest-Shamir-Adleman (RSA)

Is an encryption algorithm for confidentiality. It is asymmetric key block cipher , which means that the encryption method use multiple and different key in encryption and decryption. " A varied size for block of encryption , and key size it have been used in RSA. It is asymmetric encryption system with an asymmetric (public key) cryptosystem depending on numerical theory."[20].

- Block size: 128,256,512 bits.
- Key size: 128,256,512 bit's

As shown in RSA figure 6 RSA algorithm it's work depend on generate two keys (private and public). It consists of a sequence of processes and functions for both encryption and decryption, including Random-number generator, Block of numbers.

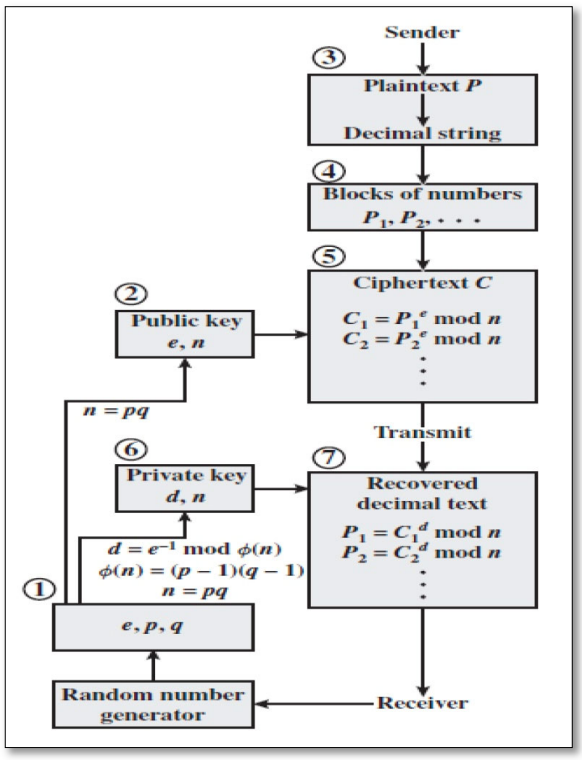

Fig. 6 RSA algorithm structure[20].

2. Methodology of proposed model

In this section, a detailed explanation of the process of the proposed model it's hybrid cryptography model for the protection of personal data of users of e-recruitment platforms by applying hybrid encryption algorithms from both type symmetric and asymmetric cryptography.in this research the proposed hybrid model focuses on three important factors : confidentiality , privacy and authentication, and encryption algorithms were selected based on these three factors. 1- confidentiality: to achieve the confidentiality need to using the symmetric encryption algorithms as mentioned in [21], for that reason the AES algorithm use it in this hybrid model because "AES algorithm is the quickest, most flexible, most scalable approach, and it is simple to use."[22] . 2- privacy:to achieve the privacy in the proposed hybrid mode applying the symmetric encryption algorithm has been added, Twofish algorithm. 3- authentication: to achieve the authentication need to applying asymmetrical algorithms for encryption , since the mechanism of RSA is used in this hybrid architecture. RSA use it at this hybrid model because "encryption with private key in RSA will help to achieve authentication about sender"[23].

In this research the hybrid cryptography model has two basic operations:

1- Encryption.
2- Decryption.

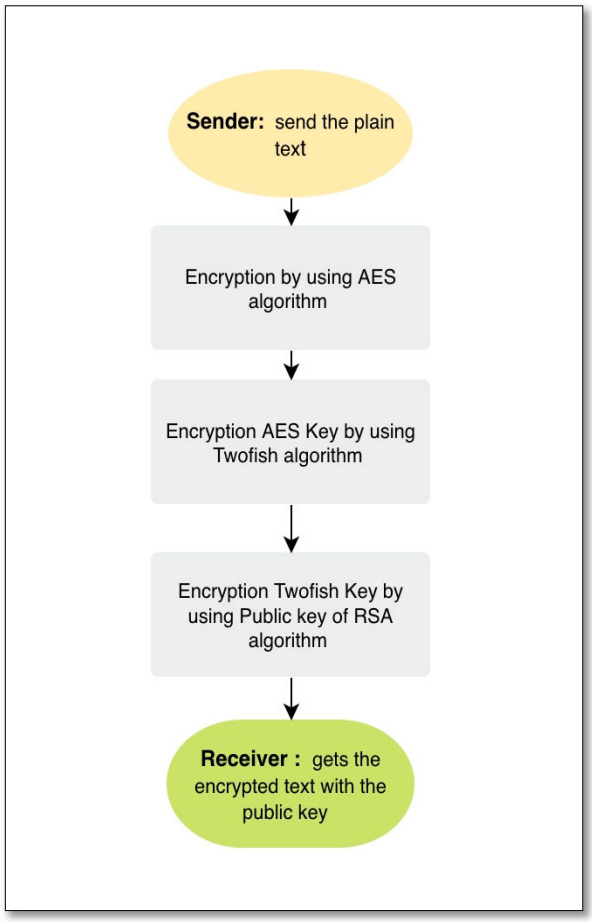

Fig. 7 Hybrid cryptography model (encryption process)

2.1 Encryption Process:

As shown in figure 7 the encryption process in hybrid model divided into three main steps:

2.1.1 *The process of encrypting the plain text(**Encryption by using AES algorithm**):*
The encryption process of the main text is done using the AES algorithm, due to the strength of this algorithm in encrypting the text in addition to its speed of execution.

*2.1.2 The process of encrypting the key of first algorithm(**Encryption AES Key by using Twofish algorithm**):*
The encryption process in this stage is decrypting AES key it's done using the Twofish algorithm, due to the strength, high speed and lightness of this algorithm in the encryption process.

*2.1.3 The process of encrypting the key of second algorithm(**Encryption Twofish Key by using the RSA algorithm's public key**):*
Encryption process in this stage is decrypting Twofish key it's done will use the RSA algorithm's public key,, due to the high security of this algorithm and its use of two encryption keys, in addition to the confidentiality that exists in this algorithm during the encryption process.

2.2 Decryption Process:

As shown in figure 8 the decryption prosecco in hybrid model divided into three main steps:

*2.2.1 The process of decryption the ciphertext(**Decryption to get Twofish Key by using the RSA algorithm's privet key**):*
Decryption procedure of the cipher text is done using the private of RSA algorithm.

*2.2.2 The process of decryption the key of second algorithm ciphertext(**Decryption Twofish Key to get AES key**):*
The decryption process in this stage is decrypting Twofish key it's done using the Twofish algorithm decryption process to get the key of AES algorithm.

*2.2.3 The process of decryption the key of second algorithm ciphertext(**Decryption AES Key to get the Plain text**):*
The decryption process in this stage it's done using the AES algorithm decryption process to get the Plain text.

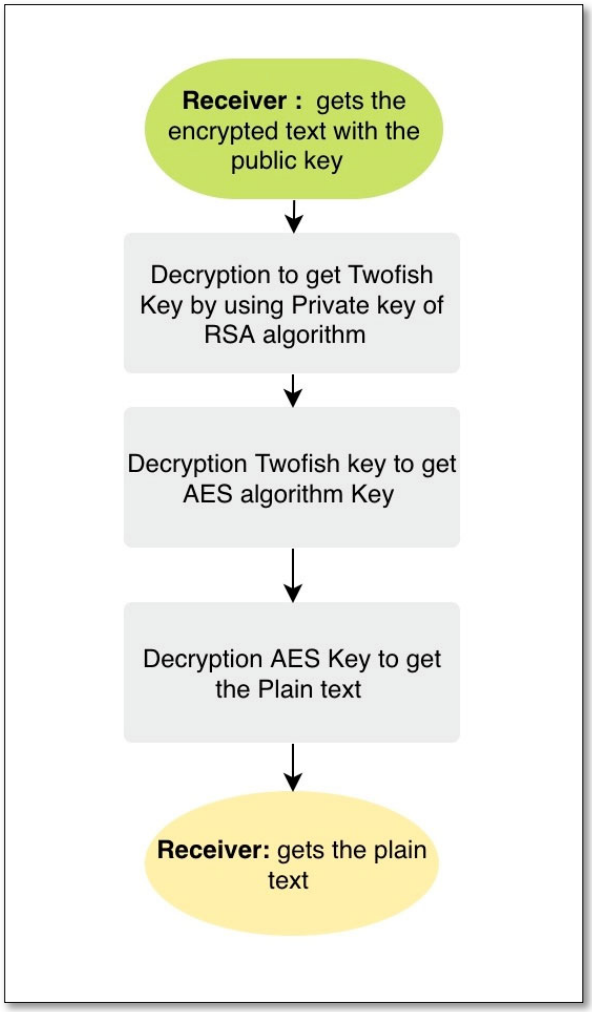

Fig. 8 Hybrid cryptography model (decryption process)

3. Result of proposed model

By experimenting with the work of encryption of personal data using the proposed model - hybrid encryption - it has proven the effectiveness of hybrid encryption in protecting and preserving the personal data of users of electronic recruitment platforms. The use of multiple algorithms has a major role in increasing protection and safety. Through the table 1, a simplified comparison is shown between all the algorithms used in this model, which include: number of Rounds, Block size, Security level, and key length. In turn, the effectiveness of the encryption algorithms has been proven for each one separately, thus demonstrating the strength of the proposed model,

Table 1: comparison for algorithm's in hybrid model.

Algor-ithm	*Rounds No.*	*Size Of Block*	*Secu-rity Level*	*Length Of Key*	*Ececu-tion Speed*
AES	10,12,14 Depend on Key length	128 bit's.	Most Secure with key =256 bit's	128,192,256 bit's	Fast with Key 128 Slow with key 256
TOW-FISH	16	128 bit's.	Secure	128,192, 256 bit's	Fast
RSA	1	128,256,512 bits. (variable	Good	128,256,512 bits. (depend on number of bits)	Average

data. which in turn makes maximum use of the benefits and strength of all the algorithms used. Each algorithm in this model was chosen based on several reasons and features. At the beginning of the encryption process, the AES algorithm is used as symmetric algorithm, which is one of the most powerful algorithms in encrypting the plain text "The significant benefits of block cipher are toughness (because to its quickness, this can encode large volumes of data quickly), and accessibility, while the major disadvantages are secret key usage and maintenance, as well as weak distribution privacy" as mentioned in [24] . It is classified as the execution speed of this algorithm increases as the size of the key is smaller. In our hybrid model we use the key length 128bits , in order to help take advantage of its strength in encryption in addition to increasing the speed in the implementation process, and as mentioned in the study "In comparison to RSA, AES is the most strong and fastest algorithm"[25], this is one of the reasons for using this algorithm, but it has a disadvantage, and it is "AES needs less storage memory" as indicated in [26]. Second, will talking about the two-fish algorithm, it is characterized by security and speed, and it was classified in one of the studies as " Because of its short encoding and decoding times, Twofish does have the greatest performance, closely with Blowfish then AES."[27], which helps to use it immediately after using the AES algorithm to increase the security ratio and raise the level of protection by encrypting the private key of the AES algorithm using Two-fish algorithm. Third, the use of the RSA algorithm, which is the highest in the security level because it is a type of asymmetric encryption , slower in the execution process i.e. "It takes long time in calculation for the encryption and decryption process" as indicated in [28]. **I**ts use in this research is for the purpose of using the type of asymmetric encryption to reduce attacks and increase the level of security and protection i.e. "Cryptographic techniques of many varieties provides excellent protection to data via network, and they also have a little downsides."[29]. Diversity of algorithms and encryption processes contribute to raising the level of protection and security and adding new ways to reduce attacks and protect

Conclusions and Future Works

In this research, a level of security and protection has been raised for the data that is transferred via the Internet, which is the data and users of employment platforms one of these data, through the use of Cryptographic, which is "Cryptographic algorithms play very important role in securing our digital data when one is communicating over internet"[30] Through this research, a proposed model was created consisting of a hybrid encryption system used to protect the personal data of users of electronic recruitment platforms. This model is based on the use of encryption algorithms of both basic types of encryption: symmetric and asymmetric encryption. Therefore, each algorithm was chosen on its merits and strength. The model first consists of using three algorithms. First, AES algorithm, which is a kind for symmetric algorithm for encrypting which employs identical key for encryption, decryption, and this algorithm is characterized by its strength and effectiveness for text encryption. Second, the use of the Twofish algorithm, which is also a type of symmetric encryption, and this algorithm is characterized by its high speed in implementation , so it works in this model to encrypt the AES algorithm's secret key. Third, the algorithm of RSA This algorithm it is type for asymmetrical cryptography where it employs two unique keys for encryption and decryption: a public key during encrypting process and a private key during decrypting process. It was used to encrypt the Towfish algorithm key through using the public key ,then the receiver of the ciphertext will have to decoding

the cipher, This would be summary of a encryption process. The decryption process performs all the steps of the opposite sequence of its encryption procedure , At first, receiver decrypts the cipher text that contains the key of the Twofish algorithm, by applying the RSA algorithm's private key. After that he obtains the Twofish algorithm key and uses the Twofish algorithm to decrypt it to obtain the AES algorithm's key, and afterwards he uses the AES algorithm's key to decrypt and get the plain text. This model has proven its effectiveness, as the algorithms were selected based on their strength, speed, and security level for each of them to achieve the general security of users' data. the proposed hybrid model in this research reach the level of security. In future, to increase the level of secure need to raising the number of iterations in the each encrypting algorithms to accommodate a degree of security desired.

References

[1] Pin, J., Laroden, M., & Saenz-Diez, I. (2001). *Internet recruiting power: opportunities and effectiveness*. Paper, Barcelona-Spain.

[2] Pritilata, Mahmood M.A. (2022) Strengthening Data Security Using Multi-level Cryptography Algorithm. In: Gandhi T.K., Konar D., Sen B., Sharma K. (eds) Advanced Computational Paradigms and Hybrid Intelligent Computing. Advances in Intelligent Systems and Computing, vol 1373. Springer, Singapore. https://doi.org/10.1007/978-981-16-4369-9_31

[3] Dayalan, M. (2019). Cryptography in Computer Security. *Journal Of Emerging Technologies And Innovative Research*, *6*(5). Retrieved 11 March 2022, from http://www.jetir.org.

[4] Abood, O., & Guirguis, S. (2018). A Survey on Cryptography Algorithms. *International Journal Of Scientific And Research Publications (IJSRP)*, *8*(7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978

[5] Sankaran P., S., & V B, K. (2019). Hybrid Cryptography security in public cloud using TwoFish and ECC algorithm. *International Journal Of Electrical And Computer Engineering (IJECE)*, *9*(4), 2578. https://doi.org/10.11591/ijece.v9i4.pp2578-2584

[6] Maqsood, F., Ahmed, M., Mumtaz, M., & Ali, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. *International Journal Of Advanced Computer Science And Applications*, *8*(6). https://doi.org/10.14569/ijacsa.2017.080659

[7] Deshmukh, S., & Patil, P. (2014). Hybrid cryptography technique using modified Diffie-Hellman and RSA. *(IJCSIT) International Journal Of Computer Science And Information Technologies*, *5*(0975-9646). Retrieved 11 March 2022, from http://www.ijcsit.com.

[8] Mandeep Kaur, N. (2016). Enhanced Security using Hybrid Encryption Algorithm. *International Journal Of Innovative Research In Computer And Communication Engineering*, *4*(7), 13001-13007. https://doi.org/10.15680/ijircce.2016.0407001

[9] Santoso, K., Muin, M., & Mahmudi, M. (2020). Implementation of AES cryptography and twofish hybrid algorithms for cloud. *Journal Of Physics: Conference Series*, *1517*(1), 012099. https://doi.org/10.1088/1742-6596/1517/1/012099

[10] Sajay, K., Babu, S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal Of Ambient Intelligence And Humanized Computing*. https://doi.org/10.1007/s12652-019-01403-1

[11] G. Chaloop, S., & Z. Abdullah, M. (2021). ENHANCING HYBRID SECURITY APPROACH USING AES AND RSA ALGORITHMS. *Journal Of Engineering And Sustainable Development*, *25*(4), 58-66. https://doi.org/10.31272/jeasd.25.4.6

[12] Et. al., P. (2021). Performance Analysis of Cascaded Hybrid Symmetric Encryption Models. *Turkish Journal Of Computer And Mathematics Education (TURCOMAT)*, *12*(2), 1699-1708. https://doi.org/10.17762/turcomat.v12i2.1506

[13] Kaur, M., & Kaur, J. (2017). Data Encryption Using Different Techniques: A Review. *International Journal Of Advanced Research In Computer Science*, *8*(0976-5697). Retrieved 1 April 2022, from http://Available Online at http://www.ijarcs.info/

[14] Patila, P., Narayankarb, P., D G, N., & S M, M. (2015). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. In *International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA*. http://www.sciencedirect.com Retrieved 1 April 2022, from.

[15] Joseph, D., & Krishna, M. (2015). Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms. *International Journal Of Advanced Research In Computer Science*, *6*(0976-5697). Retrieved 1 April 2022, from http://www.ijarcs.info

[16] Harahsheh, H., & Qatawneh, M. (2018). Performance Evaluation of Twofish Algorithm on IMAN1 Supercomputer. *International Journal Of Computer Applications*, *179*(50), 1-7. https://doi.org/10.5120/ijca2018916654

[17] Comparative Analysis of AES, Blowfish, Twofish and Threefish Encryption Algorithms. (2017), *10*. Retrieved 1 April 2022, from.

[18] Karuppiah, S., & Gurunathan, G. (2020). Secured storage and disease prediction of E-health data in cloud. *Journal Of Ambient Intelligence And Humanized Computing*, *12*(6), 6295-6306. https://doi.org/10.1007/s12652-020-02205-6

[19] Gehlot, P., R. Biradar, S., & P. Singh, B. (2013). Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL. *International Journal Of*

Computer Applications, *70*(13), 36-42. https://doi.org/10.5120/12024-8087

[20] Singh, G., & Supriya, S. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal Of Computer Applications*, *67*(19), 33-38. https://doi.org/10.5120/11507-7224

[21] Radhika, N. (2018). The Secure Data Transmission in Cloud Computing By Using Encryption Techniques AES and RSA. *International Research Journal Of Innovations In Engineering And Technology (IRJIET)*, *2*(2581-3048). Retrieved 5 April 2022, from http://www.irjiet.com.

[22] R. Pancholi, V., & P. Patel, D. (2016). Enhancement of Cloud Computing Security with Secure Data Storage using AES. *IJIRST –International Journal For Innovative Research In Science & Technology*, *2*(09). Retrieved 8 April 2022, from http://www.ijirst.org.

[23] Agrawal, A., & Patankar, G. (2016). Design of Hybrid Cryptography Algorithm for Secure Communication. *International Research Journal Of Engineering And Technology (IRJET)*, *03*(01). Retrieved 2 April 2022, from http://www.irjet.net.

[24] Harba, E. (2017). Secure Data Encryption Through a Combination of AES, RSA and HMAC. *Engineering, Technology &Amp; Applied Science Research*, *7*(4), 1781-1785. https://doi.org/10.48084/etasr.1272

[25] Arora, H., & Jain, J. (2019). Comparison among RSA, AES and DES. *International Research Journal Of Engineering And Technology (IRJET)*, *06*(4). Retrieved 25 April 2022, from http://www.irjet.net.

[26] Verma, R., & Sharma, A. (2020). Cryptography: Avalanche effect of AES and RSA. *International Journal Of Scientific And Research Publications (IJSRP)*, *10*(4), p10013. https://doi.org/10.29322/ijsrp.10.04.2020.p10013

[27] Ghosh, A. (2020). Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks, *07*(06). Retrieved 25 April 2022, from http://www.irjet.net.

[28] Ristiana, M. G. (2018). Hybrid algorithm of RSA and one time pad cryptography. ICCGANT.

[29] Jain, M., & Agrawa, A. (2014). Implementation-Of-Hybrid-Cryptography-Algorithm. *International Journal Of Core Engineering & Management(IJCEM)*, *01*(3). Retrieved 25 April 2022, from.

[30] Verma, R., & Sharma, A. (2020). Cryptography: A Comparative Analysis of AES and RSA Algorithms. *Mukt Shabd Journal*, *IX*(2347-3150). Retrieved 24 April 2022, from.