Cyber Security using Cryptographic Algorithms

Article *in* International Journal of Computer Trends and Technology · January 2024

DOI: 10.14445/22312803/IJCTT-V72I1P110

2 authors:

Shiva Kumar Sriramulugari
Verizon Communications
9 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Ashok Gorantla
Georgia Institute of Technology
11 PUBLICATIONS **76** CITATIONS
SEE PROFILE

International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I1P110

Volume 72 Issue 1, 60-67, January 2024

Original Article

Cyber Security using Cryptographic Algorithms

Shiva Kumar Sriramulugari[1], Venkata Ashok K Gorantla[2]

[1,2]*Solution Architect, Texas, USA.*

[1]*Corresponding Author : shivakumar.sriramulugari@gmail.com*

Received: 22 November 2023 Revised: 03 January 2024 Accepted: 20 January 2024 Published: 31 January 2024

Abstract *- Nowadays, individuals can connect with each other and do business anywhere in the globe, which saves time, effort, and money. This is made possible by the fast rise of Internet applications. Nevertheless, the efficacy of these apps relies on safeguarding the data from unauthorized access by malicious individuals. The protection of sensitive data from unauthorized access during transmission over the global network is widely recognized as a significant concern. A variety of strategies are used for the purpose of data security. Certain strategies include the transformation of a legible text into an illegible form using mathematical processes. At the same time, other ways involve the conversion of a legible text into either a picture or musical notes, facilitated by an encryption key. It is essential that the encryption key has a high level of security and is not transmitted through the Internet. This study presents a novel approach called the Multiplicative Cypher Homomorphic Adleman Algorithm (MCHAA), which introduces an additional layer of security to the cyber network. The research also illustrates the process of exchanging the encryption key generated by the proposed method with a second party using the MCHAA. In this scenario, when the data owner initiates a request for the file, the server will produce an authentication key and verify it with the user afterward. Upon receiving the designated key, the encrypted file undergoes decryption, hence enabling the user to get access to the decrypted file via the use of the MCHAA protocol. Ultimately, the performance analysis is conducted to evaluate the efficiency of the proposed method by comparing it with current procedures.***

Keywords *- Cyber security, Multiplicative Cipher, Homomorphic Adleman Algorithm, Cryptography.*

1. Introduction

A major challenge in the field of information and communication technology has recently been faced by the international community. Many parts of our lives have changed drastically as a result of the expansion of computer networks and Internet services. One notable aspect of the Internet is its role in the growth of several applications that need a safe environment. These include online banking, e-government efforts, bill payment systems, and e-commerce. In order to avoid breaches and illegal access, it is crucial to manage and secure applications and transactions that take place over public wired or wireless networks. Hence, these apps and transactions must have thorough and secure communication protocols. Data authenticity, integrity, privacy, and confidentiality are all guaranteed by this secured network monitoring and management method.

Cloud computing refers to the growing need for a variety of resources that may be accessible over the Internet. Computer gear, databases, applications, networks, and data collection techniques and programmes are all part of the service spectrum. Assuming the data network has an active internet connection, the programme will connect and do its operations. Protected data stored on-premises is vulnerable to many types of threats. It is possible that all data storage devices might be compromised by social engineering and rescue operations. Data kept by persons or organizations in physical locations may be more resilient, nevertheless, since security breaches are less common for those keeping such data. Abuse of personal information, lack of understanding, account hijacking, shaky server traffic, insecure APIs, inadequate cloud storage resources, and weak mutual cloud encryption methods are all factors that can compromise a network's security. Cloud computing's built-in security features might compromise the safety of cloud systems as a whole. Data stored in the cloud must be protected in more ways than just the server itself. Cloud users should emphasize the security of their cloud access by using secure mobile device storage or login credentials. Without due diligence, cloud access may be readily accessible. Ensuring the secrecy of data kept on a cloud server in a different geographic area, which is subject to various legal frameworks and privacy legislation, is another hurdle in cloud security. Data loss, spoofing, service interruption (DoS/DDoS), high energy consumption, and unidentified gateways are just a few of the numerous assaults that may exploit their lack of specialized anomaly detection systems and inadequate preventive measures. Dangerous impacts on hardware, disruptions in system access, system breakdowns, and even physical injury to persons are among the serious outcomes that might arise from the aforementioned behaviors. Therefore, there is a great deal of variance in the degree to which attacks on cloud networks impact their targets.

There are authorized personnel in every company whose job it is to keep an eye on data stored in the cloud. Through the use of strong security measures and careful attention to privacy issues, the network systems are designed to guarantee the supply of several interconnected aspects, such as the protection of data in terms of trust, integrity, control, audit, and accessibility. Using a decentralized key distribution technique, the data saved is encrypted by the decentralized access control system, which ensures that only authorized users may decode it. Files and documents stored on the server adhere to the access strategy that is known inside the domain. Improving productivity is the driving force behind turning the local servers into a private data infrastructure. Important technical solutions may be more easily provided if efforts are made to reduce costs and maximize the use of available resources. Before safely storing application data in a way that does not reveal the user's identity, the cloud platform uses an authentication method to confirm the user's authenticity. Those with the proper credentials may crack encrypted files and, with enough effort, alter, create, and understand them in the legal system. In cloud storage environments, Attribute-Based Encryption (ABE) and proxy recycling are the main tools used to guarantee data security and access control compliance. To protect against collision attacks, data files are separated into a header and a body. In the case of cloud computing, data duplication tactics may be used to improve data protection in cases when standard security measures are insufficient. The tree's static and dynamic architecture makes data security easier to provide. Intricate tree structures are input by the user into the arbitrary segments. The encrypted hidden data exchange would be dispersed over several cloud platforms in order to accomplish data access utilizing attribute-based encryption. Unauthorized access, whether from within or outside the organization, is a concern when data security is inaccessible. As a result, users are authorized to employ critical technical resources for encrypting data. For the purpose of authenticating digital communications in connection with Cloud data, the Rivest-Shamir-Adleman (RSA) digital signature technique has been thoroughly researched and used to improve security measures. Using the Attribute-Based Signature (ABS) method in conjunction with a hybrid community signature scheme is the recommended strategy. By using a secret key, this hybrid technique guarantees that the receiver's anonymity is preserved. A secret private key is in the possession of the buyer. To properly address the problem without sacrificing data integrity, the encrypted code has been enhanced with several keywords, and the trapdoor generation technique is used. The owner of the device may encrypt data using the Fine Grain Access Control technique, and then the server can decrypt it. Conspiracies involving the illegal acquisition of personally identifiable information from users force the suspension of the SDS system. Collaboration and common understanding are the means by which knowledge is gained. In addition to indicating the existence of the similarity index, the M-index is used to strengthen neighbor queries' ability to protect data from vulnerabilities. A private key signature in the system that relies on policy attributes requires two parts. The ability to generate the signature is not present in the other applications. In this proposal, the author lays out the steps necessary to launch a cloud-based improved data security cryptography system called MCHAA. Customers might own property management systems from multiple institutions; therefore, a more robust attribute encryption solution is better for cloud storage control systems. Because of this, they may get access to policy key holders and use assets that are designated for certain institutions. The management of dense stainless-steel characteristics using standard techniques of common authority has been shown to improve device efficiency. In addition, a trustworthy and approved organization must provide a thorough solution to handle the intricate data security needs. The article presents a single significant contribution, which may be summarized as follows:

- To offer a new secure system for cloud network computing secure read and write operations, enabling symmetrical encryption algorithms in order to reduce overhead computation for effective key management.
- To have an outsourced encryption and decryption verification method. The user can access the information via any device, wherever, at any time.
- The expense of processing is small.

The remainder of the paper is organized as follows: The relevant work's outline is presented in section II, while the material and methods are presented in section III. In Section IV, experimental analysis is presented. Section V serves as the paper's conclusion.

2. Related Works

Data transmissions are being encrypted using cryptographic methods. Both the sender and the receiver may benefit from these algorithms for a variety of operations that are carried out across any network. Cryptographic algorithms provide the necessary tasks—encryption, decryption, authentication, and digital identity—to protect data and communications from prying eyes. Below are some instances of recent contributions in the examples provided below. The capabilities of smartphone apps are mostly limited by the portable devices and smartphones used for communication and the exchange of data, including audio and video. The data is stored inside the cloud infrastructure; however, it should be noted that the programme in question lacks optimization in terms of meeting the specific needs and preferences of the client. When the mobile access power is off, the preservation of traditional knowledge about users and the cloud remains intact. The technique of watermarking was devised by Wang et al. (2014) as a means of ensuring the security of data transmission between cloud service providers and clients via the implementation of authentication measures. The use of Reed-Solomon coding in conjunction with watermarking techniques has the potential to reduce transmission mistakes

effectively. The check capabilities played a crucial role in cryptographic systems, and the suggested attribute-based encryption (ABE) method by Kumar et al. (2016) effectively enhanced the flexibility of access control. Quantifying the ABE approach posed significant hurdles due to its substantial expenditures, formidable obstacles, and intricate decryption process. Consumers and authorities had consistent success. The computational aspect was required to effectively provide the third party with a concise and verified answer to their findings. Essential technologies, such as authentication and access control, are required for the implementation and administration of cloud services. The functional efficacy of customer-based hierarchical access control (RBAC) and contexts-conscious RBACs was not taken into account. Choi et al. (2014) used the Onto-ACM approach to address nascent vulnerabilities in cloud computing. The computing paradigm is ensured by the service quality via several processes, such as resource virtualization, global replication, and migration. The data pertaining to cloud storage exhibited a sense of optimism among clients using cloud services, while the availability of consistent results was lacking. The authors Wei et al. (2014) proposed a reliable computer audit procedure. They conducted batch verification to ensure secure storage, optimized the sampling approach, and lowered expenses by using designer-verified signatures. The trial results unequivocally showed effectiveness and proficiency. The study conducted by Belguith et al. (2018) introduces a novel paradigm aimed at enhancing patient-centered care via the management and accessibility of online information. The approach used in this study yielded outcomes that were both transparent and adaptable. However, it is important to note that the transfer of sensitive data using attribute-based encryption methods differs from that of secure databases. In certain security jurisdictions, the complexity of key management has been reduced due to the challenges encountered in managing Personal Health Record (PHR) layouts in scenarios involving various data sources. The assurance of protection, scalability, and productivity in relation to glass and access controls has been provided. In the study conducted by Hepsiba and Sathiaseelan (2016), an extensive analysis of security concerns in cloud computing models was undertaken.

The researchers examined several solutions proposed to mitigate these difficulties, thoroughly exploring their respective advantages and disadvantages. In a study conducted by Al-Shaikhly et al. (2018), the authors used a combination of genetic and Markov algorithms to address cloud security concerns. According to Gupta et al. (2020), in this study, we provide a novel hierarchical distribution multican attribute-based encryption system (HD-MAABE). The suggested system involves the issuance of attributes by both organizations and standard attribute bodies. The study conducted by Sammy and Vigila (2020) primarily examines several techniques for multiauthority attribute-based encryption (MAABE), with a specific emphasis on the compression of attributes with the least value. According to Rasori et al. (2020), The urban sensing encryption system, known as Current ABE Cities, addresses the aforementioned issues by using Attribute-based Encryption (ABE) to maintain stringent access control over data. According to the study conducted by Deepa and Pandiaraja (2020). This paper presents a proposal for an effective file recovery method using cloud-based attribute file encryption (ERFC). According to the study conducted by Lei et al. (2020), The Late Dirichlet Assignment (LDA) methodology is used to conduct an analysis of the service description and investigate the potential correlation between the content and locational information. The optimal integration of LDA and word2vec models in this specific situation achieves a harmonious equilibrium between accuracy and speed, hence enhancing the effectiveness of service recommendations. According to Ferrag et al. (2020), this report presents an overview of the sample, data sets used, and a comparative review of deep research methodologies pertaining to intrusion detection for information security. Specifically, the authors conduct a comprehensive evaluation of intrusion detection systems that use deep learning techniques. According to the study conducted by Devi et al. (2020), The Modified Adaptive Neuro Fuzzy Inference System (MANFIS) is an advanced mechanism for achieving load balancing in a heterogeneous computing environment. The implementation of Firefly Algorithms achieves the configuration of MANFIS parameters. Enhanced Elliptical Curve Cryptography (ECC) provides a means of ensuring security in the process of user authentication. The solution used is a password-less approach to ensure the security of the device. The suggested study demonstrates good outcomes by effectively using available resources. In their study, Ghosh et al. (2020) introduced a model that uses mutual information gain as a criterion for selecting characteristics that are associated. In order to accomplish this objective, the correlativity characteristics are first grouped. Subsequently, each party proceeds to choose the qualities within their respective categories that possess the greatest level of shared knowledge value. As a consequence, there was a diminished set of characteristics that facilitated rapid acquisition of knowledge, so yielding an enhanced Intrusion Detection System (IDS) for safeguarding cloud-based data.

3. Proposed Work

The framework in which the data securing mechanism and the overall implementation mechanism are stated, and the proposed architecture and the MCHAA network data security mechanism are described in Figure 1.

3.1. Data Source

"The UNSW-NB 15 dataset's raw network packets were generated using the IXIA Perfect Storm programme inside the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS). This technology was used to produce a combination of genuine, up-to-date normal activities and artificially generated current attack behaviours.

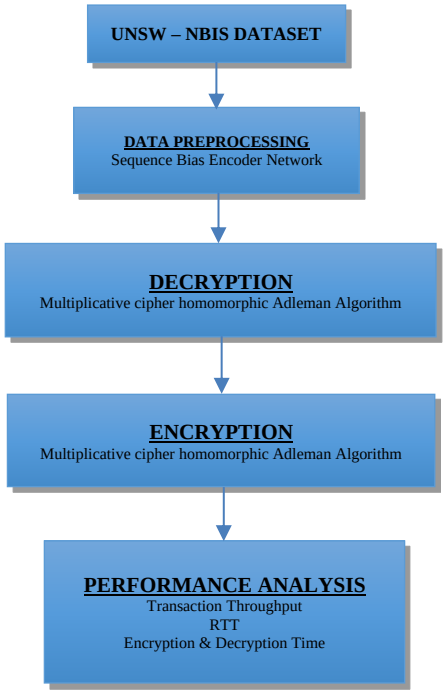

Fig. 1 Schematic representation of the suggested methodology

The Tcpdump utility is used for the purpose of capturing a total of 100 gigabytes of unprocessed network data, namely in the form of Pcap files. The dataset comprises nine distinct categories of attacks, including Fuzzers, Analysis, Backdoors, Denial of Service (DoS), Exploits, Generic, Reconnaissance, Shellcode, and Worms. The Argus and Bro-IDS tools are used in conjunction with the development of twelve algorithms to yield a total of 49 characteristics, including the class label.

The aforementioned characteristics are delineated inside the UNSW-NB15_features.csv file.

The dataset consists of a total of 2,540,044 records, which are distributed among four CSV files: UNSW-NB15_1.csv, UNSW-NB15_2.csv, UNSW-NB15_3.csv, and UNSW-NB15_4.csv.

The table containing the accurate and reliable data is referred to as UNSW-NB15_GT.csv, whereas the file containing the list of events is denoted as UNSW-NB15_LIST_EVENTS.csv.

The dataset is divided into two partitions, namely, UNSW_NB15_training-set.csv and UNSW_NB15_testing-set.csv, which are specified as the training set and testing set, respectively.

The training set consists of 175,341 records, whereas the testing set has 82,332 records. These records are categorized into two types: attack and normal.

3.2. Preprocessing

The practice of normalizing numbers that have been measured on multiple scales is essential in data processing, particularly prior to averaging. Certain forms of standardization just include a process of rescaling in order to align the values with those of another variable. If the population parameters are known, it is necessary to make simple changes in order to alter errors. In this study, the sequence bias encoder network is used for the purpose of data preparation.

The proposed network consists of input (jd) and forget (Fd) gates, as well as an output (ud) gate. The following action of a particular cell is controlled by the summation of the contents of its input gate and its forget gate. The error values are sent based on the present state of the cell via the output gate of the cell.

$$F_d = \partial(O_F p_d + f_F H_{d-1} + B_W \quad (1)$$

$$j_d = \partial(O_j p_d + f_j H_{d-1} + B_j \quad (2)$$

$$u_d = \partial(O_u p_d + f_u H_{d-1} + B_u \quad (3)$$

$$R_d = F_d R_{d-1} + j_d \approx dANH(O_R H_{d-1} + f_R p_d + B_R) \quad (4)$$

$$H_d = u_d \approx dANH(R_d) \quad (5)$$

"R_d is a hidden state in the internal memory cell Hd. The parameters to be learned are O_W, O_j, O_u, $O_R \exists s^{M\times M}$, f_W, f_j, f_u, $f_R \exists s^{M\times N}$ denotes element-wise multiplication, "dANH" stands for hyperbolic activation function, and "LSF" stands for logistic sigmoid function.

The proposed network unit is used for the purpose of encoding time series data. The intended output sequence $q_1, q_2, \ldots, q_I$ may be derived from the input sequence $P = (p_1, p_2, \ldots, p_I)$ where p_d sn. The sequence P is defined as the product of the sensor data features N and the previous value of the hidden state, denoted as d, for each given set of sensor data features.

$$q_d = F_A(H_{d-1}, q_d) \quad (6)$$

Where $H_d \exists s^M$, H_d The amount of the encoder's secret state at time d is denoted as S_d, and M represents the encoding technique that varies with time. The trajectory is not linear. The value of attention may be determined by the following calculation.

$$E_d^j = U_E dAnH(f_E[H_{d-1}; K_{d-1}]) \quad (7)$$

$$\beta_d^j = \frac{\exp(E_d^j)}{\sum_{i=1}^{I} \exp(E_d^i)} \quad (8)$$

"Two examples of learnable parameters in this context are the hidden state of the encoder (H_(d-1) sM) and the hidden state of the decoder$H_{d-1}\exists\ s^{M}$, where M represents the size of the hidden state.

The attention weight U_E, denoted as ∃ s^M, represents the significance of directing attention towards the hidden state of the encoder at time d.

The context vector Cd may be derived using weighted summation, 64tilizing the attention weight R_{d-1} ∃ s^{M} and the encoder's hidden state$\{H_1, H_2, \ldots, H_I\}$, as shown in the following calculation.

$$C_d = \sum_{j=1}^{I} \beta_d^j H_j \quad (9)$$

"Subsequently, the concealed state of the decoder may be ascertained by using the context vector in conjunction with the present time, denoted as d. One prediction of the coefficient of drag (C_d) at time d and the difference in the previously hidden state (q d+1-1) is sought. ".

$$R_d = W_A([\overline{q}I + d - 1; C_d], R_{t-1}$$

"The suggested model employs an error binning technique to update the hidden state Rd of the decoder. This approach is advantageous as it addresses the requirements of both Rd and $C_{d,\ which}$ are nonlinear functions: $[\overline{q}I + d - 1;\ C_d]$ $\exists s^{M+1}, R_{d-1}\ \exists\ s^{M}, W_A$.

The ultimate projected value is derived by re-establishing the link between the context vector Cd and the present hidden state Rd of the decoder via the use of two fully connected matrices, similar to the previous computation.".

$$\overline{q}I + d = W_q O_q([\overline{q}I + d - 1; C_d; R_d]) \quad (10)$$

"Where $O_q\exists\ s^{(2M+1)\times M}$and $f_q\ \exists s^{M}$ the criteria that need acquisition via learning.

The detection of data anomalies may be achieved by initiating the analysis of anomalous motion.

Subsequently, the feature scaling procedure may be used to normalize all values within the range of 0 to 1. The technique is often referred to as unity-based normalization.

$$Z' = \frac{(Z - Z_{min})}{(Z_{max} - Z_{min})} \quad (11)$$

3.3. Data Security

Here, for improving data security, the MCHAA algorithm was used.

Step 1: Examine the unadorned textual content P with dimensions M×N.

Step 2: The process involves the random selection of two big prime integers, p and q. Subsequently, the private key, denoted as d, is calculated using the public key, e, and the MCHAA algorithm.

Step 3: The information entropy (s) and pixel sum (sumpx) are extracted from the picture P. Additionally, two random integers (w and r) are generated. In order to increase the sensitivity of the plaintext, a matrix is created to derive three plain messages, denoted as α, β, and γ, as seen in the following equation:

$$\begin{cases} \alpha = \mathrm{mod}(\lceil (t + r) \times e^{s} \rceil, n) \\ \beta = \mathrm{mod}(\mathrm{sumpx}, n) \\ \gamma = \mathrm{mod}(w, n) \end{cases}, \quad (12)$$

Step 4: Perform the encryption process on the aforementioned plaintext messages using the RSA encryption algorithm, resulting in the matching cipher text messagesα', β', and γ'.

Step 5: A novel nonlinear function is formulated to include both plain messages and cypher messages. Additionally, three starting values, denoted as x_0, y_0, and z_0, are generated for the chaotic system, as seen in the subsequent equation:

$$u = \sin\left(\mathrm{mod}\left(2\pi v + \tan(v'), \frac{\pi}{2}\right)\right), \quad (13)$$

Step 6: To get three chaotic sequences, denoted as x, y, and z, to solve the 3D chaotic system using the Rouge-Kutta technique. The length of each sequence is determined by the formula m×n/3+t+2max (m,n), where m and n are variables, and t is a constant. The function max (p, q) is used to determine the largest value between p and q.

In order to mitigate the influence of transitory effects inside chaotic systems, it is customary to exclude the first t values of the series. In this particular study, the value of t is established as 128.

Step 7: The sequences p^' and q^' are formed by removing the first 2×max (m, n) values from the sequences p and q, respectively. The concatenation of the sequences p, q, and r results in a new sequence denoted as r^'. Subsequently, Equation (14) is used to compute the values of p^', q^,' and r^,' resulting in the generation of three novel sequences x^", y^", and z^".

$$\begin{cases} p'' = \mathrm{mod}(\lfloor (x' - \lfloor x' \rfloor) \times 10^{15} \rfloor, 256) \\ q'' = \mathrm{mod}(\lfloor (y' - \lfloor y' \rfloor) \times 10^{15} \rfloor, 128), \\ r'' = \mathrm{mod}(\lfloor (z' - \lfloor z' \rfloor) \times 10^{15} \rfloor, 256) \end{cases} \quad (14)$$

Step 8: The first stage of perplexity over the cycle. The first M values in the odd positions of the sequence p^" are used to introduce confusion to the plain picture in the row direction.

Similarly, the first N values in the even positions of the sequence p^" are utilized to induce confusion in the column direction. Consequently, the resulting image Q is created.

Step 9: After doing an additional operation on the data Q, four coefficient matrices of dimensions (M/2) × (N/2) are derived. These matrices are referred to as the approximation matrix CA, as well as the three detail matrices CH, CV, and CD.

Step 10: The phenomenon of cycle misunderstanding at the second layer. The first M/2 values in odd positions of the sequence y^" are used to introduce complexity into the approximation matrix CA. Similarly, the first N/2 values in even positions of the sequence y^" are utilized to complicate the matrix in the column direction further. As a result of these operations, the resulting picture G is created.

Step 11: The matrix G is joined with the three detail matrices CH, CV, and CD and then subjected to the inverse operation to get the resulting data R.

Step 12: The topic of discussion is diffusion encryption. Initially, the variable R is transformed into a unidimensional sequence denoted as A. Subsequently, the sequences z^" and A are used to execute the diffusion operation using Equation (15), resulting in the acquisition of the diffused sequence B. As a result, the sequence B is reorganized into an M×N matrix in order to generate a cypher data C.

$$\begin{cases} c(0) = 0 \\ c(1) = \mathrm{mod}(c(0) + z'(1) + A(1),256) \\ c(i) = \mathrm{mod}(c(i-1) + z'(i) + A(i),256) \end{cases} \quad (15)$$

$$i = 2,3,4,\dots,M \times N$$

The process of decryption is similar to the encryption steps but in an inverse order.

4. Performance Analysis

In this section, experiments are conducted to gauge performance. The suggested method is implemented inside the Python environment. The computation time for encryption and decryption is determined. In contrast to other methodologies, the suggested scheme demonstrates a significant improvement in performance while requiring a reduced burden.

Additionally, it has the advantage of being readily manageable for a wide range of consumers. The proposed approach incorporates data files of varying sizes (measured in kilobytes) that have been both validated and decoded. The proposed method is often used for primary generation. The method has been specifically built to provide reliability and minimize the running time required for encryption and decoding processes**.**

id	dur	sbytes	rate	sinpkt	smean
1	0.000011	496	90909.09	0.011	248
2	0.000008	1762	125000	0.008	881
3	0.000005	1068	200000	0.005	534
4	0.000006	900	166666.7	0.006	450
5	0.00001	2126	100000	0.01	1063
6	0.000003	784	333333.3	0.003	392
7	0.000006	1960	166666.7	0.006	980
8	0.000028	1384	35714.29	0.028	692

Fig. 2 Sample input

The sample dataset input is illustrated in Figure 2.

```
Data Shape: (82332, 41)

Sequence Bias Encoder Network

array([[117,   6, 111,  41,  77,  95,  32,  30,  44,  49, 106,   4,  13,
         23,  25,  76,  85, 127,  72,  19,  33,  83, 114, 115, 128,  64,
         65,  57,  88,  74,  67,  66,   0,  37,  20,  38, 113,  51,  96,
         52,  55,  39,  68,  34,  90,  70,  73,  99, 112,  53,   3,  54,
         12,  91,  50,  61,  92,  16, 126,  86,  10, 108, 125, 122, 116,
        120,  75,  22,  24, 110, 103,  63,  71,   7,  47,   2,  69,  26,
         82,  31,  40,  81,  87,  94,  11,   8,  42,   9, 109, 121,  46,
         15,  60, 124,  98,  97, 129,  43,  89, 118,  28,  59,  27,  79,
          5,   1,  45, 102,  14,  56,  78, 123,  62, 130,  21,  35, 107,
        105, 119, 100, 101,  58,  84,  29,  17,  18,  93,  48,  80, 104,
         36]])
```

Fig. 3 Processed output

The standardized output is illustrated in Figure 3

Encrypted.csv

"[1380063686, 1301357092]","[1301357092, 90018948, 2367795505]","[507212286, 2367795505, 854099662, 465895025, 854099662]","[441686144, 507212286, 1964619523, 465895025, 441686144]","[1301357092, 507212286, 1964619523, 465895025, 441686144]","[441686144, 395186802, 203927987, 465895025, 1561885035, 441686144]","[1301357092, 395186802, 203927987, 465895025, 1561885035, 441686144]","[2367795505, 2269163478, 465895025, 1561885035]","[441686144, 465895025, 465895025, 2447118238]","[1301357092, 465895025, 465895025, 2447118238]","[1301357092, 2447118238, 854099662, 2269163478, 1301357092]","[441686144, 2447118238, 854099662, 441686144, 441686144]","[1301357092, 2447118238, 854099662, 441686144, 441686144]","[441686144, 1380063686, 1697295611, 507212286, 1964619523, 465895025]","[1301357092, 1380063686, 1697295611, 507212286, 1964619523, 465895025]","[441686144, 1741030703, 1380063686, 465895025]","[1301357092, 1741030703, 1380063686, 465895025]","[441686144, 934138311, 1380063686, 1697295611]","[441686144, 465895025, 2297430423, 507212286, 395186802]","[1301357092, 465895025, 2297430423, 507212286, 395186802]","[1301357092, 934138311, 1380063686, 1697295611]","[465895025, 2297430423, 507212286, 2367795505, 465895025, 465895025]","[441686144, 203927987, 1697295611, 2269163478, 2297430423, 1964619523]","[2269163478, 2297430423, 1964619523, 1301357092, 2269163478, 465895025]","[441686144, 2258291537, 1561885035, 2269163478, 1697295611]","[1301357092, 2258291537, 1561885035, 2269163478, 1697295611]","[465895025, 2367795505, 2269163478, 1697295611, 441686144, 581268469, 1301357092, 1561885035, 507212286, 465895025, 840406024]","[2367795505, 1561885035, 441686144, 507212286, 854099662, 1697295611, 441686144, 1561885035, 581268469, 395186802, 854099662, 1301357092, 203927987, 581268469, 2447118238, 1561885035, 1697295611]","[2297430423, 465895025, 581268469, 441686144, 2367795505, 2103925505, 581268469, 441686144, 2367795505, 2297430423]","[2297430423, 465895025, 581268469, 441686144, 465895025, 2269163478, 465895025, 1561885035, 581268469, 465895025, 465895025, 2447118238]","[2297430423, 465895025, 581268469, 441686144, 1301357092, 441686144, 465895025, 581268469, 2447118238, 465895025, 2258291537]","[2297430423, 465895025, 581268469, 441686144, 2367795505, 2297430423, 581268469, 1301357092, 507212286, 854099662, 2367795505, 465895025, 581268469, 2447118238, 465895025, 2258291537]","[2297430423, 465895025, 581268469, 441686144, 2367795505, 2103925505, 581268469, 441686144, 2367795505, 2297430423, 581268469, 441686144, 465895025, 581268469, 2447118238, 465895025, 2258291537]","[2297430423, 465895025, 581268469, 441686144, 2367795505, 2297430423, 581268469, 2447118238, 465895025, 2258291537]","[1380063686, 441686144, 581268469, 1626966283, 465895025, 507212286, 581268469, 2447118238, 854099662, 1533727638, 1380063686, 1697295611]","[2297430423, 465895025, 581268469, 1626966283, 465895025, 507212286, 581268469, 2297430423, 2258291537, 1301357092]","[2297430423, 465895025, 581268469, 1626966283, 2447118238, 934138311, 581268469, 840406024, 465895025, 465895025, 507212286, 581268469, 2258291537, 465895025, 840406024, 1301357092]","[2297430423, 465895025, 581268469, 441686144, 2367795505, 2297430423, 581268469, 2447118238, 465895025, 2258291537]","[2297430423,

Encryption Time: 187.95484948158264 seconds

Decrypted.csv

ID,DUR,PROTO,SPKTS,DPKTS,SBYTES,DBYTES,RATE,STTL,DTTL,DLOAD,SLOSS,DLOSS,SINPKT,DINPKT,SJIT,DJIT,SWIN,STCPB,DTCPB,DWIN,TCPRTT,SYNACK,ACKDAT
,SMEAN,DMEAN,TRANS_DEPTH,RESPONSE_BODY_LEN,CT_SRV_SRC,CT_STATE_TTL,CT_DST_LTM,CT_SRC_DPORT_LTM,CT_DST_SPORT_LTM,CT_DST_SRC_LTM,IS_FTP_LOGI
N,CT_FTP_CMD,CT_FLW_HTTP_MTHD,CT_SRC_LTM,CT_SRV_DST,IS_SM_IPS_PORTS,LABEL
1,0.000011,UDP,2,0,496,0,90909.0902,254,0,0,0,0,0.011,0,0,0,0,0,0,0,0,0,0,248,0,0,0,2,2,1,1,1,2,0,0,0,1,2,0,0
2,0.000008,UDP,2,0,1762,0,125000.0003,254,0,0,0,0,0.008,0,0,0,0,0,0,0,0,0,0,881,0,0,0,2,2,1,1,1,2,0,0,0,1,2,0,0
3,0.000005,UDP,2,0,1068,0,200000.0051,254,0,0,0,0,0.005,0,0,0,0,0,0,0,0,0,0,534,0,0,0,3,2,1,1,1,3,0,0,0,1,3,0,0
4,0.000006,UDP,2,0,900,0,166666.6608,254,0,0,0,0,0.006,0,0,0,0,0,0,0,0,0,0,450,0,0,0,3,2,2,2,1,3,0,0,0,2,3,0,0
5,0.00001,UDP,2,0,2126,0,100000.0025,254,0,0,0,0,0.01,0,0,0,0,0,0,0,0,0,0,1063,0,0,0,3,2,2,2,1,3,0,0,0,2,3,0,0
6,0.000003,UDP,2,0,784,0,333333.3215,254,0,0,0,0,0.003,0,0,0,0,0,0,0,0,0,0,392,0,0,0,2,2,2,2,1,2,0,0,0,2,2,0,0
7,0.000006,UDP,2,0,1960,0,166666.6608,254,0,0,0,0,0.006,0,0,0,0,0,0,0,0,0,0,980,0,0,0,2,2,2,2,1,2,0,0,0,2,2,0,0
8,0.000028,UDP,2,0,1384,0,35714.28522,254,0,0,0,0,0.028,0,0,0,0,0,0,0,0,0,0,692,0,0,0,3,2,1,1,1,3,0,0,0,1,3,0,0
9,0,ARP,1,0,46,0,0,0,0,0,0,0,0,60000.688,0,0,0,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,0
10,0,ARP,1,0,46,0,0,0,0,0,0,0,0,60000.712,0,0,0,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,0
11,0,ARP,1,0,46,0,0,0,0,0,0,0,0,60000.688,0,0,0,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,0
12,0,ARP,1,0,46,0,0,0,0,0,0,0,0,60000.712,0,0,0,0,0,0,0,0,0,0,0,46,0,0,0,2,2,2,2,2,2,0,0,0,2,2,1,0
13,0.000004,UDP,2,0,1454,0,250000.0006,254,0,0,0,0,0.004,0,0,0,0,0,0,0,0,0,0,727,0,0,0,3,2,1,1,1,3,0,0,0,1,3,0,0
14,0.000007,UDP,2,0,2062,0,142857.1409,254,0,0,0,0,0.007,0,0,0,0,0,0,0,0,0,0,1031,0,0,0,3,2,1,1,1,3,0,0,0,1,3,0,0
15,0.000011,UDP,2,0,2040,0,90909.0902,254,0,0,0,0,0.011,0,0,0,0,0,0,0,0,0,0,1020,0,0,0,1,2,1,1,1,3,0,0,0,1,1,0,0

Decryption Time: 145.92648696899414 seconds

```
Total Transactions: 1000
Elapsed Time: 60.9690363407135 seconds
Transaction Throughput (TPS): 16.40176817
641821 transactions per second
Transaction Throughput (TPM): 984.1060905
850925 transactions per minute
```

Fig. 4 Simulated output

The overall simulated output is illustrated in Figure 4. Here, as shown in Figure 4, the suggested mechanism expresses satisfied performance by obtaining a high range of output.

To prove the efficiency of the suggested mechanism, it can be compared with the existing mechanisms.

Table 1. Comparative performance analysis

File size	Encryption time (s)				Decryption time (s)				Execution time (s)			
	MCHAA (Proposed)	DES [16]	RSA [17]	AES [18]	MCHAA (Proposed)	DES [16]	RSA [17]	AES [18]	MCHAA (Proposed)	DES [16]	RSA [17]	AES [18]
20	70.0	78.0	76.0	81.0	0.880	0.990	1.050	1.50	3.460	5.550	4.570	4.70
40	77.0	78.0	84.0	83.0	0.940	0.880	0.790	1.10	3.770	3.660	4.050	40
60	80.0	82.0	85.0	91.0	1.060	1.540	1.770	0.80	2.880	3.040	2.990	3.30
80	78.0	84.0	80.0	95.0	0.780	1.570	0.990	0.80	4.050	3.780	3.990	3.30

Table 1 presents a detailed temporal analysis and visual depiction of the encryption, decryption, and execution procedures across various file sizes measured in megabytes (Mb). The presented table provides information on the lengths of both the encryption and decryption procedures. The proposed approach has been subjected to rigorous testing, and its results have been compared to those obtained from known algorithms such as MCHAA, RSA, DES, and AES. The MCHAA technique, which is suggested, exhibits a reduction in the necessary duration for the processes of data encryption, decryption, and execution.

Table 2. Security analysis

Security level (%)				
File size (mb)	DES [16]	RSA [17]	AES [18]	Proposed
20	78.0	77.23	73.0	85.0
40	80.0	85.0	76.0	90.0
60	83.0	88.0	80.0	92.0
80	85.0	80.0	79.0	98.0
100	90.0	90.0	85.0	94.0

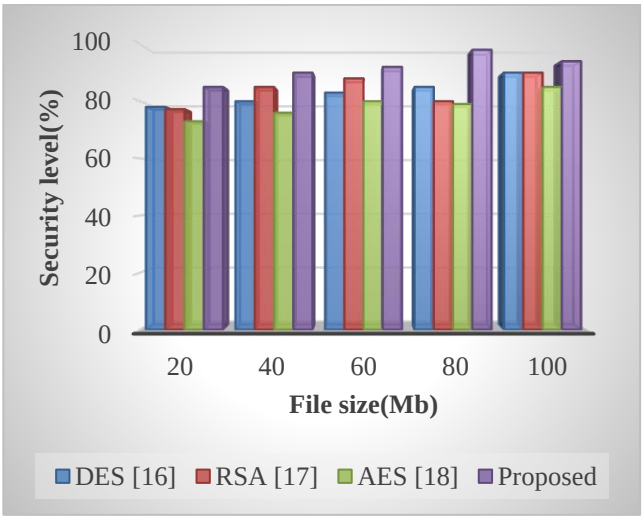

Fig. 5 Security rate analysis

Table 2 and Figure 5 give a thorough analysis and comparative evaluation of the safety levels offered by different encoding schemes. The encryption algorithms that provide the most robust security measures for a 20 MB file are DES, RSA, and AES, with success rates of 78%, 77.23%, and 73%, respectively. Additionally, a comprehensive examination is undertaken to assess the security protocols used for files within the range of 40 to 100 megabytes in size. The graph shown above illustrates that the suggested technique provides a superior degree of security when compared to the encryption methods that are already used.

Based on the obtained findings, it can be inferred that the suggested methodology exhibits good efficacy in safeguarding the integrity and confidentiality of the data.

5. Conclusion

The issues of user identification and data security pose significant challenges inside a network context. This study proposes a system for access management that is both effective

and scalable. In contrast, the MCHAA encryption method provides not just data security for a cloud service provider with limited trustworthiness but also a streamlined key management framework for large-scale applications, which is devised by central authorities. In this context, safe encryption and decryption techniques are used to ensure the secure transmission of data. When the authenticated user initiates a request to access the cloud, the cloud system will transmit the appropriate files in an encrypted format, which is determined based on the server's computational capacity. Subsequently, the data proprietor will decipher the data using the cryptographic key generated by the modified blowfish technique. The findings indicate that the adopted technique demonstrates efficiency in terms of protection, durability, and performance. The future magnitude of the planned research will be addressed by the use of re-encryption, quality-based coding, and secure information transmission".

References

[1] Mazin H.R. Al-Shaikhly, Hazem M. El-Bakry, and Ahmed A. Saleh, "Cloud Security Using Markov Chain and Genetic Algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 96-106, 2018. [Google Scholar]

[2] Sana Belguith et al., "PHOABE: Securely Outsourcing Multi-Authority Attribute Based Encryption with Policy Hidden for Cloud Assisted IoT," *Computer Networks*, vol. 133, pp. 141-156, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Chang Choi, Junho Choi, and Pankoo Kim, "Ontology-Based Access Control Model for Security Policy Reasoning in Cloud Computing," *The Journal of Supercomputing*, vol. 67, pp. 711-722, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[4] N. Deepa, and P. Pandiaraja, "Retracted Article: E Health Care Data Privacy Preserving Efficient File Retrieval from the Cloud Service Provider Using Attribute Based File Encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 4877-4887, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] T.J.B. Durga Devi, A. Subramani, and P. Anitha, "Retracted Article: Modified Adaptive Neuro Fuzzy Inference System Based Load Balancing for Virtual Machine with Security in Cloud Computing Environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 3869-3876, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mohamed Amine Ferrag et al., "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," *Journal of Information Security and Applications*, vol. 50, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Partha Ghosh et al., "An Improved Intrusion Detection System to Preserve Security in Cloud Environment," *International Journal of Information Security and Privacy*, vol. 14, no. 1, pp.1-14, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Reetu Gupta, Priyesh Kanungo, and Nirmal Dagdee, *HD-MAABE: Hierarchical Distributed Multi-Authority Attribute Based Encryption for Enabling Open Access*, International Conference on Intelligent Computing and Smart Communication, pp. 183-193, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] C. Linda Hepsiba, and J.G.R. Sathiaseelan, "Security Issues in Service Models of Cloud Computing," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 3, pp. 610-615, 2016. [Google Scholar] [Publisher Link]

[10] Kumar SS, Prasad S, Parimala M & Someswar GM 2016, 'Scalable and Secure Sharing of Personal Health records in Cloud Computing Using Attribute Based Encryption', COMPUSOFT: An International Journal of Advanced Computer Technology, vol. 5, no. 6

[11] Chao Lei et al., "A Service Recommendation Algorithm with the Transfer Learning Based Matrix Factorization to Improve Cloud Security," *Information Sciences*, vol. 513, pp. 98-111, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Marco Rasori, Pericle Perazzo, and Gianluca Dini, "A Lightweight and Scalable Attribute-Based Encryption System for Smart Cities," *Computer Communications*, vol. 149, pp. 78-89, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] F. Sammy, and S. Maria Celestin Vigila, *An Efficient Multiauthority Attribute-Based Encryption Technique for Storing Personal Health Record by Compressing the Attributes*, Advances in Communication Systems and Networks, pp. 571-575, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Honggang Wang, "Security Protection between Users and the Mobile Media Cloud," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 73-79, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[15] Lifei Wei et al., "Security and Privacy for Storage and Computation in Cloud Computing," *Information Sciences*, vol. 258, pp. 371-386, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ritesh Shivhare, Ritu Shrivastava, and Chetan Gupta, "An Enhanced Image Encryption Technique Using DES Algorithm with Random Image Overlapping and Random Key Generation," *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, Bhopal, India, pp. 1-9, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[17] Rao V. Seetha Rama et al., "FPGA Implementation of Digital Data Using RSA Algorithm," *Journal of Innovation in Electronics and Communication Engineering*, vol. 9, no. 1, pp. 34-37, 2019. [Google Scholar] [Publisher Link]

[18] Xiao Dong, David A. Randolph, and Subhash Kolar Rajanna, "Enabling Privacy Preserving Record Linkage Systems Using Asymmetric Key Cryptography," *AMIA Annual Symposium Proceedings*, vol. 2019, pp. 380-388, 2019. [Google Scholar] [Publisher Link]