iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43621

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Database Security using Cryptography

Yash Singhal[1], Adwit Agarwal[2], Shivank Mittal[3], Shrishti Katyayani[4], Amit Sharma[5]
[1, 2, 3, 4, 5]*Department of Information Technology, Inderprastha Engineering College, Ghaziabad, India*

Abstract: ***There has been an explosion in data since last two decades and this explosion of data is due to high rates of data conversion and better internet services worldwide [21]. All the conventional methods of data handling have been replaced by much more sophisticated means. One of the typical shifts of the emerging information society is that information is becoming a crucial if not the most vital source. Information contrasts profoundly from further resources; for example and it can be imitative without cost, it can be erased without leaving traces. [22] Protecting the new resource information is a major issue in the information economy [20]. One such means is a Database. It makes it easier for data related queries but it can be dangerous if this data is leaked or sent outside the organization. A high price is positioned on confidentiality when information concerning state secrets, business plans, war strategy, medical records and financial transactions needs to be stored or transmitted. Since its inception, the Internet has enable [19]. A cyber crime emerging in recent years data breach is one of the most notorious and disastrous data crimes majorly caused due to unsecure database. To secure these databases we can apply the concepts of AES algorithm. It is an algorithm used in cryptography which changes normal text to unreadable or cypher text.***
Keywords: Cryptography, AES, cypher, digitzation, confidentiality

I. INTRODUCTION

There are wider range of internet applications in the modern world. There are various organizations that need intense information security such as Government Agencies, Financial Institutions, law enforcement etc. They need modern crypto algorithms to make sure that their confidential information is safe and secure and can't be accessed by any third party. All Cryptosystems use either Symmetric or Asymmetric encryption. [8] Symmetric Encryption requires only one Cryptographic key for encryption and decryption and is considered faster as compared to Asymmetric Encryption whereas Asymmetric Encryption consists of two cryptographic keys namely: Public key (which is disseminated key) and a private key (which is known only to the author). DES, Triple DES, AES algorithm etc. are -some of the examples of Symmetric Encryption. Diffie-Hellman, RSA algorithm are few of the examples of asymmetric algorithm [4].

There are various incidents of data breach. A data breach incident is a security incident in which a third party or person obtains access to the information which had to confidential. As per reports, India positions 3rd in the world in relations of number of data breaches. A whole of 86.3 million users information breached till November 2021.India showed an increase of almost 300 times in affected accounts compared to previous quarter. It states that approx 1 billion email accounts have been uncovered in both the years 2020 and 2021. Till November 2021, 952.8 million accounts were penetrated, which means that 1 out of every 5 population were affected worldwide [5]. So, a strong and reliable key management process is essential to prevent access to unauthorized access to sensitive data and information. Performance, strength of algorithm, data access, data type, community acceptance, cost, and key management should all be considered in order to choice the most suitable resolution [6].

Ensuring a suitable level of protection to database content affects the overall security model. Even though encrypting the data provides important protection, there are implementation decisions that affect the encryption process. These factors may be where will be the encryption of data would take place, what type of encryption algorithm is used, how well the encryption keys are managed [14] and protected, etc. In conventional client server-based encryption, the data is encoded using a server key or a client key in the database. There will be a constant vulnerability if there is a weak key at any end. In both the cases, the most important issue is the loss of the key used in the encryption process[7]. If the key is lost all the data is lost.

In this research paper, we will be mainly focusing on AES Algorithm. With an increase in computing power a vulnerability against certain key searches were found. Triple DES was created to overcome this problem but it failed. It is found about 6 time faster than the triple DES. It has 128-bit data, 128/192/256-bit keys. It can be implemented in Java and C. It is based on 'substitution–permutation network'. [3] It contains of a series of related operations, few of which comprise swapping inputs by confident [18] outputs (substitutions) and others involve shuffling bits around (permutations). Surprisingly, AES performed all its computations on bytes where other conventional algorithms extensively used bits for their operations. AES treats the 128 bits of a normal text [2] block as of 16 bytes. These 16 bytes are organized in 4 columns and 4 rows for handling a form of matrix.

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

The word cryptography comes from the word Cryptos, which means hidden words and Graphen which have the meaning of writing, so the word cryptography can be interpreted as an art or science that examines how data is converted into certain forms that are more specific and difficult to understand by others. Cryptography has the purpose of being able to maintain the confidentiality of information or data that must not be known by others who have no interest in the information or data. Much work has been done related to this field of Cryptography. [13] Prior relational database cryptography research considered the encryption and decryption process of fields in accounts using Symmetric Encryption and Asymmetric Encryption. Recent research papers show that various research has been done in the area of Database as a Service (DAS). The main reason behind these research is to encrypt the database so that our information can't be accessed by any third party and only a set of authorized and desired users have the access to that database.[25] Approach proposed by Mykletun and Tsudik familiarizes a server coprocessor also known as SC, which is hardware with a processor, an input device, a backup battery, protected memory, and a tamper proof container. A server coprocessor is installed on the server which supports all the ongoing cryptography operations. The client can communicate with the server coprocessor with the help of a secure channel. A model was proposed by the authors and developers to counter DOS attacks but the bigger problem was still not addressed.

Database encryption allows a business house or an enterprise to secure data as all the query operations are taking place in the background. Database-level encryption defends the data within the DBMS and also guards against a inclusive range of threats, including storage media theft, well known storage attacks, database-level attacks, and malicious DBAs. All the application-based models are eliminated by Database-level encryption. While this solution can certainly safeguards data, it does want some integration work at the database level, comprising alterations of existing database schemas and the use of triggers [1] and stored procedures to undertake encrypt and decrypt function. Many algorithms were implemented but it failed to provide protection against application-based attacks.

Das displayed a fresh algorithm for partial program authentication that runs in polynomial time and space, this algorithm can verify that a program pleases a specified sequential safety property. Their intuition is that by precisely demonstrating only those branches in a program for which the property-related behavior varies along the supports of the branch, an algorithm can be designed which is accurate in verification of the program. This is very helpful in solving the state-space explosion problem and can be applied to large programs. They have used the algorithm to provide the first verification of temporal safety properties for a program of the size of GCC.

During Covid-19 Outbreak, several incidents have been observed where cybercriminals acted as Officials from World Health Organization (WHO), Centre for Disease Control and Prevention (CDC). As per reports, 92% malware is transmitted through mails. Third party apps store almost 100% of discovered mobile malwares. On an average 70 records were stolen every second. It was found that it took around 7 months to detect a data leak within an enterprise. The average rate of data breach was found to be almost 5 million USD. Small businesses and enterprises were the victims of almost 50% of the data breaches. 54% of the data companies hold is Outdated. The largest data breach in the history of mankind is the 2013 Yahoo Data Breach where the data of almost half the population of world users were breached.

III. ALGORITHM

In cryptography algorithms are based on the process of encryption and decryption[18].Encryption is changing the database into non-recordable script. Decryption shows the reverse process of encryption where it changes the cipher text to a normal text and decryption is the is the opposite operation of the technique of altering the normal text into illegible. There are basically two types of cryptography algorithms[19]:

A. Asymmetric Cryptography

Asymmetric cryptography is a cryptographic system in which public and private keys are used as a pair. Public key disseminated publicly and on the further side private key is known by real owner only.[17]

B. Symmetric Cryptography

In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. [16] The key plays a crucial part in symmetric cryptography since their security straightly counts on the nature of key[15] i.e. the key length and other factors.

\

There are multiple types symmetric cryptography whichare widely used in the industry[14].They are-

1) Data Encryption Standard(DES)
2) Triple Data Encryption Standard(3DES)
3) Blowfish
4) Advanced Encryption Standard(AES)

Each of the above mentioned algorithms uses different approaches for encryption purposes in a secured system however the methods used by DES and 3DES are mostly same. Data Encryption Standard(DES) practices a 56 bits to make the key secure whereas Triple Data Encryption Standard(3DES) uses 168 bits to make the key. The main difference is of size in both the algorithms, but the functioning of both the algorithms is more or less same[13].But for our security system we will be using Advanced Encryption Standard(AES).

Advanced Encryption Standard(AES) whose orinial name is Rijndael, developed by the US National Institute of Standards and Technology(NIST) in early 2000s[12]. AES is the latest of the 4 present algorithms accepted for federal us in USA. AES is a symmetric encryption algorithm which is processing data in block size of 128-bits. AES is symmetric algo as the identical key is used for encryption as well as for the reverse transformation, decryption. The only secret necessary to keep for security is the key [11].

Features of AES are that in the contrast of DES algorithm [10] it works on SP network instead of a Feistel Cipher. AES can automatically expand keys as the number of rounds increase in successive trials. In AES the operations are performed [12] on byte data butnot bit data ,hence it treats the 128-bit key size as 16 byte during the procedure of encryption.

IV. METHODOLOGY

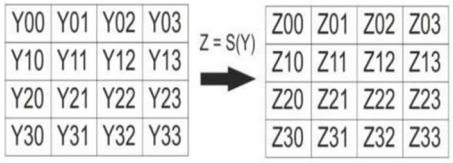
AES algorithms is one of the most complex algorithmsof the recent times and takes a really long time to be broken. The complexity of this AES algorithm is hidden in it's complex working [9]. AES algorithm follows the given to convert our Plain Text to Cipher Text.

A. *Transformation Step*

The processing steps are known asTransformation steps in which the Plaintext is changed into an array before proceedingfurther with the steps.

B. *Substitution Step-*

In this step each and every byte in the array is swapped with its sub byte.



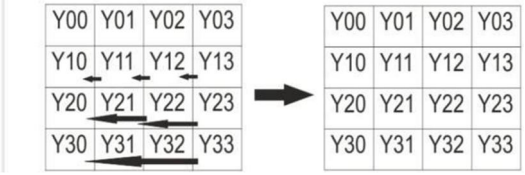
For Example-

Y12 is replaced with Z12, whereZ12=S(Y12) = Sub Byte of Y12Y12, Z12 = A Array Byte

S = Sub Byte

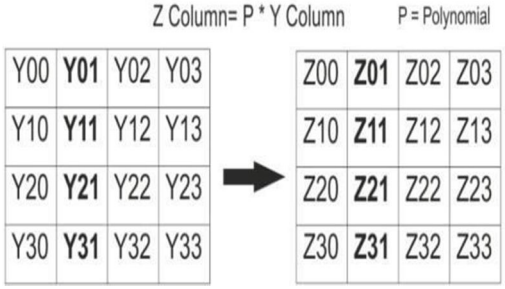
C. *Row-shifting Step-*

The initial row remains the same in this step but thesecond row is moved from Right to Left single stepat a time. These number of rounds keeps on increasing by one for every next row.



D. Column Mixing Step

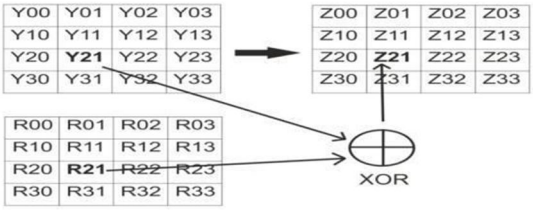
In the following step the columns are selected one by one and each column is multiplied by a polynomial P.



E. Round-Key Addition Step

In the final step a round key is added in each byte of an array. A XOR gate is used for the purpose of adding of round key in the array.

Y, Z = Array ByteR = Round Key



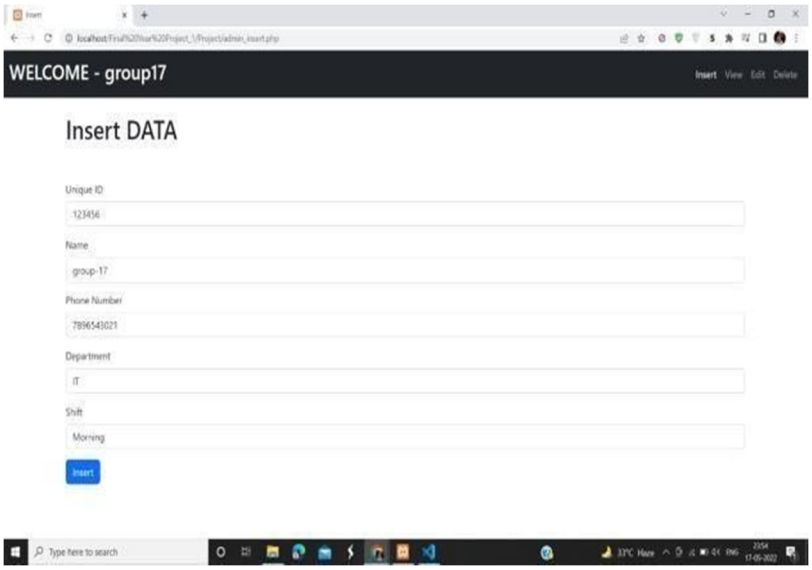
In the above process we can convert the Plain text into Cypher Text (encryption process). To convert the Cypher Text into Plain Text (decryption process) we have to reverse the same process and we will acquire the Plain Text.

V. RESULT

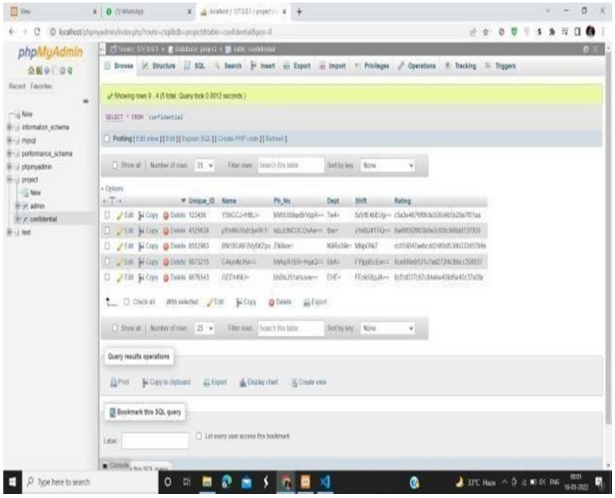
As a result, we have developed a system that is somewhat capable of encrypting the data within the database so that it can be stored in the encrypted form and when retrieved by an authorized personal it shows the decrypted form.

Below are some screenshots attached to show how the system works,

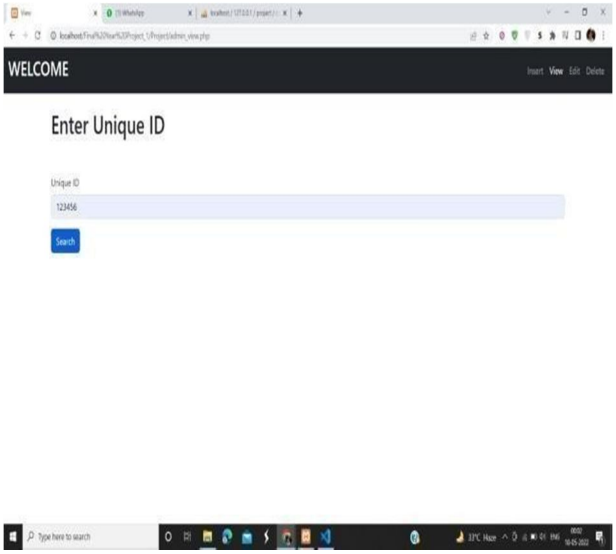
1) The main interface of the system from where a user can enter all the details to be entered.



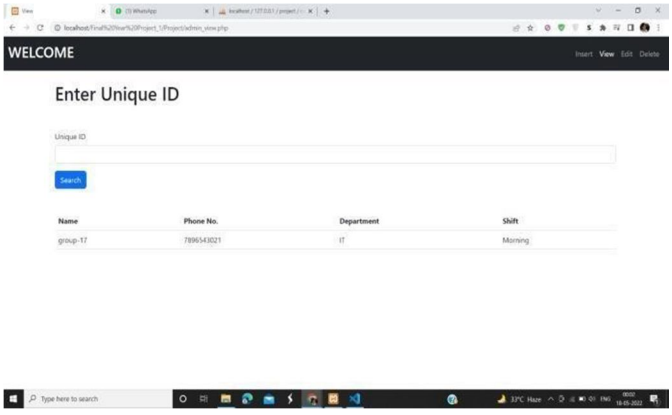
2) *This is the database where the text is stored in the encrypted form. Even if there is a data leak,the text stored is unreadable.*



3) *To retrieve the decrypted form of data a special is to be entered so that the data can be viewed in a readable form*



4) *If the key entered is correct than the data will be extracted in a readable or decrypted form. If the key (hash value) entered is wrong it will give out an error*



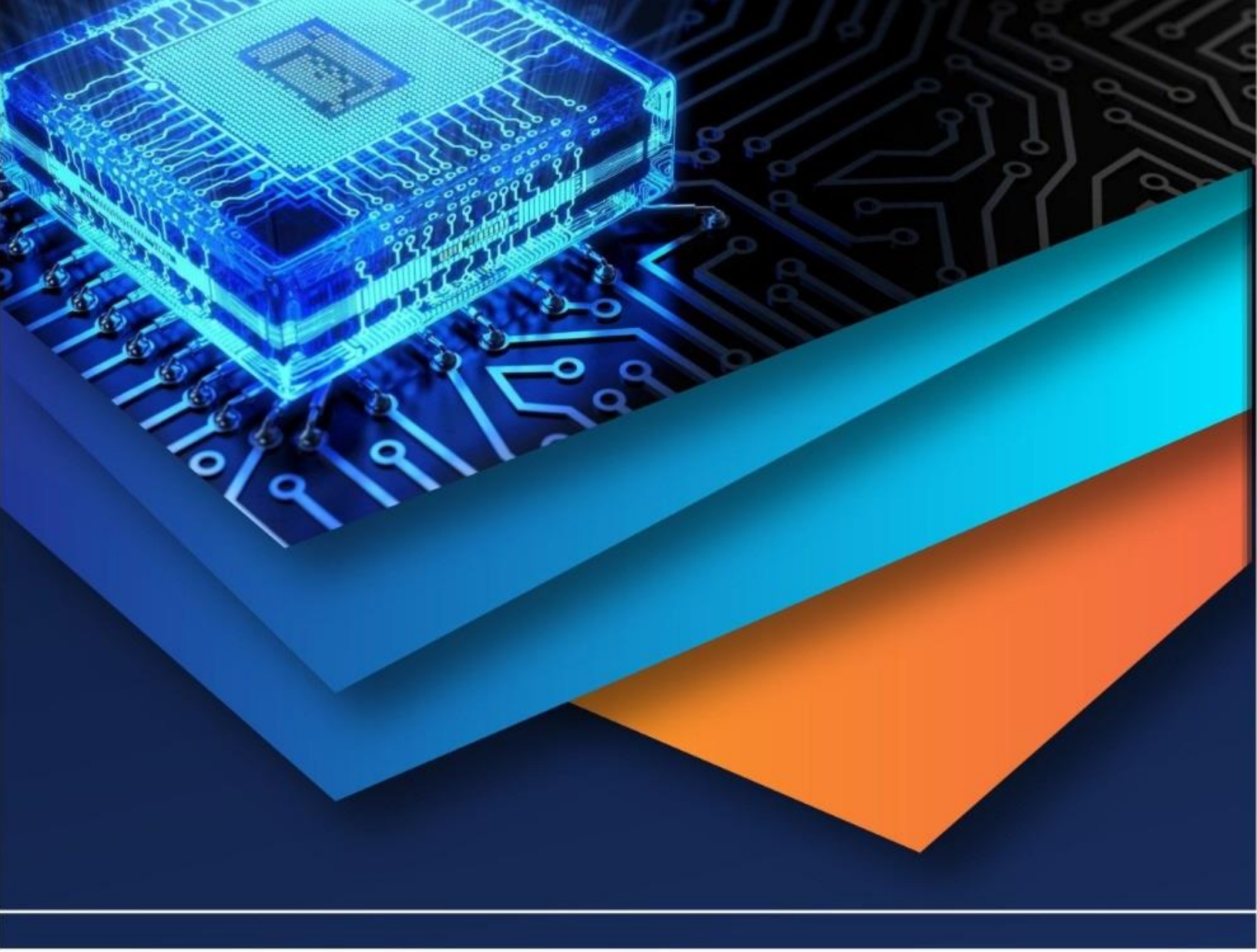
VI. CONCLUSION

In this paper, we checked several cryptographic techniques and it is their components on which the whole method of cryptography works. Although, many difficulties arise in carrying out different cryptographic algorithms but there is always a technique that overpowers the concerns of threats. In our research paper we even conversed about diverse areas and sub techniques of cryptography. But although how hard we may try there's always a scope of error and threat. The systems, techniques and algorithms are getting advanced no doubt but we have to keep in mind that malicious persons are also using advanced techniques to steal the information by every fair or foul means. While enabling Transparent data Protection, it is a prudent idea that you should immediately backup the private key associated with the certificate and the certificate. If our certificate somehow gets inaccessible then you must attach the database on a different server, you must have backups of both: the certificate and the private key or else you will not be able to access the database. Deploying and integrating this system to its maximum potential requires massive funding and research.

REFERENCES

[1] An Efficient and Secure Public Key Authenticated Encryption with Keyword Search in the Logarithmic Time and calculation variance LIDONG HAN 1,2, JUNLING GUO2, GUANG YANG2, QI XIE 1,2, AND CHENGLIANG TIAN 3 1Key Laboratory of Cryptography Technology of Zhejiang Province, Hangzhou 311121, China 2School of Information Science and Technology, Hangzhou Normal University, Hangzhou, Zhejiang 311121, China 3School of Computer Science and Technology, Qingdao University, Qingdao 266071, China
[2] "A Novel Framework for Database Security based on Mixed Cryptography"-2009 Fourth International Conference on Internet and Web Applications and Services.
[3] "DES Algorithm Security Fortification Using Elliptic Curve Cryptography"- Conference: 2015 Tenth International Conference on Computer Engineering & Systems (ICCES)At: Cairo, Egypt
[4] "Global Information Assurance Certification Paper." May 2011, Conference: Global Information Assurance Certification Paper, at: SANS Institut
[5] "An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions"-Wenner and Gren Centre,113 46 Stokholm ,Sweden
[6] "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis"- Department of Computer Science, Himachal Pradesh University, Shimla, Indi
[7] "New Modification on feistal DES algorithm based on multi-level keys"- Suhad Muhajer Kareem1, Abdul MonemS.Rahma,1)Department of Computer Science, University of Basrah, Iraq,2)Department of Computer Science, University of Technology, Iraq
[8] A Collaboration of RSA Algorithm using EM2B Key with word auto key encryption cryptography method in encryption of SQL Plaintext Databases
[9] Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data and Analysis, Muhamad Abdullah MSc Computer Science –UK PhD
[10] A Study of Encryption Algorithms AES, DES and RSA for Security By Dr. Prerna Mahajan & Abhishek Sachdeva IITM, India"Global Journal of Computer Science and Technology Network, Web & Security"
[11] J. Daemen and V. Rijmen, The block cipher Rijndael, Smart Card research and Applications, LNCS 1820, Springer Verlag pp. 288-296
[12] Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Ako Muhamad Abdullah MSc Computer Science –UK PhD Student in Computer Science Department of Applied Mathematics & Computer Science Eastern Mediterranean University – Cyprus
[13] Design and Simulation DES Algorithm of Encryption for Information Security, "American Journal of Engineering Research (AJER),e-ISSN: 2320-0847 p-ISSN :2320- 0936,Volume-7, Issue-4, pp-13-22,www.ajer.org"
[14] International Journal of Advanced Research in Computer Science and Software Engineering" Comparative Analysis of Symmetric Key Encryption Algorithms"
[15] An Overview of Public Key Cryptography by Martin Hellman
[16] A Comparative Survey on Symmetric Key Encryption Techniques
[17] Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange
[18] "Global Information Assurance Certification Paper Revised 2019"-
[19] "Global Information Assurance Certification Paper"- Global Information Assurance Certification Certified UNIX Security Administrator
[20] "The Role of Cryptography in Database Security Ueli Maurer"- Department of Computer Science ETH Zurich CH-8092 Zurich, Switzerland
[21] A Novel Framework for Database Security based on Mixed Cryptography Hasan Kadhem1, Toshiyuki Amagasa1;2, Hiroyuki Kitagawa1;21Department of Computer Science, Graduate School of Systems and Information Engineering 2Center for Computational Sciences, University of Tsukuba1-1- 1 Tennodai, Tsukuba, Ibaraki305
[22] "An Efficient Secure System for Fetching Data From the Outsourced Encrypted Databases"-SULTAN ALMAKDI 1, BRAJENDRA PANDA2, (Senior Member, IEEE),MOHAMMED S. ALSHEHRI 1, (Graduate Student Member, IEEE), AND ABDULWAHAB ALAZEB 1,2, (Graduate Student Member, IEEE)1Department of Computer Science, College of Computer Science and Information systems, NajranUniversity, Najran 55461, Saudi Arabia2Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, AR 72701, USA

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)