DETECTION OF ERRORS IN CRYPTOGRAPHIC DATA USING ARTIFICIAL INTELLIGENCE - A Survey

Prof.Santosh.Y.N, Gowthami Suresh, Kamankatta Ruthvik, N Darshan Raju, Supritha S
Sai Vidya Institute of Technology

ABSTRACT- There has been a rise in the number of in recent years proposed attacks against various cryptographic systems, some of which involve injecting deliberate errors during the computation process. This emphasizes how crucial data security is to guarantee that only the intended recipient can access the data and that unauthorized modification or change is avoided. Different algorithms and methods have beendeveloped to achieve this level of security, with the RSA algorithm being the most widely adopted public-key cryptosystem. However, hardware faults can be exploited to break cryptographic algorithms and retrieve the key, posing a significant security threat. This research intends to create a residue-based error detection techniquethat guards against such attacks in order to increase the protection of the RSA architecture. The scheme will analyze and detect errors and utilize AI techniques to evaluate and correct them, ensuring that information is in the expected format or area. This will enhance the safety of and reliability of cryptographic data, providing a robust defense against attacks.

Keywords:Cryptography,RSAalgorithm,Cipher

text , Encryption , Decryption, Data Security , Machine learning algorithm.

I INTRODUCTION

Cryptography is a technique to achieve confidentiality of messages.Crypto means hidden secret and graphy means to write.It involves transforming plain text into an encrypted message, which intended readers must subsequently decrypt back to plain text..This is mostly done to avoid adversaries or in order for it to be protected by an unintended user.Cryptography remains important to protecting data and users, ensuring confidentiality, and preventing cyber criminals from intercepting sensitive corporate information.Cryptography also secures browsing, such as with virtual private networks, which use encrypted tunnels, asymmetric encryption, and public and private shared keys.

II TYPES OF CRYPTOGRAPHY

1. Symmetric Key Cryptography:

Symmetric key cryptography, also referred to as secret key cryptography, is a method that encrypts and decrypts messages using the same key. The secretkey is used by the sender to encrypt the plaintext message before sending it to the recipient, who then uses it to decrypt the communication and view the original plaintext message. This method ensures that the message cannot be read by any individual withoutthe secret key and offers a safe and effective way to send messages between persons who share the key.

Stream Ciphers: It works on a single bit or byte any moment and constantly changes the key using feedback mechanisms.The algorithms used are RC-4, OTP, A5/1.

Block Ciphers: Block ciphers encrypt one block of fixed-size data each time. It will always encrypt a plaintext data block with the same key, the same ciphertext will be generated .The algorithms used are DES, AES, Blowfish.

2. Asymmetric Key Cryptography:

Public key cryptography is another name for asymmetric key cryptography.It encrypts and decrypts the data using private and public keys.Both

keys are interrelated in that you require both to decrypt and encrypt data, respectively.

RSA: It was the first asymmetric key cryptography algorithm and is still used the most. The algorithm, which is used in data encryption, digital signatures, and key exchanges, is named after its MIT mathematicians Ronald Rivest, Adi Shamir, and Leonard Adleman. It employs a big number that is produced by factoring two chosen prime numbers. The prime factors cannot be figured out by an adversary, making RSA particularly safe.

ElGamal: It is an asymmetric key cryptography technology that encrypts the message and uses public and private key encryption for safe communication between two parties. The discrete logarithms in a cyclic group are hard to find, so the cryptosystem assures that the message is protected from unauthorized access. To ensure that only the intended recipient can see the message, the sender encrypts it using the recipient's public key and decrypts it using the recipient's private key.This method provides a secure and efficient means of transmitting messages between parties without the need for them to exchange secret keys.

III LITERATURE SURVEY

[1] Nagalakshmi Gangupam,Chandra Sekhar Akkapeddi,Ravi Shankar Nowpada,Viswanath Kiran Nalam this article presents a new approach to enhancing the security of the RSA algorithm using a Laplace Transform-based cryptosystem. The proposed algorithm offers a potential method for enhancing data security in various applications.

[2] Jianbing N,Yong Yu,Kuan Zhang,Tingting Yang The paper provides a detailed description of the scheme, including the client-server interaction, the key generation and distribution, and the IB-PDP protocol. The authors also provide a security analysis of the scheme and demonstrate its efficiency through experimental results. Overall, the proposed scheme provides a practical solution for secure cloud storage that addresses the key challenges of data integrity and

The Algorithms used are RSA, Elliptic Curve Cryptography(ECC),ElGamal,Rabin.
privacy. The use of an identity-based cryptosystem simplifies key management, while the RSA assumption ensures the security of the scheme.

[3] Kaijie Wu ,Ramesh Kam,Grigori Kuznetsov, Michael Goessel, The paper provides a useful contribution to the field of concurrent checking for cryptographic algorithms by presenting a low-cost method for detecting errors in the implementation of AES. The proposed method can be implemented on a variety of hardware platforms and has the potential to detect both technical and deliberate faults, making it a valuable tool for ensuring the security of cryptographic chips.

[4] Hong Lai,Ming-Xing Luo,Josef Pieprzyk ,Jun Zhang,Lei Pan The paper presents a significant contribution to the field of quantum cryptography by proposing a new QKD protocol that offers high capacity and fast transmission speeds. The proposed protocol is also designed to be simple and robust against various types of attacks, making it suitable for practical implementations. The experimental demonstration shows that the protocol is capable of transmitting data at a high rate over a long-distance optical fiber link, which is a promising result for the future development of high-speed and secure communication networks

[5] Naglaa F. Saudy ,Ihab A. Ali ,Reda El Barkouky In the paper, a detailed analysis of potential errors during the implementation of elliptic curve cryptography (ECC) algorithms is presented. The study proposes a comprehensive set of error detection procedures to identify and correct errors that may pose a security threat to ECC-based systems. The paper stresses the significance of error analysis and detection in ECC implementations, particularly in applications where security is paramount. The proposed solution's implementation error detection procedures can help to safeguard the integrity and security of ECC-based systems, and their adoption is essential in any ECC-based system to ensure reliable and secure data transmission.

[6] Sergei Bauer,Stefan Rass,Peter Schartner The paper presents experimental results for several ARX ciphers, including SPECK, SIMON, and PRINCE. The findings indicate that the proposed technique can achieve error detection rates of up to 99.9999% with only a small increase in area and power consumption. The authors also compare their technique with existing error detection methods and show that it outperforms them in terms of error detection rate and overhead. Overall, the paper provides a practical and efficient technique for detecting errors in lightweight ARX ciphers, which can improve their reliability and security in practical applications

[7] MehranMozaffari-Kermani,Arash Reyhani Masoleh The authors evaluate the performance of the proposed scheme using simulation and synthesis results, and compare it with other fault detection schemes for AES. The findings indicate that the proposed scheme achieves high fault coverage with low overhead, making it suitable for low-power and high-performance applications. Overall, this article presents a novel approach to fault detection in the AES algorithm using composite fields, which can improve the security and reliability of the algorithm in various applications.

[8] Piyush Mishra,Kaijie Wu,Yongkook Kim This article provides a new perspective on the use of concurrent error detection schemes to protect symmetric block ciphers from side-channel attacks. The proposed schemes offer an effective and efficient solution for detecting faults in the implementation of ciphers and preventing the leakage of secret key information

[9]A new approach to error detection and correction has been proposed by Mohammad Wedyan, Hadeel Al-Zoubi, and Jaffar Atwan, which uses a genetic algorithm to optimize the parameters of a low-density parity-check (LDPC) code. The approach has shown promising results in simulations and has the potential for implementation in digital communication systems, offering an effective means of detecting and correcting errors in data transmission. By utilizing genetic algorithms to optimize the LDPC code parameters, the approach provides an efficient and robust solution for error correction, which can help to enhance the reliability and accuracy of digital communication systems.

[10]Peter Awon-natemi Agbedemnab,Edward Yellakuor Baagyere,Mohammed Ibrahim Daab proposed a powerful method that can identify and correct both single and multiple errors after and/or during computation and/or transmission provided the redundant moduli are sufficient enough. A theoretical analysis of the performance of the proposed scheme shows it will be a better choice for detecting and correcting computational and transmission errors to existing similar state-of-the-art schemes.

[11]J.Mathew,S.Banerjee,Mahesh.P,D.K.Pradhan the paper presents a method for multiple bit error detection and correction in GF arithmetic circuits using a modified Berlekamp-Massey algorithm. The proposed method is highly effective in detecting and correcting multiple bit errors in GF arithmetic circuits and outperforms other state-of-the-art methods. The method has potential applications in many digital signal processing applications and communication systems.

[12] Miodrag J. Mihaljevic this article presents a security enhanced encryption scheme and evaluatesits cryptographic security. The scheme is based on a combination of a substitution permutation network and a chaotic map. The evaluation of cryptographic security is performed using various statistical tests, including the frequency, block frequency, and runs tests, as well as the chi-square and autocorrelation tests. The findings indicate that the proposed scheme has high cryptographic security and can be used for secure communication in various applications. The author is affiliated with the Mathematical Institute of the Serbian Academy of Sciences and Arts. The article was received in June 2019, accepted in July 2019, and published in the same month.

[13] IgnacioAlgredo-Badillo,KelseyA.Ramirez-Gutier rez proposed solution consist a hybrid pipeline hardware architecture focusing on error and fault detection.The design of the hybrid-redundancy architecture has a pipeline structure based on five stages, where each stage is a set of data processing

elements connected in series, which are executed in parallel and filled with the same data blocks in a time-sliced manner for independently computing five results.The pipeline architecture is used for processing the same data block, focusing on the detection and correction of errors.

[14] Ahmed Drissi Tangier, Morocco , the paper provides a comprehensive overview of the use of error-correcting codes in cryptosystems and their security. The author presents attacks against code-based and McEliece cryptosystems and discusses their advantages and disadvantages. The paper highlights the importance of error-correcting codes in cryptography and their potential for post-quantum cryptography.

[15] Onyeyili T.I, Azubogu A.C.O, Okafor C.S ,the paper describes a simple cryptographic data security algorithm for wireless sensor networks. The proposed algorithm aims to provide confidentiality, integrity, and authenticity of data transmitted by the sensor nodes in the network. The algorithm is designed to be lightweight and suitable for resource-constrained wireless sensor nodes.

[16] Emmanuel A. Adeniyi ,Peace Busola Falola ,this paper proposes a secure method for sharing sensitive data using two cryptographic algorithms, RSA and ElGamal, along with hash functions. The RSA algorithm is used for key generation and distribution, while ElGamal is used for data encryption. Data integrity and message authentication are both achieved through the usage of hash functions. A mechanism for rescinding access to shared data is also included in the suggested approach in the event of unauthorized access or user termination. The authors assert that their technology enables efficient and secure data sharing for private information in a range of contexts, including healthcare and banking.

[17] Alexander Volokh, Gunter Neumann, the paper presents a method for automatic detection and correction of errors in dependency treebanks using a combination of rule-based and statistical approaches. The proposed method is highly effective in detecting and correcting errors in the treebank and out performs other state-of-the-art methods. The method has potential applications in natural language processing tasks such as parsing and information extraction.

[18] Lavanya K. Galla, Venkata SreeKrishna Koganti, the paper presents a detailed description of the implementation of the RSA public-key encryption algorithm on an FPGA using VHDL. The authors demonstrate the high performance of the FPGA implementation and show that it provides significant advantages over software-based implementations of RSA.

[19] Narendra Babu T, Fazal Noorbasha, the paper presents a high-security cryptographic system that combines the AES block cipher with the Reed-Solomon error correction code and includes a mechanism for detecting and correcting errors in the input data. The proposed system provides high levels of security and reliability and can be implemented on an FPGA for high-speed encryption and decryption of data.

[20] Mamathashree A M, Remya K and Santhosh Kumar B J, the paper presents a study on fault attacks on the RSA public key cryptosystem and proposes a method to detect such attacks. The proposed method is effective in detecting fault attacks and can be used in conjunction with other countermeasures to protect against such attacks.

[21] Christophe Giraud , the paper proposes a method to protect RSA implementations against fault attacks and simple power analysis by adding redundancy to the computation of the modular exponentiation operation. The method provides protection with a negligible increase in hardware resources and can be applied to other cryptographic algorithms as well..

[22] Alberto Battistello and Christophe Giraud , In the article, the authors introduce a new type of

fault attack called infective fault attack, which is based on the injection of faults in the computation of AES using a maliciously modified key schedule. They analyze the effectiveness of this attack by testing it against different AES implementations and discussing the results. The authors also propose a countermeasure to prevent infective fault attacks by modifying the key schedule algorithm.

[23] Alessandro Barenghi, Guido Bertoni, The authors describe how low voltage fault attacks work by introducing a controlled fault into the execution of the RSA algorithm. By doing so, an attacker can manipulate the computation andrecover the secret key used for encryption or decryption. The authors present a case study of a low voltage fault attack on a 1024-bit RSA implementation and show how it can be used to recover the private key with a relatively small number of fault injections.

[24] Mona M. Elamir, May S. Mabrouk's The article presents a secure framework for Internet of Things (IoT) technology based on a combination of RSA and DNA cryptography. The authors propose a novel approach to secure data transmission in IoT devices using a combination of public key cryptography and DNA cryptography. The RSA algorithm is used to generate the public and private keys, while the DNA cryptography is used to encode the data for secure transmission.

[25] Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir The article provides a thorough introduction of a number of cryptographic encryption techniques, including RSA and Elliptic Curve Cryptography (ECC), as well as symmetric-key encryption algorithms like DES, AES, and Blowfish.The writers offer a thorough examination of the into the strengths and limitations of each, enabling readers to make informed decisions about which algorithm to use in specific scenarios.

[26] Helen Thackray, Chris Richardson, Huseyin Dogan, Jacqui Taylor, John McAlaney The article provides insights into the challenges of collecting data from a secluded community and the ethical considerations that need to be taken into account when conducting research with this population. The article may be of interest to researchers and practitioners working in the field of cybersecurity and social psychology.

[27]R Manjula and R Anitha this article presents a new approach to identify the encryption algorithm used in a given data using a decision tree. The proposed approach offers a promising solution for improving the accuracy and efficiency of identifying encryption algorithms used in various applications.

[28] Mahnaz Sinaie and Vahid Tabataba Vakili the article provides a useful contribution to the field of information security by proposing a secure arithmetic coding scheme with error detection capabilities. The article may be of interest to researchers and practitioners working in the fields of data compression, information security, and error detection.

[29] Eduardo Berrueta 1 , Daniel Morato 2 , Eduardo Magaña1 , And Mikel Izal1 this article provides a comprehensive overview of the current state of detection techniques for cryptographic ransomware and highlights the need for continued research in this area to address the evolving threat landscape of ransomware.

[30] Mr. Akash V. Malasane* , Prof S. P. Bhonge in this article reviews the use of metamorphic encryption to secure data. Metamorphic encryption is a technique that transforms the original data into another form, making it difficult for attackers to intercept or read. The article discusses various metamorphic encryption techniques and their applications in different fields.

IV. TABLE

PAPER	ALGORITHM	KEY SIZE	EXISTING SYSTEM	PROPOSED SYSTEM	RESULT
1	RSA and Laplace	1024, 2048, 4096	Enhancement to the RSA formula by incorporating the Laplace transform cryptosystem	Aims to improve the data security and confidentiality by adding an additional layer of encryption using the Laplace transform.	The proposed system can enhance the security of cryptographic systems without significantly increasing the computational overhead.
2	RSA	2048, 4096	technique used to ensure the integrity of data stored on untrusted cloud storage systems.	Aims to improve the efficiency and security of PDP by using an identity-based approach, which eliminates the need for a certificate authority and simplifies key management.	The suggested plan achieves excellent security guarantees with low computational overhead, making it a practical solution for secure cloud storage.
3	AES	128,192,256	Based on the Hamming code, which adds redundant bits to the data being encrypted to detect errors.	Uses a modified Hamming code that has lower overhead and can detect more errors. This system also incorporates an error-correcting code to correct errors that are detected.	Detecting errors in the implementation of AES that can improve the security and reliability of the system without significantly increasing the cost or overhead.
4	Parity-check algorithm.	does not mention the specific number of bits.	based on the BB84 protocol, which is a widely used quantum key distribution protocol	Uses a high-capacity protocol called theB92 protocol, which can transmit more information per qubit than the BB84 protocol	novel technique for implementing high-capacity quantum cryptography that combines the advantages of DPS and QPS protocols with efficient error detection, making it a practical solution for secure communication in a wide range of applications.
5	ECC	does not mention the specific number of bits.	ECC is susceptible to errors that can lead to significant security breaches	presents a novel approach for error detection in ECC that uses a matrix representation of the elliptic curve points.	improve the reliability and security of ECC, making it a more practical solution for secure communication in various applications.
6	Parity-Based Concurrent Error Detection for Lightweight ARX Ciphers	does not mention the specific number of bits.	involves adding redundancy to the data or using checksums to verify the integrity of the data	uses parity-based error detection that can be used for any data size and requires minimal additional memory.	The proposed method can improve the reliability and security of the system without significantly increasing the cost or overhead.
7	AES	128	current methods for fault detection AES and propose a new lightweight fault detection scheme that can detect faults in the S-box and Mix Columns operations of the algorithm	uses composite fields, which can enhance the performance and reduce the hardware cost within the system.	The suggested approach can improve the reliability and security of the system without significantly increasing the cost or overhead, making it a practical solution for fault detection in AES implementations.

8	It does not focus on a specific symmetric block cipher algorithm, but instead presents a generic approach that can be applied to various algorithms.	does not mention the specific number of bits.	Refers to the symmetric block ciphers that are vulnerable to fault-based side-channel attacks. These attacks exploit the fact that the cipher computation is performed in hardware and introduce errors in the computation to reveal the secret key. The current system does not comprise any CED scheme to prevent these attacks.	The proposed system introduces two CED schemes to protect the cipher against fault-based side-channel attacks. The first scheme is based on the comparison of two replicas of the cipher computation, while the second scheme uses parity prediction to detect any errors in the computation.	The results showed that both schemes were effective in preventing fault-based side-channel attacks on symmetric block ciphers.
9	The paper does not mention a specific error detection and correction algorithm that is used in conjunction with the genetic algorithm.	does not specify the exact number of bits	The existing system in this context refers to traditional error detection and correction techniques such as parity checking, checksums, cyclic redundancy checks (CRC), and Hamming codes.	The proposed system introduces a new approach to error detection and correction using a genetic algorithm. The authors proposed a genetic algorithm-based method to automatically generate error detection and correction codes that can be used to protect digital systems against errors.	The results showed that the genetic algorithm-based approach outperformed the traditional techniques in terms of error detection and correction capabilities and system overhead, and concluded that the proposed approach is a promising solution for error detection and correction in digital systems.
10	Chinese Remainder Theorem (CRT)	Bits used in the algorithm depends on the size of the input data. The authors tested their proposed technique on different sizes of input data ranging from 8 to 32 bits.	The existing system refers to traditional error detection and correction techniques such as Hamming codes, CRC, and parity checking.	The proposed method introduces a new approach to error detection and correction using RRNS and proposed scheme that can be utilized for RRNS based error detection and correction cryptographic and stenographic applications.	The proposed scheme was effective in detecting and correcting errors in the transmitted data and outperformed the traditional techniques in terms of error detection and correction capabilities.

V. EXISTING SYSTEM

The following several papers and projects that have focused on analyzing and detecting errors in cryptographic data. However, it is worth noting that some of these efforts have only focused on error detection and not on error correction. Various existing systems utilize artificial intelligence to detect errors in cryptographic data. Machine learning techniques are used by these systems to find patterns and abnormalities in the data. They can be used to identify various errors, including tampering, data corruption, and key exchange attacks, among others. These AI-based systems are particularly useful in detecting complex errors that may not be detected through manual inspection, and they can provide a high level of accuracy in identifying and isolating errors in cryptographic data. Nonetheless, it is crucial to ensure that any identified errors are also corrected, to ensure the security and integrity of the data.

VI. PROPOSED SYSTEM

In this particular project, our goal is not only to analyze and detect errors in cryptographic data but also to correct them using AI techniques. By employing machine learning algorithms and utilizing accurate data, we aim to develop a system that can enhance the security and reliability of cryptographic data. This system will identify any errors in the data, determine their root causes, and apply appropriate

corrections to ensure that the data is error-free. The end goal is to develop a system that can be trusted to deliver precise and safe cryptographic data to all parties involved.

VII. CONCLUSION

In this project, we are working towards achieving error-free cryptographic data using AI and cryptography methods. In recent years, tremendous progress has been made in using artificial intelligence to find mistakes in cryptographic data. Machine learning, deep learning, and neural networks are just a few of the AI techniques that have been used to find mistakes and anomalies in encrypted data. By spotting problems that manual inspection or more conventional error detection methods could miss, thisstrategy has demonstrated encouraging results and can help avoid security breaches.The use of AI algorithms in this context provides a high level of accuracy in detecting and isolating errors in cryptographic data, which is essential for ensuring thereliability and security of the data.

REFERENCES

[1] Nagalakshmi Gangupam,Chandra Sekhar Akkapeddi,Ravi Shankar Nowpada,Viswanath Kiran Nalam The International Journal of Recent Technology and Engineering (IJRTE) published an article in July 2019 that explores the potential of "Enhancing data security by combining the RSA algorithm with Laplace Transform Cryptosystem".

[2] Jianbing N,Yong Yu,Kuan Zhang,Tingting Yang "Identity-Based Provable Data Possession From RSA Assumption for Secure Cloud Storage" Ieee Transactions On Dependable And Secure Computing, Vol. 19, No. 3, May/June 2022.

[3] Kaijie Wu ,Ramesh Kam,Grigori Kuznetsov, Michael Goessel "Low Cost Concurrent Error Detection for the Advanced Encryption Standard" Itc International Test Conference 0-7803-85802/04 $20.00 Copyright 2004 IEEE .

[4] Hong Lai,Ming-Xing Luo,Josef Pieprzyk ,Jun Zhang,Lei Pan "Fast and simple high-capacity quantum cryptography with error detection" 13 April 2017 .

[5] Naglaa F. Saudy a,⇑ , Ihab A. Ali b , Reda El Barkouky c "Error analysis and detection procedures for elliptic curve cryptography" 26 November 2018.

[6] Sergei Bauer,Stefan Rass,Peter Schartner "Generic Parity-Based Concurrent Error Detection for Lightweight ARX Ciphers" August 14, 2020. Digital Object Identifier 10.1109/ACCESS.2020.3010555

[7] MehranMozaffari-Kermani,Arash Reyhani-Masoleh "A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields" Ieee Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 19, No. 1, January 2011.

[8] Piyush Mishra,Kaijie Wu,Yongkook Kim "Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers"Ieee Transactions On Computer-Aided Design Of Integrated Circuits And Systems, Vol. 21, No. 12, December 2002 .

[9] Mohammad Wedyan, Hadeel Al-Zoubi and Jaffar Atwan Prince Abdullah Ben Ghazi "Error Detection and Correction Using a Genetic Algorithm"International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184, Volume 8, Number 2 (April 2019) .

[10] Peter Awon-natemi Agbedemnab,Edward Yellakuor Baagyere,Mohammed Ibrahim Daab "Single and Multiple Error Detection and Correction using Redundant Residue Number System for Cryptographic and Stenographic Scheme" Asian Journal of Research in Computer Science 4(4): 1-14, 2019; Article no.AJRCOS.53646 .

[11] JMathew,S.Banerjee,Mahesh.P,D.K.Pradhan "Multiple bit Error Detection and Correction in GF Arithmetic Circuits" Article · December 2010 DOI: 10.1109/ISED.2010.28

[12] Miodrag J. Mihaljevic "A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security"Mathematical Institute, The Serbian Academy of Sciences and Arts,17 July 2019 .

[13] Ignacio Algredo-Badillo Luis Alberto Morales-Rosales ,Daniel Pacheco Bautista ,and

Claudia Feregrino-Uribe,"Hybrid Pipeline Hardware Architecture Based on Error Detection and Correction for AES" Sensors 2021.

[14] Ahmed Drissi "The Security of Cryptosystems Based on Error-Correcting Codes" 2020 DOI: http://dx.doi.org/10.5772/intechopen.93784 .

[15]1Onyeyili T.I, 2 Azubogu A.C.O, 3Okafor C.S, 4Oranugo C.O. "Simple Cryptographic Data Security Algorithm for Wireless Sensor Network"International Journal of Innovative Science and Research Technology ISSN No:-2456-2165 Volume 6, Issue 5, May – 2021 .

[16] Emmanuel A. Adeniyi 1, Peace Busola Falola 1, Mashael S. Maashi 2, Mohammed Aljebreen 3 and Salil Bharany4* "Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions" 2022, 13, 442. https://doi.org/10.3390/ info13100442.

[17] Alexander Volokh, Gunter Neumann "Automatic Detection and Correction of Errors in Dependency Treebanks"Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics Portland, Oregon, June 19-24, 2011.

[18] Lavanya K. Galla, Venkata SreeKrishna Koganti, Nagarjuna Nuthalapati "Implementation of RSA" 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT).

[19] Narendra Babu T*, Fazal Noorbasha*, Leenendra Chowdary Gunnam** The International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 2, April 2016 features a research paper entitled "Implementation of High Security Cryptographic System with Improved Error Correction and Detection Rate using FPGA.

[20] Mamathashree A M, Remya K and Santhosh Kumar B J "Fault Analysis Detection in Public Key Cryptosystems (RSA)" International Conference on Communication and Signal Processing, April 6-8, 2017, India .

[21] Christophe Giraud "An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis".

[22] Alberto Battistello and Christophe Giraud " Fault Analysis of Infective AES Computations" Article · August 2013 DOI: 10.1109/FDTC.2013.12

.[23]Alessandro Barenghi, Guido Bertoni "Low Voltage Fault Attacks on the RSA Cryptosystem" .

[24] Mona M. Elamir1*, May S. Mabrouk2 and Samir Y. marzouk "Secure framework for IoT technology based on RSA and DNA cryptography" Elamir et al. Egyptian Journal of Medical Human Genetics (2022) 23:116 https://doi.org/10.1186/s43042-022-00326-5.

[25] Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir "A Survey on the Cryptographic Encryption Algorithms" (IJACSA) International Journal 2017 .

[26] Helen Thackray, Chris Richardson, Huseyin Dogan, Jacqui Taylor, John McAlaney "Surveying the Hackers: The Challenges of Data Collection from a Secluded Community" June 2017 Conference: 22nd Annual CyberPsychology, CyberTherapy & Social Networking Conference.

[27]R. Manjula and R. Anitha "Identification of Encryption Algorithm Using Decision Tree*" Department of Mathematics and Computer Applications, PSG College of Technology, Coimbatore, India .

[28] Mahnaz Sinaie and Vahid Tabataba Vakili "Secure Arithmetic Coding with Error Detection Capability" Hindawi Publishing Corporation EURASIP Journal on Information Security Volume 2010, Article ID 62152

[29] Eduardo Berrueta 1 , Daniel Morato 2 , Eduardo Magaña1 , And Mikel Izal1 "A Survey on Detection Techniques for Cryptographic Ransomware

[30] Mr. Akash V. Malasane* , Prof S. P. Bhonge "A Review Paper On Survey Of The Secure Data By Using Metamorphic Encryption" Malasane, 2015.