Volume 9, Issue 5, May – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY785

Report on Contemporary Cyber Security Issues

Sarah Fawzia[1]; Mujiba Shaima[2]; Norun Nabi[3]; Mazharul Islam Tusher[4]; Md Nasir Uddin Rana[5]
Estak Ahmed[6]; Sushanta Saha[7] and Sarder Abdulla Al Shiam[8]
[1]Department of Data Science, Edith Cowan University, Western Australia.
[2]Department of Computer Science, Monroe College, New York, USA.
[3]School of IT, Washington University of Science and Technology (WUST), Virginia, USA.
[4]Department of Management-Business Analytics, St Francis College, USA.

Abstract:- The contemporary landscape of cybersecurity is fraught with challenges, necessitating a keen understanding of evolving threats and robust defense mechanisms. By examining the Data Encryption Standard (DES) as a key element therein, this paper explores the complexities of cryptography, a foundational element of contemporary security paradigms. Securing confidential data from unwanted access is one of the many facets of cryptography, the art of secure communication. In the context of data protection, DES is recognized as a foundational cryptographic algorithm, valued for both its historical importance and ongoing applicability. But as technology moves more quickly and cyberattacks get more complex, DES's effectiveness is called into question, which has sparked debate about whether it is still sufficient in modern security scenarios. Here, in this paper we explore the complexities surrounding cryptography and DES, elucidating their strengths, limitations, and implications for cybersecurity practices. By examining current trends and emerging challenges, it endeavors to offer insights into mitigating risks and fortifying defenses against cyber threats in the digital age.

Keywords:- *Cryptography, Data Encryption Standard (DES), Advanced Encryption Standard (AES).*

I. INTRODUCTION

The world is now increasing so rapidly that people are now trying to connect technology with the human brain and try to read them [1] but the way Elon Musk is planning to read human brain that needs to have secure. Again, all this research data should be secure. Digital connectivity and the growth of sensitive data is more important than ever to protect information from cyber threats. Cybersecurity is now considered as the vanguard against a relentless tide of malicious actors seeking to exploit vulnerabilities in digital systems. The complex science of cryptography, which serves as the fundamental basis for protecting data integrity and communication in the world of digital media, is at the center of this defense [2]. Every organization that uses the internet has ongoing and increasing concerns about cybersecurity [3] and giant companies like Amazon [7], Google, Facebook, Twitter and other day by day is improving their security system to ensure a secure infrastructure. Modern computers have built-in strong defense systems to prevent unauthorized, vulnerable attacks. But technology is more advanced now, as is the human brain. Hackers and cybercriminals have become smarter to break these computer's built-in defense systems. This is only the beginning; there are a plethora of other challenges that also require proper attention, such as cyberterrorism and cyberwarfare. As previously said, the resilience of any entity utilizing the cyber realm is dependent upon the robustness of their systems and their ability to defend against off-target attacks. One of the essential building blocks for reaching this objective is cryptography. Any data, whether stored locally or transferred across a network, is susceptible to abuse and manipulation if it falls into the wrong hands. This is something that should be avoided at all costs. Making the data worthless to any unauthorized user who manages to access it is the best approach to stop this from happening, and here is where cryptography comes into play [5][6].

Cryptography is a method of protecting information and communications using codes so that only those for whom the information is intended to read and process it [2]. Here, our research and review work embark on a comprehensive exploration of contemporary cyber security issues, with a particular lens on cryptography and the enduring legacy of the Data Encryption Standard (DES). Cryptography, both an art and a science, encapsulates the methodologies and algorithms utilized to encode and decode information, ensuring its confidentiality and authenticity. Within this preview, DES emerges as a seminal cryptographic algorithm, renowned for its historical significance in providing robust data encryption. However, amidst the relentless evolution of cyber threats and technological advancements, questions persist regarding the efficacy and relevance of DES in contemporary security contexts.

Through a critical examination of cryptography and DES, this review endeavors to illuminate the prevailing challenges and emerging trends shaping the cybersecurity landscape. By delving into the complexities of cryptographic protocols and encryption standards, it aims to provide insights that empower stakeholders to fortify defenses and navigate the ever-evolving cyber threat landscape with resilience and foresight.

II. METHODOLOGY

We employed terms associated with cryptography, Data Encryption Standard (DES), Advanced Encryption Standard (AES), and modern cybersecurity to do a comprehensive search throughout IEEE Xplore, ACM Digital Library, and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY785

ResearchGate. Reviewing abstracts from 2015 to 2024, we concentrated on current works; complete texts are available upon request. Only relevant papers on current cybersecurity issues, as well as those that shed light on the advantages, disadvantages, and uses of DES and AES, were considered for inclusion in the study. According to preset criteria, we eliminated redundant and pointless research. Our methodological technique synthesized the major findings of this paper. It also guaranteed that current research would be included.

III. CRYPTOGRAPHY

Cryptography is the process of safeguarding information by converting it into an incomprehensible form, referred to as cipher text, through the utilization of mathematical methods and keys. This technique guarantees that only authorized entities possessing the right cryptographic keys can gain access to and comprehend the content [4].

Diagram 1 helps us to comprehend the cipher. Here, Adith and Jenny were speaking while encrypting their exchange using cryptography. Only they have the keys to encrypt and decrypt the conversation. Keys are kept in a safe place. Since he lacks the secret key, if someone else intercepts the encrypted communication, they will be unable to decipher anything. Consequently, some cipher text algorithms exist. The outcome of applying that technique to our plain text or plain data is a cipher, which is a type of unintelligible data. We can get the original data if we incorporate that encryption in the algorithm using a secret key. Therefore, the major objective of the encrypted text is to protect confidentiality.

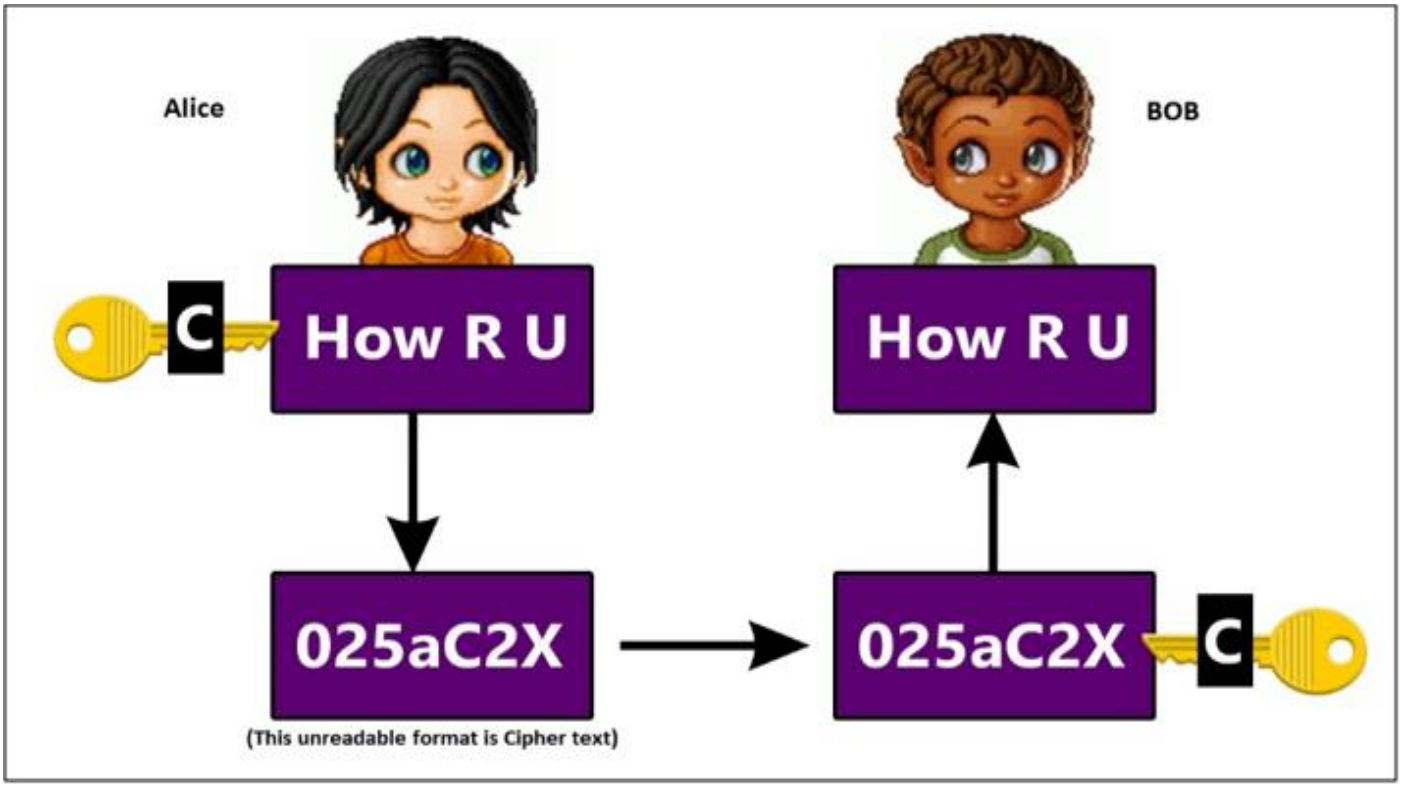

Diagram 1: Cipher Text Basic Understanding

The world is home to a large number of cryptographic algorithms that have been around for a long time. In this piece of writing, we are going to investigate a particular kind of cryptographic algorithm that is known as Data Encryption Standard (DES). Some of these algorithms have some significant flaws that could be exploited by malicious actors.

➢ *How DES Works*

A known flaw or weakness is present in the Data Encryption Standard (DES), which is a classic cryptographic technique. A symmetric-key cryptographic algorithm was created by IBM in the 1970s. This algorithm is a symmetric-key algorithm. The data is encrypted and decrypted with a key that is 56 bits in length.

Consider diagram 2 as an example, where an individual intends to transmit a private letter to another person while ensuring that no unauthorized individuals have access to its contents. Therefore, it is necessary for us to personally visit the post office and explicitly request that they mail it in a secure manner. The post office employs a robust encryption method to safeguard the letter's contents during transmission, ensuring that only the intended receiver possesses the means to decipher it.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY785

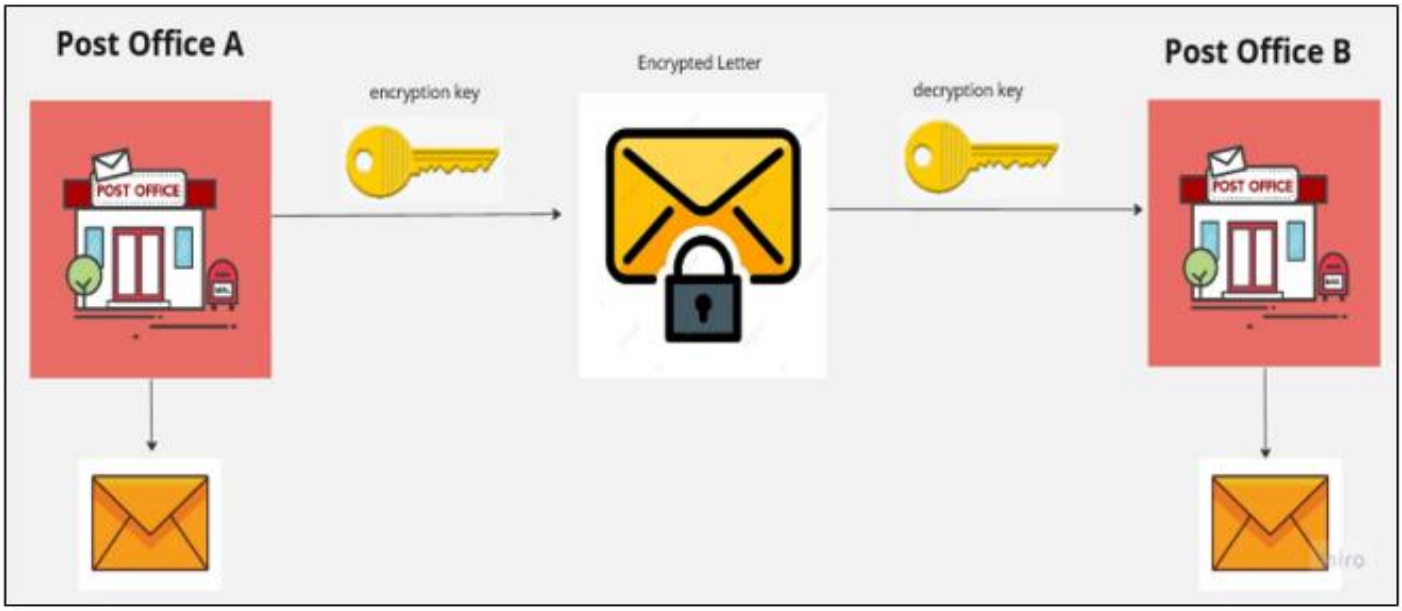

Diagram 2: Understanding how DES Works

➢ *This is how this could be Connected to DES:*

- *Key Generation:*

The post office possesses a primary key which they utilize to create an exclusive key for every combination of sender and recipient. This key is analogous to the key utilized in DES encryption.

- *Encryption:*

The mail is encrypted by the post office using DES encryption, with the sender-recipient key serving as the encryption key. This is analogous to the encryption process of the Data Encryption Standard.

- *Mail Sorting:*

The letter that has been encoded is organized and dispatched to the intended post office. This is analogous to the data transmission phase in the Data Encryption Standard (DES).

- *Decryption:*

Upon arrival at the destination post office, the letter undergoes decryption using the identical key employed for encryption. This is analogous to the decryption process of the DES.

- *Delivery:*

The deciphered letter is then conveyed to the intended receiver, who is able to peruse its contents. This resembles the result obtained by the DES decryption procedure.

In general, the procedure of mailing a confidential letter through the postal service bears resemblance to employing the DES method for the encryption and decryption of data. Both processes entail the utilization of a distinct key to safeguard a valuable entity from unwanted entry while it is being transmitted.

➢ *DSE Algorithm*

As we already mention above, DSE uses a 56-bit key for data encryption and decryption. Using this 56-bit key DES takes an input block of 64-bit plain text and creates 64-bit cipher text block. So, creating 16 subkeys, each of which is 48-bits long is DSE algorithm's first step. Then, it encodes 64-bit block of data. Next performing permutation, and some calculation steps it gets an output. And at the last it decrypts the output to get the actual result (Diagram 3).

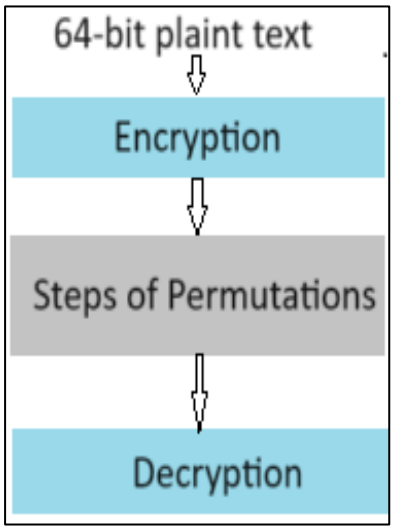

Diagram 3: DSE Algorithm Steps

➢ *Vulnerability in DES*

DES is a symmetric cryptographic algorithm, wherein the sender and receiver employ an identical key for both encryption and decryption. The key size of the Data Encryption Standard (DES) is a mere 56 bits, rendering it susceptible to brute force attacks.

Diagram 4 depicts the susceptibility of DES to brute force assaults, which can be elucidated using a straightforward analogy involving a door and key.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY785

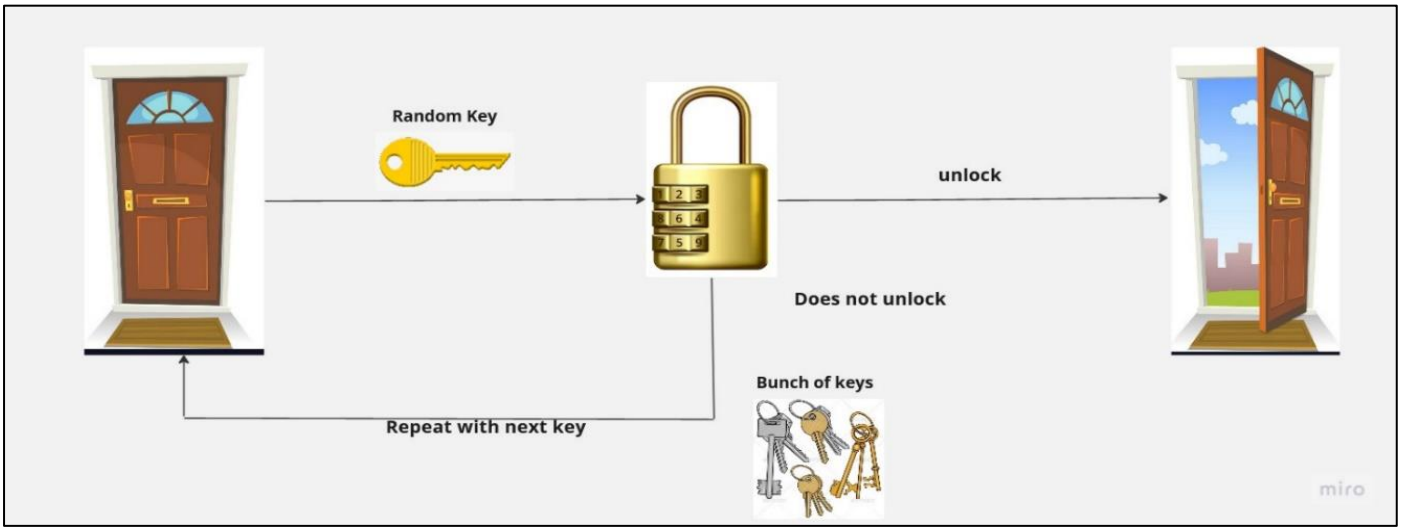

Diagram 4: Vulnerability of DES to Brute Force Attacks Understanding

Suppose we possess a locked door that can only be unlocked using a particular key. Nevertheless, the key can be readily replicated, and there exists a finite number of potential keys capable of unlocking the door. Below is a sequential graphical depiction of the process of utilizing a brute force attack to get access to the door:

- *Key Generation:*
  The assailant creates a key by either generating a random key or attempting to use a replicated key from a known source.

- *Key insertion:*
  The assailant places the key into the lock and attempts to rotate it in order to open the door.

- When comparing with the target, if the door does not unlock, the attacker will attempt to use a different key until they locate the correct one.

- *Continuing with the Next Key:*
  If the door remains locked, the intruder produces or attempts another key from a collection of known keys and repeats the procedure until the correct key is discovered.

As evident, the assailant systematically produces or attempts several keys in order to get access through the door. In the event that a key fails to function, individuals attempt alternative keys till they locate the appropriate one.

This analogy demonstrates the susceptibility of DES to brute force assaults. The limiting key size of DES restricts the amount of possible keys available for data encryption and decryption. Utilizing the computational capabilities of contemporary technology, one can execute a brute force assault on DES by systematically attempting each conceivable key until the accurate one is discovered, analogous to employing many keys to unlock a door.

Diagram 5 illustrates a real-life scenario where a hacker attempts a brute force assault on the Data Encryption Standard (DES) used in ATM transactions. The hacker's strategy involves intercepting the communication between the ATM machine and the bank's network. Subsequently, they would document the encrypted transaction and endeavor to decipher it by employing a key-guessing program that systematically tests every conceivable key combination until the accurate one is identified.

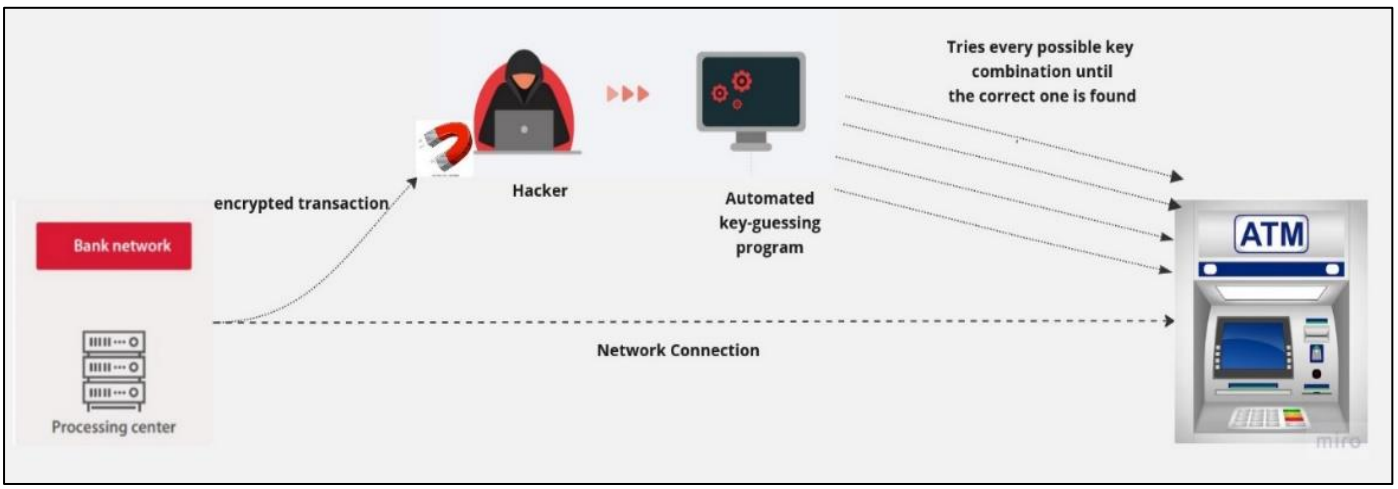

Diagram 5: A Brute Force Attack on DES used in ATM Transactions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY785

In addition, the usage of weak keys is another vulnerability that DES has. When a weak key is used, the output is always the same, which leaves it open to attacks. This makes it prone to attacks. Similarly, in Diagram 5, we can observe that the same output is generated each time the same key is used to open the door. This is the case even if the attacker uses a weak key to unlock the door. Since this, the lock is susceptible to attacks since an adversary can use the same weak key to unlock the lock each and every time.

IV. COMPARISON WITH A MODERN ALTERNATIVE

The Advanced Encryption Standard (AES) is a contemporary and secure alternative to DES that is currently employed. AES is a type of encryption algorithm that uses a single key to both encrypt and decrypt data in fixed-size blocks [8].

The key length is a fundamental distinction between DES and AES. The Data Encryption Standard (DES) utilizes a constant key length of 56 bits, but the Advanced Encryption Standard (AES) allows for key lengths of 128, 192, and 256 bits. AES possesses a significantly greater key space compared to DES, rendering it more impervious against brute force attacks. Furthermore, AES employs a more intricate key expansion algorithm compared to DES, rendering it more challenging to deduce the round keys from the original key.

Another distinction lies in the quantity of rounds employed during the encryption procedure. DES employs a total of 16 encryption rounds, whereas AES utilizes either 10, 12, or 14 rounds, depending on the length of the key. The increased intricacy of AES renders it more challenging to decipher compared to DES.

AES employs a distinct form of substitution-permutation network (SPN) in contrast to DES. The Substitution-Permutation Network (SPN) used in AES is characterized by a higher level of complexity and security compared to the Data Encryption Standard (DES), resulting in increased resistance against assaults. Furthermore, AES typically exhibits higher speed compared to DES, rendering it more effective for implementation in contemporary systems.

In general, AES improves upon the limitations of DES by employing a longer key size, additional encryption rounds, a more robust SPN (Substitution-Permutation Network), and a more secure key expansion method. The enhancements implemented in AES have significantly enhanced its security and efficiency compared to DES. As a result, AES has become the prevailing encryption algorithm adopted by several companies and governments worldwide.

V. CONCLUSION

In a nutshell, our investigation of cryptography, specifically the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), has revealed the lasting importance and changing nature of secure data encryption. DES, previously acclaimed as the stronghold of cryptographic protection, is now overshadowed by the more resilient AES, illustrating the continuous advancement of technology and the need for adaptable security solutions.

The comparison between DES and AES has clearly shown that AES is superior in terms of computing efficiency, resilience to brute-force assaults, and greater applicability across various security scenarios. Although DES still holds historical importance and is used in specific situations, its vulnerabilities against contemporary cyber threats are becoming more evident.

As we are exploring the complex realm of cybersecurity, it becomes clear that AES is the leading example of cryptographic strength, representing the result of years of research and advancement in industry. By adopting AES and using its powerful encryption capabilities, individuals and organizations can strengthen their security measures against the constantly changing threat environment, guaranteeing the privacy and reliability of valuable data in an increasingly digitalized society. In the ongoing battle between cybersecurity and cyber threats, it is crucial that we remain watchful and adaptable in order to stay ahead.

REFERENCES

[1]. Mujiba, S., Nurun, N., Md, NUD., Md, TA., Estaq, A., Mazaharul, IT., Moushumi, HM., Quazi, SM. (2024). Elon Musk’s Neuralink Brain Chip: a review on ‘Brain-Reading’ device. Journal of Computer Science and Technology Studies. 6(1). 200-203. https://doi.org/10.32996/jcsts.2024.6.1.22

[2]. Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer. https://doi.org/10.1007/978-3-642-04101-3

[3]. Singh, S. (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Doubleday.

[4]. National Institute of Standards and Technology. (2001). Federal information processing standards publication 197: Advanced encryption standard (AES). https://csrc.nist.gov/publications/detail/fips/197/final

[5]. M. Das, X. Tao, and J. C. P. Cheng. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. Automation in construction.126 https://doi.org/10.1016/j.autcon.2021.103682

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY785

[6]. S. Naeem, M. Zubair, M. M. Ahmed, A. Ali, S. Anam (2023). Network security and cryptography challenges and trends on recent technologies. Journal of Applied and Emerging Sciences.13(1). https://journal.buitms.edu.pk/j/index.php/bj/article/view/546

[7]. Mujiba, S., Estaq, A., Md, NUD., Md, TA. (2024). An optimizing business process: a comprehensive analysis of amazon inc.'s information architecture. European Journal of Engineering and Technology Research. 9(1). 47-58. https://doi.org/ 10.24018/ejeng.2024.9.1.3097

[8]. Ratnadewi, Roy P. A, Yonatan H, Saleh A, & Setiawan M I. (2016). Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). Journal of Physics. v954. 10.1088/1742-6596/954/1/012009