International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 1 September 2020

Data Encryption and Decryption Techniques for a High Secure Dataset using Artificial Intelligence

B. Herawan Hayadi[1], Edy Victor Haryanto[2]
[1]Universitas Ibnu Sina, Indonesia,
[2]Universitas Potensi Utama
b.herawan.hayadi@gmail.com[1], edyvictor@gmail.com[2]

Abstract: The science of extracting patterns, trends, and actionable data analysis detail of large data sets. The growing existence of data in different county's servers with structured, semi-structured, and unstructured data formats, such as the data. The demands of these are not met by conventional IT infrastructure, a modern landscape of "Data Analysis." For these reasons, several companies are turning to as a possible solution to this unmet commercial business, Hadoop (open-source projects). The amount of data collected by organizations, especially unstructured data, as businesses burst, Hadoop is increasingly emerging as one of the primary alternatives to store and execute operations on that data. The secondary question of data analysis is defense, the rapid increase in internet use, the dramatic shift in acceptance of people who use social media apps that allow users to generate content freely and intensify the already enormous amount of the site. In today's firms, there are a few stuff to bear in mind when starting innovation ventures for big data and analytics. In the business environment, the need for secure data analytics tools is mandatory. In the previous paper, they implemented a high profile dataset using the encryption technique. Using only the encryption method, cannot secure data very highly. There is a chance of knowing the original data to the third party. To reduce the above issues, the paper introduces a new technology called "Artificial intelligence". Using this new technology, paper can achieve more security for data sets. Using both encryption and decryption models in artificial intelligence can solve the drawback in an existing paper. This will provide the data with either a significant degree of authentication analyzed to ever be. The provision of data analytics is pursued with attribute-based restricts Data extraction allows enabled. This model will work better than the present model. In both security and sensitive economic restructuring, data analytical tools.

Keywords: Data analysis, Hadoop, big data, dataset, encryption, artificial intelligence, and decryption.

I. INTRODUCTION

The focus of Artificial Intelligence (AI) is now at the heart of the Industry of cybersecurity. AI is a word that exceeds these relatively Days, but it applies to a few approaches that can be very useful. Precious for protection. It requires machine learning, Algorithms that can recognize threats and respond to them as It'll happen. They can predict whether the incoming data is likely to be safe or malicious. Many assaults are occurring these days, Uh, not new. These attacks have happened with some other attacks. Before, people in several other locations. Additionally, if we build a database that collects all the data ever generated gets existed and feeds it to neural networks, it is possible to attack Prevented although it takes place. In classification one, we can look at the learning styles and preferences to going to have to decide whether it is malicious or not.

A few other procedures include these procedures. Detecting data processing issues immediately in the everyday world Way-Time To fix incoming data as a stream that collects and then every single point uses an algorithm that can track what pattern of action that's become common and looks good. Deviations that may mean that a hack or a hack has been made Trespassing. And then there's a third one that utilizes a process named programming probabilistic. This is a database suite of Languages for which a computer algorithm is not recorded with Deterministic regulations, but probabilities can be expressed and there are some very interesting analytics testing to malware genealogy so that we can map the roots constantly reminding potential responses to these infectious viruses.

Neural networks and algorithms for deep learning can process a Quickly, a lot of data and features of all sorts of things are discerned, If the pictures or texts on the internet are used and characteristics for deciding whether or not

the knowledge is malicious. Utilizing past knowledge, they can learn and never again make mistakes. That is complex and hard to understand neural networks for humans. The output is not concrete. Accordingly, conventional protection. The method is deteriorating. increases in the use of AI in cyber defense velocity and scalability. An integral aspect of society is data communication. Privacy policy to preserve privacy, proper data security protection of access, authenticity, and availability has been a real concern Issue in the communication of data.

The need for strong encryption from prying eyes is greater than ever before, today in the e-age. Cryptography, encryption science It plays a critical role in communication around the mobile phone, e-commerce, pay-TV, sending private e-mails, transmitting Capital accumulation details, and touches on many elements of lives daily. A cryptosystem specifies a pair of transformations of data encryption and decryption-called. Encryption is performed To the plain text, i.e. the knowledge to be transferred to ciphertext formation, i.e. encrypted data using an encryption key. To convert, decryption uses the decryption key to encrypt text into plain text, i.e., the original data. The Symmetric cryptosystem, where the key for encryption and if the decryption key is the same, it can be broken easily if You may find the key used for encrypting or decrypting. In 1976, Whitfield Diffe and Martin Hellman of Stanford University proposed the Public Key cryptosystem to implement a security mechanism. It utilizes a pair of similar keys, one for encryption and another for encryption with decryption. One key, referred to as the private key, is held confidential and another classified as a public key is revealed.

Artificial intelligence (AI), intelligence is embodied by computers, unlike the natural intelligence displayed by humans and animals. Leading AI textbooks classify the profession as the study of "intelligent agents": any system That perceives its atmosphere and takes the best course of action its chance to effectively accomplish that goal. The word 'artificial intelligence' is now used to describe machines (or computers) in colloquial terms This tries to imitate "cognitive" human soul-related functions, such as "learning" and "problem-solving. When computers become increasingly capable, the notion of AI, a phenomenon known as the AI effect, remains increasingly capable", often excludes tasks thought to require “intelligence”.

In Tesler's Theorem, a quip says that AI is something that has not yet been finished. For example, optical character recognition, which has become a common technology, was also excluded from manufacturers due to be AI. Typically known as AI, modern computer capabilities include a strong perception of a voice signal, competing in strategic game systems (such as chess and Go) at the highest level, autonomously driving vehicles, Intelligent routing, and military simulations in the content distribution system. Artificial intelligence was founded as an academic discipline in 1955, and many waves of excitement have been encountered in the years since, followed by disappointment and loss of funding (known as an 'An I winter'), New approaches, innovation, and renewed financing have been followed. AI science has been divided into sub-fields for much of its history, which frequently struggle to engage with each other.

The emphasis of these sub-fields is on technical aspects, such as basic goals (e.g. 'robotics' or 'machine learning'), the use of particular technologies ('logic' or artificial neural networks), or fundamental philosophical differences. Sub-fields also focused on government conditions (specific organizations or researchers' work). AI research's conventional problems (or goals) include reasoning, representation of information, planning, learning, processing of The players to convey and exploit objects, natural language, sight, and one of the field's long-term targets is general intelligence. Distributing the questionnaires, computational intelligence, and innovative symbolic techniques AI are among the approaches. In AI, several instruments are used, including search and mathematical optimization versions, artificial neural networks, and statistical, probability, and economic methods. Computer science, information processing, mathematics, psychology, linguistics, philosophy, and many other areas are the basis of the AI field.

The field was built on the assumption that "human intelligence" can be so adequately interpreted that a computer can reproduce it. "This raises metaphysical arguments about the mind and ethics " of producing human-like intelligence-endowed artificial beings. Since antiquity, myth, fiction, and philosophy have discussed these problems. Engineers and developers have also come up with a number where to collect And gather extra information, such as asking users to accept a cookie, tag friends in screenshots, rate a product or play a game made to find street monsters. Data has become the "New Oil." We built an unparalleled global data infrastructure. As AI

was finding its way at the same time, connect with this infrastructure any browse, buy something, play a game, or check your inbox, bank balance, or social media feed to read the news. access the internet. It's not only A physical one for systems and cables but also one for applications, such as social networks and microblogging websites. Data-driven AI both feeds on and shifts this electric grid- it is hard to envisage one without the other.

And it is impossible to live without them all. In needed to conduct, intelligent machines need to collect data, often personal data. This fundamental argument ultimately transforms them into surveillance instruments: They understand our rankings, our history of browsing, and our social networks. Protective applications (i.e. anti-virus, detection of intrusion) Systems, etc.) are part and parcel of an operating system, e.g. Administrators of scripts, browsers, text processors, etc. Nonetheless, also There is no need for the new protective software devices, ensure that the climate for computers and/or computing is 'Secure'.

II. LITERATURE SURVEY

An algorithm for encrypting-decrypting images using RSA algorithm structures is proposed as the most cryptographically susceptible to illegitimate decryption identified with images with certainly explicit edges. The use of components of the RSA algorithm as coefficients of any linear-quadratic affine transformation is suggested. Compared to the RSA algorithm, the proposed algorithm has greater cryptographic stability[1].

An encryption method, a method of decryption, and a related apparatus are embodiments of the present application. The method of encryption includes: generating a keystream where the keystream is used to encrypt a piece of data to be encrypted in an initial layer-3 message, and small data would be included in the data set to be encrypted; generating by performing an exclusive OR operation on the originally layer-3 message keystream and the initial layer-3 message, the initial layer-3 message in which the paid is encrypted; and the initial layer-3 message in which the data component is encrypted, where the initial layer-3 message provides a flexible encryption indication, and the encryption indication is used to signify that the pay to be encrypted in the initial layer-3 message is encrypted[2].

Attribute-based encryption (ABE) enabled encrypted data to be handled with fine-grained access. The use of The indirect revocation procedure in which a Key Generation System (KGC) regularly transforms key data update information via a public channel to all data users is a feasible and important approach to handing over revocation in ABE. Unfortunately, the latest RABE systems are prone to attacks on decryption key transparency that The identity-based culture has been well studied. In this article, we introduce a new RABE method called re-randomizable piecewise key generation by allowing a data user to generate data post-randomize The combined secret key and key update to access the decryption key, and even though the client uses both the decryption key and the key update, the secret key is unrecoverable. A new primitive is then listed, RRABE, which can support both re-randomizable piecewise key generation and ciphertext delegation, which is called re-randomizable attribute-based encryption. In terms of generating decryption key exposure resistance, we also refine the inrush current model for RABE and present a generic RABE construction from RRABE. Finally, we have a limited RABE program that often strengthens decryption key exposure resistance and ciphertext delegation simultaneously by introducing our generic transformation [3].

Zhang, Y, et.al [4], proposed, Imposed on a piece-wise linear map, a symmetric key image cryptosystem is presented. In this cryptosystem, the meaning of encryption and the decryption procedure is the same. Both comprise the same scrambling operations linked to plaintext once, twice diffusion, and four times 180-degree matrix rot. In the framework, Encryption and the mechanism of decryption are the same in this cryptosystem. The same scrambling operations linked to plaintext are used in both. The results of the simulation and comparison analysis show that the proposed system has many advantages, such as the high speed of encryption/decryption, vast keyspace, high efficiency to the key, strong plaintext Sensitivity, sensitivity and selectivity to cipher-text, good statistical properties of glyph images, and entropy of large cipher-text information. So it is time to identify the proposed scheme on real communications.

The use of fluorescent inks, due to its convenience and low cost, has become the most feasible technology for information privacy applications. However, fluorescent inks are proud of either Whereas preserved stimulus-responsive inks are kept in a single skin tone, ambient light, or UV light. Full-color stimuli-responsive inks for information coding, encryption, and decryption are

validated for the first time, based on the ease of application and Perovskite quantum dots conversion. Under ambient and UV light, the details printed by the halide salt solution is invisible, but after spraying a similar developer, it becomes readable under UV light. Besides, for many years, even decades, primitive knowledge can be maintained. It can still be kept on file for multiple weeks, even after the decryption process. More interestingly, the luminescence can be powered off / on by the Introduction of Butyl amine and acetic acid as reagents, respectively, for encryption and decryption. Written data can be encrypted and decrypted in this way, which shows great potential for network security applications [5].

In the information system, security is a priority, especially in the exchange of data that is confidential or confidential. The material that would be going to be It is important to correctly safeguard the party entitled to the information, to not even fall into the hands of those who have no right to such knowledge. Concerning information. One way to ensure the security of information can also be to use cryptographic techniques communicated in a system. The art and science of removing information from third parties is cryptography. In cryptography, an agent with a private key can translate plaintext data into unique and unreadable data (ciphertext) and can use each ciphertext in plaintext form with its private key. Development of the system (Lifecycle of System Development) may mean developing a new system in partnership with either the old system to replace the old system. The prototyping technique to develop a Nur algorithm cryptographic method that is implemented using the programming language used is Montage (MASM32). In Nur Aminuddin's Encryptor, there are two data reading techniques, namely the encryption technique (the technique of encoding data from the original into unreadable code) and decryption technique (the mechanisms of reading unreadable codes become unreadable) Readable) Encryption technique is installed by adopting a new cryptography technique that preserves the symmetric key free so that the symmetric key is free. Encryption performance relies only on the key and does not depend on whether or not citizens remain aware of the algorithm[6].

In almost every domain, stability has become a critical course in science. In many other communication fields of inquiry, cybersecurity has taken the front seat. Everyone needs to maintain their information or data secure from fraudulent activity. This paper explores a hybrid approach for the application of advanced encryption in communication. Watermarking and cryptography include the approaches used. For images, video, audio, and text, this encryption and decryption technique can be used. We have used the graphic in this paper as the encryption and decryption info. Mishra, S, et al.[7] illustrates the use of the Secure Force (SF) algorithm for encryption and decryption process. Using MATLAB, simulation work was carried out. Experimental properties were also evaluated, also including PSNR, MSE, and Entropy.

Cities are increasingly turning to technical technology to solve financial, biological, phenotypic, and many other questions. The revolutionary invention of Smart Cities strongly promotes this prospect by embracing the Internet of Things (IoT) combination of sensors and Big Data. This data rapid increase opens up new opportunities as well as economic prospects In planning and operating towns. Even though Artificial Intelligence (AI) processing of Big Data The urban fabric will contribute greatly to, dimensions of sustainability and living ability shouldn't ever, however, be justified based on physical ones. This article examines AI's urban potential and proposes a new structure that combines Advanced technology and cities are recognized as essential for the smooth integration of smart cities while ensuring the integration of key dimensions of community, metabolism, and governance in Compliance to Target 11 for Sustainable Growth and the Latest Urban Agenda. Allam, Z., & Dhunny, Z. A[8], pointed at policymakers, data scientists, and engineers, proposed striving to enhance the adoption of Artificial Intelligence and Big Data in Smart Cities to improve the living ability of the urban fabric while supporting social growth and opportunities.

Our access protocol draws its inspiration from the authentication scheme for MIT-Kerberos in which a client For that local service server, who needs to communicate with that service server needs a session key and ticket wanting to meet. To provide authentication, the principles of key distribution are now used. The data privacy transmitted is Achieved using algorithms for encryption and decryption. We introduce using the Hash functions here to meet the requirements of complete a task, generate the public and private keys for each session in order. In this project, we wish to build a security protocol independent of the mobile routing protocol. Adhoc networks to support primary communication with added infrastructure. Here, separate from the complaints in Traditional wired networks take a few more parameters,

such as node and node durability. Due to a single communication channel, the openness to attacks by external intruders had increased. Solid initial communications between the mobile node and the main distribution center are made through to the collected directly. Another result of the proposed protocol is that the surveillance-paying mobile nodes are dedicated dynamically, authentication keys thus solve the issues associated with static passwords around existing methods. We use artificial intelligence puzzles for this purpose to have upgraded authentication [9].

III. PROPOSED WORK

The method of converting information is encryption, so it is to all but the end line, unintelligible. The method of encrypted data transformations to make it intelligible again is decryption. A mathematical feature that is used for encryption or decryption is a cryptographic algorithm, sometimes called a cypher. Two similar functions are used in the majority of cases, One to encrypt and the other to decrypt. The capacities to remain encrypted information secure is not based on the generally recognized cryptographic algorithm for most modern cryptography, But on a number called a key that must be used with the algorithm to achieve an encrypted consequence or decrypt previously encrypted records. It is easy to decrypt with the proper password. It is very difficult to decrypt without the correct key and, in some of these cases, for all practical purposes, impossible.
The parts following introduce the use of encryption and decryption keys.

- Symmetric-Key Encryption
- Public-Key Encryption
- Key Length and Encryption Strength

Symmetric-key encryption

The Symmetric-key alternative makes it possible to build the encryption key from the decryption key and vice versa. Both encryption and decryption use the same key for most symmetrical algorithms as shown in figure 1.

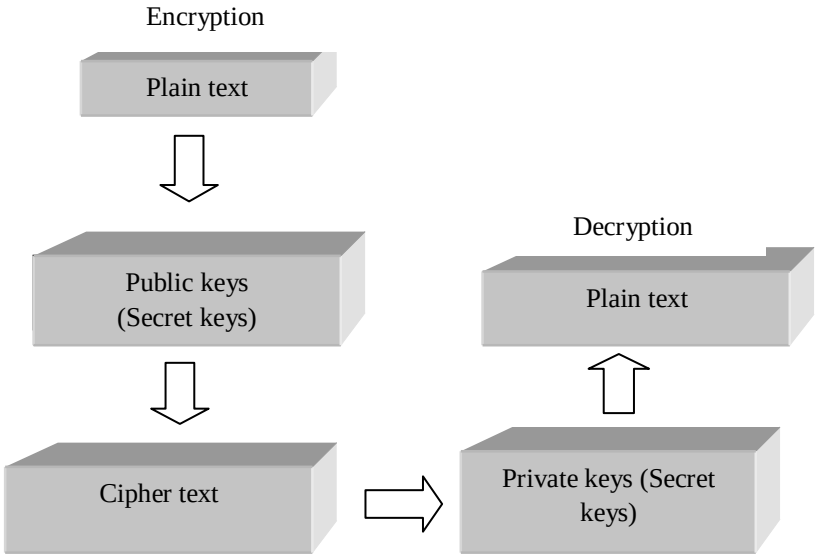

Figure 1. Block diagram of symmetric key encryption

Symmetric-key encryption applications can be extremely effective, even as there is no considerable time delay for users as a result of encryption and decryption. A degree of authentication is also produced from symmetric-key encryption, Therefore it is not practicable to unlock Specifics encrypted to every other symmetric key with one Symmetrical key. Key. Therefore, as long as the spherical key is secured, encryption is often used by parties to encrypt communications as long as the intercepted messages begin to make sense, each party may indeed be guaranteed that it is communicating with the other. Symmetric-key encryption is only powerful if the encryption is two sides involved hold the symmetric key secret.

It affects both confidentiality and authentication if the key is found by anyone else. A party with an unacceptable Not only can the symmetric key decrypt messages sent with that key, but new messages can be intercepted and sent as if they came from one of the two parties using the key originally. In the protocol for SSL, which is In authentication, tamper detection, and encryption over TCP / IP networks, symmetric key encryption plays an important role. SSL uses public-key encryption techniques there too, which are discussed in the next section.

The source The text is encrypted with the encryption of a symmetric key, or a symmetric key is used, and the scrambled text is delivered through the Internet to its destination. Employing the same key, the shuffled text is decrypted into the original text. To achieve this, the key and the encryption and decryption algorithms are always circulated between the source and its destination. Up until recently, this was the type used encryption system. A mutual key with symmetric key encryption shares the source and the destination. The famous key is secret, but it is not the encrypting and decrypting algorithm.

Types

Encryption through symmetric-key should use either cryptographic algorithms or hash algorithms

- Authentication systems encrypt a message's digits (typically bytes), or letters (in substituted cyphers) one at a time. Vigenère Cipher is an example.
- A number of bits are captured by encryption algorith ms and encrypted as a single particle, padding the plainte xt to A multiple of the size of bricks. In the Advanced Encryption Standard (AES) algorithm, endorsed by NIST in December 2001, 128-bit blocks are mostly used.

Implementations

Camellia, Salsa20, ChaCha20, Blowfish, CAST5, Kuznyechik, RC4, DES , 3DES, Skipjack, Safer, and Concept, Twofish, Serpent, AES (Rijndael), are three of the most common symmetric-key algorithms.

Public –Key encryption

Algorithms are the most commonly used public-key encryption implementations that seem to be owned by RSA Data Security. Therefore, the RSA approach to public-key encryption is quoted as follows. Public-key encryption (also known as asymmetric encryption) contains a pair of individual-related keys that can be encoded electronically Authenticate its identity-a public key and a private key-or sign or encrypt data. Each public key is printed and the corresponding private key is kept secret data encrypted with your public key can be decrypted only with your private key. A simplified view is shown in the way public-key encryption works is shown in Figure 2.

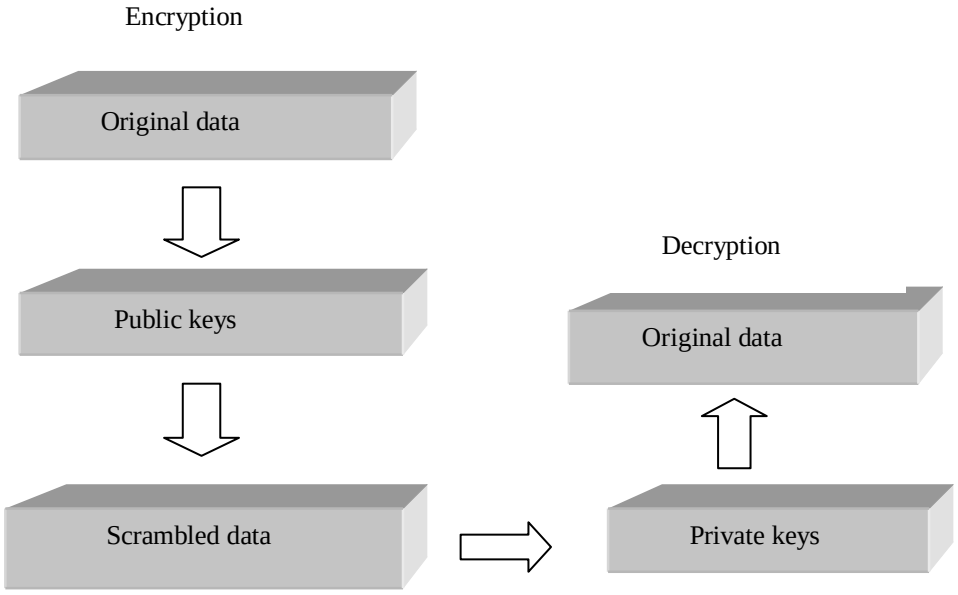

Figure 2. Block diagram of public-key encryption

The scheme shown in Figure 2 makes it possible to general contract a public key and only you can use this key to read the encrypted data. You encrypt the data with the public key of that person to send encrypted data then onto, and the patient received It decrypts the encrypted data with the corresponding private key. More computation is available for public-key encryption compared to symmetric-key encryption For large quantities of data and is therefore not always useful. Nonetheless, to send a symmetric key, it is possible to use public-key encryption, that can then be used for the encryption of useful information. This is the framework used by the SSL protocol. As it happens, the exact reverse of the scheme shown in Figure 2 also works: data can only be encrypted with your public key with your private key be decrypted.

However, This would not be an ethical way to encrypt personal data, because the data might well be decrypted by someone with the public key, which is made public by definition. Encryption by private-key is beneficial, however, since it ensures that You can sign your digital signature data using your private key, a significant requirement for electronic commerce and other commercial cryptography applications. Your public key should now be used from proxy servers like Firefox to evaluate That your private key was signed with the message and that it has not been tampered with since it was signed. "Digital Signatures" helps clarify how this confirmation technique performs.

Public-key cryptography, or asymmetric cryptography, is an encryption procedure that provides two keys-a a public key and a private button-that are mathematically compatible but not identical. Each key performs an essential purpose, unlike symmetric key algorithms that rely on one key to both encrypt and decrypt. To encrypt, the public key is used, and to decrypt, the private key is used. The virtualization of the private key based on the public key is computationally infeasible. Because of this, public keys can be freely exchanged, give customers a cheap way to encrypt content, and prove digital signatures, and private keys can be kept secret, maintaining that content can be intercepted and digital signatures can only be established by the owners of the private keys.

They are stored for messaging function and exchanging on digital certificates, as public keys need to be communicated, but are too heavy to be easily remembered. They are processed simply in the computer or operating system you have are now using or on hardware (e.g. USB token, hardware support module) containing drivers that allow the software or operating system to be used, since private keys are not circulated.

Business Applications

For public-key cryptography, the biggest consumer applications are:

- **Digital signatures:** The stuff is digitally signed with the private key of an individual and is validated by the public key of that same individual.

- **Encryption:** It is encrypted using the public key of an object and can only be decrypted with the private key of its individual.

Key length and encryption strength

Ultimately, cracking an encryption algorithm exposes the key in plain text for accessing the encrypted data. Breaking the algorithm appears to mean that the key used to encrypt the text for symmetrical algorithms is currently being established. Breaking around the algorithm pretty much means receiving the corresponding secret data between the two recipients for a public key algorithm. One strategy to smash A symmetric algorithm is simply to try each key until the correct key is found or the general algorithm is inside. As half of the key pair is available online, it is possible to derive the other half (private key) using printed, however complex, mathematical calculations for public-key algorithms. A brute force attack is called a manual determination of the key to crack an algorithm.

By breaking an algorithm, the risk of intercepting, or even impersonating and fraudulently investigating, private information is introduced. Looking at the fastest way to crack and link the algorithm with a brute force attack, the main strength of an algorithm is determined. Encryption strength is also defined for symmetric Keys typically provide better encryption in terms of the size or length of keys used to perform the encryption: longer keys. The key's length is measured in bits. For example, 128-bit keys to use with the Filezilla-supported for use with the same crypto, the RC4 symmetric-key protocol offers markedly better encryption algorithms than 40-bit keys. 128-bit RC4 encryption is an action line of 3 x 1026 rather than 40-bit RC4 encryption, roughly. (See "Introduction to SSL" for more info on RC4 and other cyphers used with SSL.) If the key is no further to the

best-known attack to break the key than a brute force effort to test any price of an asset, an encryption key is called full power. To achieve the same degree of encryption power, different cyphers can require different key lengths. For instance, the RSA cypher used for public-key encryption, due to the nature of the mathematical problem on which it is based, can use only a subset of all possible values for a key of a given length. In other cryptosystems, All possible values, rather than a subset of those values, can be used for a key of a given length, such as those used for symmetric key encryption. And stealing an RSA key is relatively trivial, to be considered cryptographically safe, A very long key, at least 1024 bits, must have an RSA public-key encryption code. With an 80-bit key for most algorithms, on the other hand, symmetric-key block cipher can achieve approximately the same level of discretion.

Artificial Intelligience

Artificial Intelligence, this includes the different neural network architectures and laws of Schooling. Biological neural networks influenced machine intelligence, (the central nervous system, the brain in particular) and may be ready to implement in various complicated control design methods Issues like comprehension of function approximation variations, Data mining, machine learning, prediction, and so on. In many aspects, the application of artificial intelligence in computer network security is manifested, one of which is the adoption of artificial intelligence in the management of computer network security. At both, the moment, a very important computer technology Firewall technology and the fundamental technology of firewall technology are network security management technology towards proposed detection.

When another network including n hosts exists, the network is considered as a framework as a whole. A package like that That is, A = {a1, a2, ... ,an} can be obtained. Then, every host move can be tracked in this system, as a unit for execution, i. e. V. When the host is in the vicinity of the system connects outside the system with the host, the unit of motion began to count towards. When the host or within the network is viewed by the external host, the value of V is V Increases by 1, and when handled by the internal host outside the framework, the host decreases the V value from 1T. The below figure 3. shows the chart of artificial intelligence.

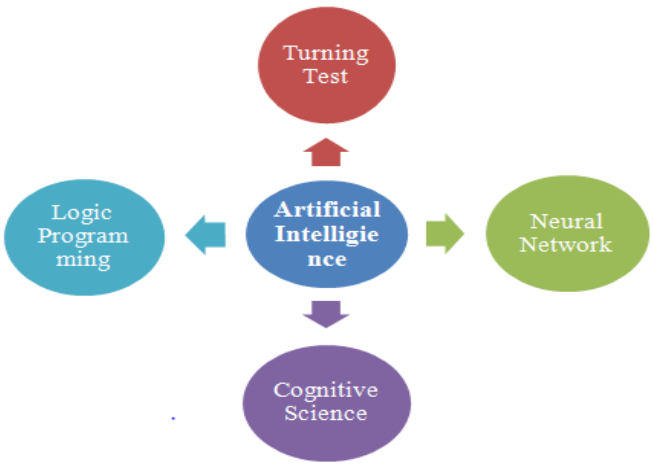

Figure 3. Artificial Intelligience

The interpretation of active entropy can be drawn from applying the entropy regards to the influence on the above probability. The flag-raising in this article needs to be rewritten. The size of the detection window, as increased, traffic to the network. It is not difficult to see a network that is traffic varies in different, but from a managerial point of view, long-term outlook and point of view, it is unnecessary to change any speed limits, the acceptance of a clear solution to diverse traffic. To give maximal play to the effects of physical activity, entropy in the air traffic of network incidents, it is good to construct concurrent conclusions based on will choose the detection window size. If there is n if there is n, Quasi-repeat elements with {a1, a2, an} in the category of Length T, the set of times of occurrence for each of the relevant The value is {d1,

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 6 Issue: 1 September 2020

d2,.. {d1, d2, Dn}. At this phase, the formula for the entropy margin as shown in equations 1 and 2.

$$HA = \sum_{k=1}^{i} (gi)\log(gi) \quad (1)$$

$$G(x) = \sum_{n=1}^{k} \left(\frac{ai}{t}\right) \log(ai/t) \quad (2)$$

The operation of modular exponentiation is simply an operation of exponentiation where modular multiplication is tried to carry out intensively. The 512-bit and we incorporated the 512-bit Modular exponentiation components of 1024-bit using the LRR Binary method, where the left-to-right stands for LR. The Exponent's scanning orientation. The pseudo-code of the binary LR I algorithm as shown below

Output= B = G^k mod m
Input = a, b, k
G < =1;
  For I =k – 1 to ∞
If b_i =1
  G< =B*a mod m ,
End if
  If I ≠ 0
  G >= b*b mod n,
  End for
End if
  Return B

The algorithm in our research work was implemented using C language Using Turbo C+++, codes were compiled and managed. Compiler including IDE.

IV. EXPERIMENTAL RESULTS

The ultimate aim of this study was to encrypt and decrypt the data that is encoded using artificial intelligence. In 500 (five hundred) datasets of this research paper, documented from diverse transmitters and saved as a file format for .wav. From the order to encrypt similar data, We first extracted the integer information from the original .wav file. And saved as a .txt format into another file. Encryption the txt file is taken as input by the software and performed the process of encryption on the file to generate an unreadable file message encrypted and another txt file saved. The decryption code, on the other hand, took over the message file encrypted as input and rolled out the function of decryption on the file to recover the original file including text. The below graph 4.decribes the encoding and encryption data.

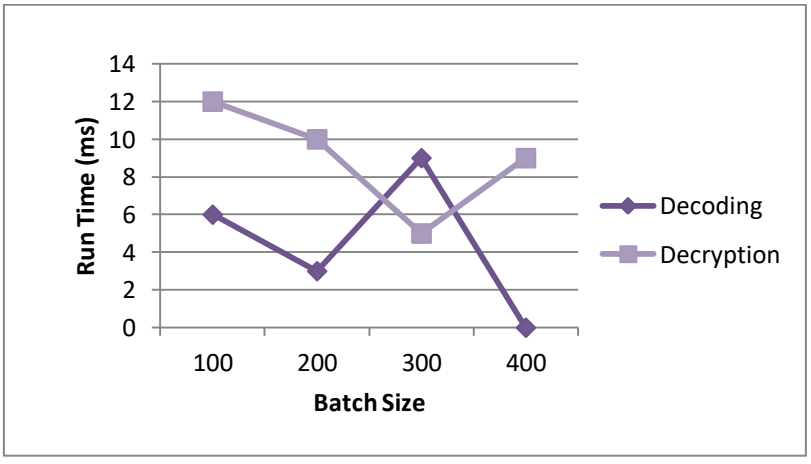

Figure 4. Graphical representation of encoding and encryption data

Different values for p to produce the main pair Q and q have indeed been examined. P = 13 and q = 29 were in this work used to evaluate the keys for encryption and decryption, and some rather virtues have yielded improved outcomes for encryption. We Marked 5 as the encryption key value B. Accordingly, the {5, 377}, and {269, 377} were the public and private keys, respectively. In this dissertation, the positive production of messages is used to Encrypt the original data and decrypt it. That's really ought to be It was remembered that the integer representation. In the set, the message to be encrypted should lie described by the modulus. (i.e., M would be within the [0, n1] range), which denotes a cap on the maximum amount of units. Characters can also be encrypted in a single instant. The below graph 5. describes the decoding and decryption data.

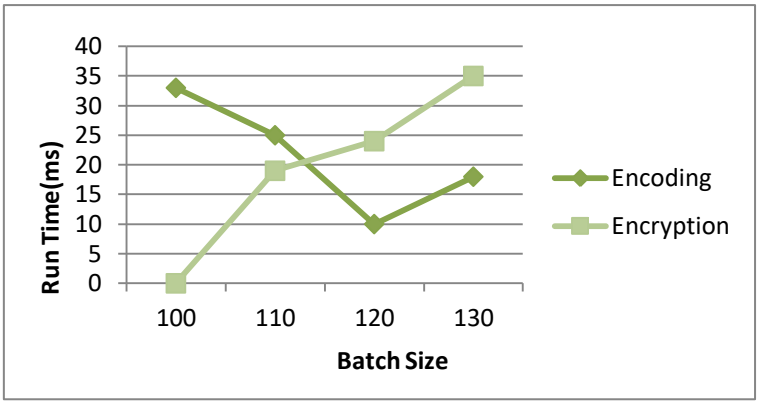

Figure 5. Graphical representation of decoding and decryption data

V. CONCLUSION

Practical cryptography insists on the delivery of established survey information tests aimed at ensuring a pseudo-random property pseudo-random sequences are taken from even a generator to be most cryptographic sequences, used instead of purely random sequences, applications. This paper presents a framework for designing pseudo-random (chaotic) new look algorithms to grow an integer that is taken to use purely random strings. These sequences must have been an approximation. This methodology doesn't always budget for any attention to the iterator's algorithmic ambiguity, which is one of the biggest hurdles of implementing complexity to chaos regarding cryptography. Neither does it reflect the structural stability of the iterator or its complexity related to the topic. Additionally, it does provide a logical approach to things of producing a Massive PRNG database for the application of segmentation Strictly 'one-to-one' communications encryption algorithms data storage, or 'one-to-Cloud' (encrypted). By using Evolutionary systems of technology such as Eureqa were seeded with Noise, a nonlinear function can be provided with necessary standards for operation. Consequently, the one-step Unpredictability does not ensure that the sequence of operation is when an attacker has access to a target, it will be unpredictable.

REFERENCES

[1] Kovalchuk, A., & Lotoshynska, N. (2018, August). Elements of RSA algorithm and extra noising in binary linear-quadratic transformations during encryption and decryption of images. In 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP) (pp. 542-544). IEEE.

[2] Zhang, L., & Chen, J. (2018). U.S. Patent No. 9,992,669. Washington, DC: U.S. Patent and Trademark Office.

[3] Xu, S., Yang, G., & Mu, Y. (2019). Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. Information Sciences, 479, 116-134.

[4] Zhang, Y., & Tang, Y. (2018). A plaintext-related image encryption algorithm based on chaos. Multimedia Tools and Applications, 77(6), 6647-6669.

[5] Sun, C., Su, S., Gao, Z., Liu, H., Wu, H., Shen, X., & Bi, W. (2019). Stimuli-responsive inks based on perovskite quantum dots for advanced full-color information encryption and decryption. ACS applied materials & interfaces, 11(8), 8210-8216.

[6] Irviani, R., & Muslihudin, M. (2018). Nur algorithm on data encryption and decryption. International Journal of Engineering & Technology, 7(2.26), 109-118.

[7] Mishra, S., & Dastidar, A. (2018, March). Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High-Security Applications. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) (pp. 1-5). IEEE.

[8] Allam, Z., & Dhunny, Z. A. (2019). On big data, artificial intelligence, and smart cities. Cities, 89, 80-91.

[9] Raman, B., & Ramanathan, A. Artificial Intelligence Based Authentication Scheme for Mobile Adhoc Networks.

