JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DESIGN OF HIGH SECURITY BASED DATA TRANSFER SYSTEM BY USING CRYPTOGRAPHY ALGORITHM

[1]T.GunaPrakash Reddy,[2]Dr.K.Venkatachalam,[3]M.Prasad Rao
[1]PG Scholar,[2]Assistant Professor, [3]Assistant Professor ,Dept. of E.C.E
[1,2,3]Audisankara College of Engineering and Technology (Autonomous), Gudur, SPSR Nellore (Dt.) A.P

Abstract: Data security upgrade utilizing the multilayer linear feedback shift register (LFSR) cryptographic procedure to beat the issue of data hacking. The data security is accomplished with a One Time Pad (OTP) calculation created in multilayer which characterizes the sign transmission in the medium. The Pseudorandom Noise (PN) succession made by the primitive polynomial is utilized to get the seed esteems that are utilized to portray OTP usefulness. The single-layered LFSR cryptography is examined with a fell LFSR cryptography strategy to demonstrate the security of digitized data. The authentication key generation circuits for different degrees of bit dealing with in data correspondence frameworks are carried out in LFSR cascaded cryptography in both encryption and decryption measure.

I.INTRODUCTION

Cryptography has had an interesting history and has undergone many changes through the centuries. It seems that keeping secrets has been important throughout the ages of civilization for one reason or another. Keeping secrets gives individuals or groups the ability to hide true intentions, gain a competitive edge, and reduce vulnerability. The changes that cryptograph has undergone throughout history closely follow the advances in technology. Cryptography methods began with a person carving messages into wood or stone, which were then passed to the intended individual who had the necessary means to decipher the messages. This is a long way from how cryptography is being used today. Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique of hiding the plain information from the web. By using cryptography we can assist this shaky information by secrete writing on our computer network. Cryptography renders the message unintelligible to outsider by various transformations. Information that are disseminated within an office, across offices, between branches, of an organization and other external bodies and establishments at times get into the hands of the unauthorized persons who may tamper with the contents of the information. And if no security measures are taken, there is no doubt that such data and other sensitive information will be exposed to threats such as impersonation, insecrecy, corruption, repudiation, break-in or denial of services that may cause serious danger on the individual or organization. A secure system should maintain the integrity, availability, and privacy of data. Data integrity

usually means protection from unauthorized modification, resistance to penetration and protection from undetected modification. Therefore, algorithms which help prevent interception, modification, penetration, disclosure and enhance data/information security are now of primary importance. This is to ensuring that the intruders do not have access to the plaintext without a secret key. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric schemes, one key is used for encryption and another is used for decryption. The increased confidence in the integrity of systems that use encryption is based on the notion that cipher text should be very difficult to decipher without knowledge of the key. Fig.1 explains the process about how the plain text converting into encrypted data and encrypted data converted into plain text using decryption algorithm.

II.LITERATURE REVIEW

A Database Record Encryption Scheme Using the RSA Public Key Cryptosystem and Its Master Keys

This paper presents two different encryption schemes for database. Both schemes use RSA algorithm. The first one is field based encryption system. All fields are accessed by master key of user. Next, represents record oriented encryption. It uses only one master key. This method applied in subsets and integers group. [18-22]To provide security to the database is one of the complicated problems. For this, asymmetric crypto system is commonly used. Basically encryption keys are used to write data in protected fields. Decryption keys are used to read the data. So it provides the access rights for user. The simple encryption method for database is RSA method. RSA master key pair contains two different keys. Encryption keys are used to represents the right of write operation. The right of read operation is represents by decryption keys. The key pair is maintains by database manager. All rights of fields are combined by RSA master keys. Database manager establishes each field of database in database encryption schemes. Access rights are allocated by using this method. This is used to allocate the access rights depend upon the user requirements. Generally, dynamic data storage is used. Read operation is the most frequent compare to other. Generally, write operationsaremove to write proxy for approval. [23-24] The Scheme 2 establishes CRT. This method prevents from the outside attack. It prevents the traffic analysis also. To manage key management problems, both schemes use the RSA master key. Both provides the access rights to user and database security.

Chip-Secured Data Access: Confidential Data on Untrusted Servers

Major aim of ubiquitous computing is to provide data anywhere, anytime, anyhow only. It is used to enhance the database connections to Internet. And also it should ensure about the data confidentiality. Day by day, malicious attacks and security threats are increased. So, Trusting traditional database security methods is somewhat danger. In this paper, a new method named C-SDA (chip secured data access) is proposed. This control the users' access rights and provides data confidentiality. And also act like a inter mediator between client and encrypted database. This element is embedded in a smartcard. This consists, combined hardware and software. It ensure against attacks. Query evaluation techniques are used mostly.

A Framework for Efficient Storage Security in RDBMS

Day by day, growth of E-business is tremendously increased. So everybody should be aware about data security and database security. Some RDBMS storage models (such as the N-ary Storage Model) stores records. Offset table is used at the end of the page. It is used to locate the starting point of record. If query is more sensitive, NSM provides tremendous performance. It is used to transfer data to and from secondary storage. This is suitable for online transaction processing. [25-28] this paper proposes a novel protective model for storage and key management architecture. It consists of various encryption methods. It ensures high level of database security. In this paper, TPC-H dataset is used with Partition Attribute across (PAX). [29-31] a page will be divided into mini pages. So it increases cache performance. A mini-page contains one attribute of record. Depend upon plain and cipher text attributes, the plaintext and

cipher text of PAX used to divide the page into two mini pages. So each record is dividing into two subordinate records. It reduces the cost of encryption as well as storage and computation costs. It takes benefits of NSM. It needs few modifications to page layout.

III.EXISTING SYSTEM:

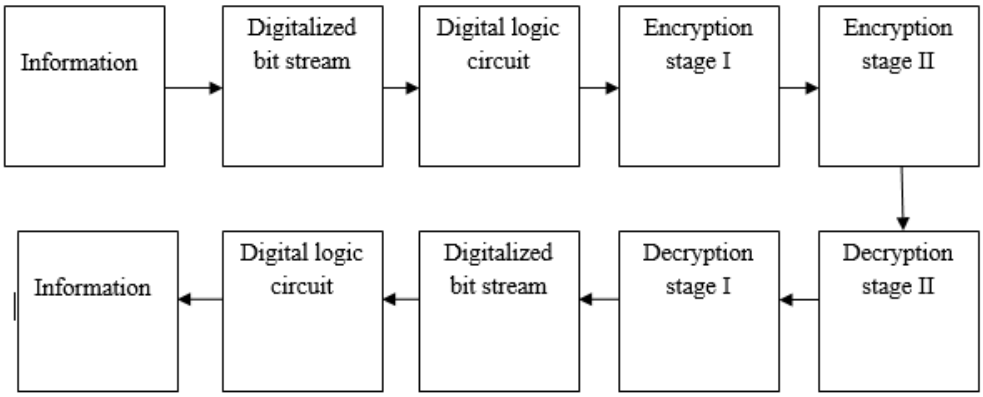
Internet of things is a complex structure of all the objects, which can be managed through internet. Due to its advance features of accessibility and management it is rated as one of the most in demand technology in the approaching eras, with a proven performance to serve the human society in their daily life with the help of numerous allianz of objects. It faces the security challenges such as peer-to-peer authentication, data confidentiality from eaves dropping. As Internet of things are multicast user approach in which there is a continuous communication between the numerous objects and the user. It is very much necessary to provide strong security system to secure our resources from any type of rupture in security and vulnerability. So converging on this precise matter, we proposed the system with the combined approach of two security techniques. One is layered authentication approach followed by Elgamal end to end security technique. Operation of this technique is to work in two phases: at first level authentication process is working along with sub-server for providing authentication to access the real data server, and in the second phase. Once user approaches to the real server he has to go through the public cryptography technique, where data is encrypted with Elgamal cryptography technique to provide end-to-end security. The entire work is deeply analyzed with the available factors related to authentication and cryptography. Finally the proposed system will provide strong security for the data preservation and the communication more effectively.

IV.PROPOSED METHOD

LFSR OTP encryption and decryption algorithm is used. The number of steps has been increased in both the encryption and the decryption process to attain the high security level of data. Here the OTP algorithm is presented in such a way that the process includes a Bit reversal process after the EXOR operation. The reversed sequence is performed with a 1's complement operation then once again the bit reversal operation is performed to get the Ciphertext. This helps to improve security than a single layer. In the above proposed LFSR cryptography technique, multi-layers can be used to achieve higher security. The LFSR OTP decryption. Here the reverse process of the encryption process is performed to retrieve the original information. Then the sequence is made to experience the routine extraction process using the PN sequence. Without the knowledge of the OTP algorithm network hacking will be difficult on the information transmitted.

Multilayer or Cascaded Cryptography Multilayer or cascaded cryptography is the process of encrypting an already encrypted data into two or more times either by using the same or different algorithms. Block diagram for the proposed multilayer cryptography is explained. Information is the input image. The input image is then converted into the digitized bit stream. This bit stream is taken for the encryption and decryption stages. The resultant bit stream is then converted into the original image which is the input.

V.BLOCK DIAGRAM



In this block diagram, information is the input image. The input image is then converted into the digitized bit stream. This bit stream is taken for the encryption and decryption stages. The resultant bit stream is then converted into the original image which is the input. Conversion of the image into bit stream and bit stream into an image is done by using the Matlab software.

Before doing the cryptography process, the input image is converted into the digitized bit stream. For converting the input image into the digitized bit stream the Input RGB image is converted into the grayscale image. At the same time, the corresponding matrix format is also generated. A grayscale image is converted into a black and white image and the corresponding matrix is also generated and viewed. To attain the digitized bit stream, the encoding process is done. This digitized bit stream generated from image processing is very much important and used for the multilayer cryptography process. Multilayer LFSR OTP encryption and decryption algorithm is explained in the Figure 2 and 3 respectively.

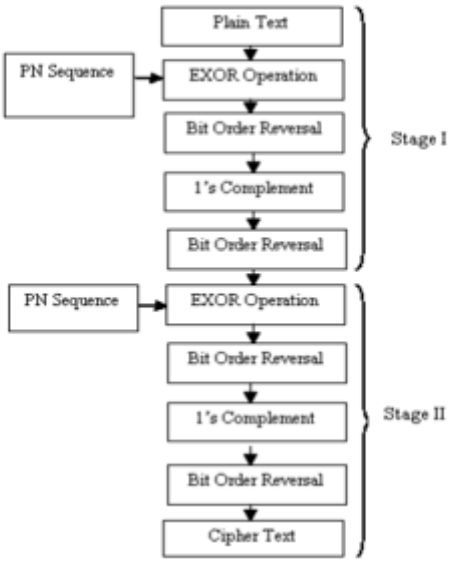
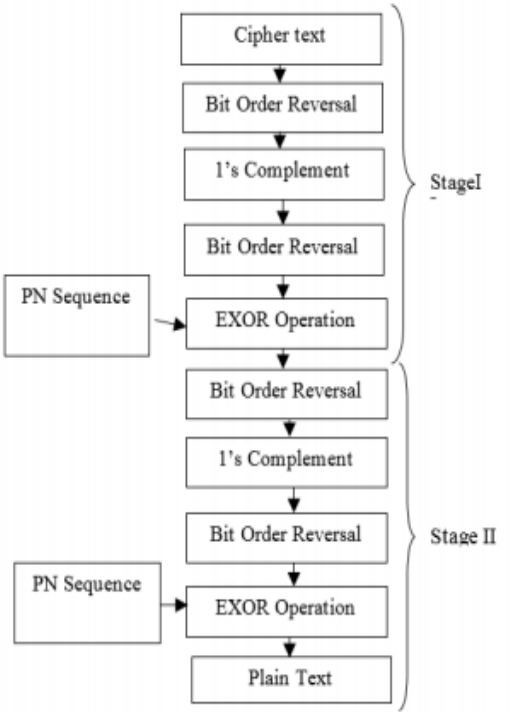


Fig 2: Two stages of LFSR OTP encryption

Fig 3: Two stages of LFSR OTP decryption



VI.RESULTS:

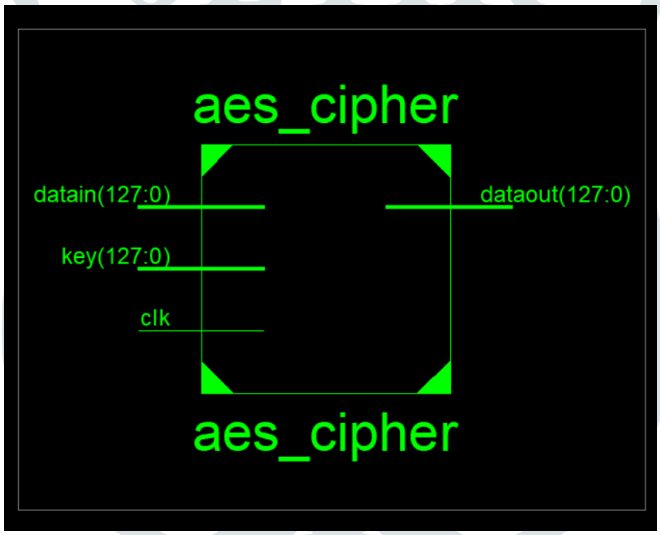


Fig 3:RTL Schematic

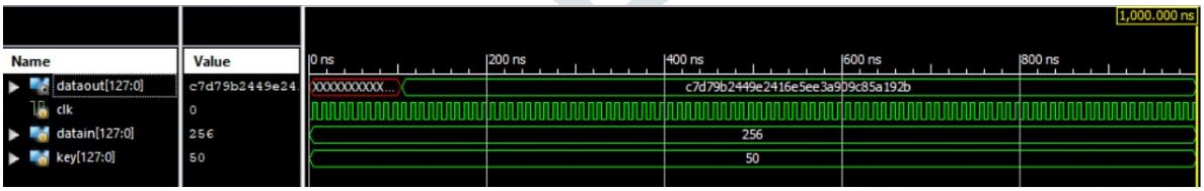


Fig 4:Encryption process

Fig 5:Decryption process

V.CONCLUSION

The importance of wireless networks and various threats faced by them. To secure the wireless networks various techniques can be used. Encryption algorithms play a main role in information security systems. On the other side, those algorithms put CPU load and consume battery fast. This paper provides evaluation of encryption algorithms like AES, DES, and A comparison has been conducted for those encryption algorithms and Blowfish is found to be the best encryption algorithm. Several points can be concluded from the simulation results. The first layer and second layer of cryptography are completed with the help of the LFSR cryptographic technique. The cipher text for the LFSR cryptography is generated. Here both the encryption and the decryption process are done by the OTP algorithm. Due to this security of the data has been enhanced and the various cryptographic techniques have been summarized. The work focused on the design of effective single-layered cryptography as well as multilayer cryptography by using the LFSR cryptographic technique. Various levels of the bit handling process in the data communication system are implemented successfully through this LFSR cryptographic technique by generating the authentication key.

REFERENCES:

[1] Alessandro Cilardo "Exploring the Potential of Threshold Logic for Cryptography-Related Operations" In IEEE Transactions On Computers, Vol. 60, No. 4, (April 2011).

[2] Babitha P. K, Thushara T, Dechakka M. P. "FPGA based N-bit LFSR to generate random sequence number" in International Journal of Engineering Research and General Science Volume 3, Issue 3, Part2 , May-June, 2015, ISSN 2091-2730.

[3] Divya Jenifer D' Souza, Minu P Abraham "A multilayered Secure for Transmission of Sensitive Information based on Steganalysis" in ELSEIVER, Procedia computer science 78 (2016).

[4] HuiXua, Xiaojun Tonga, XianwenMenga, "An efficient chaos pseudo-random number generator applied to video encryption" in ELSEIVER, OPTIK 127 (2016).

[5] IrithPomeranz "Computing Seeds for LFSR-Based Test Generation FromNontest Cubes" in IEEE transactions on very large scale integration (vlsi) systems, vol. 24, no. 6, june 2016.

[6] Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011)

[7] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4, July-August 2014 ISSN 2278-6856.

[8] NouraAleisa "Comparison of the 3DES and AES Encryption Standards" in International Journal of Security and Its Applications Vol.9, No.7 (2015), ISSN: 1738-9976

[9] PushpLata, V. Anitha, "Multi-Layered Cryptographic Processor for Network Security" in International Journal of Scientific and Research Publications, Volume 2, Issue 10, October 2012 1 ISSN 2250-3153.

[10] Ritu Tripathi, Sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" in International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

[11] Sahil Agarwal, Barkha Khattar , Dr. Inder Singh, "multi-layered security for private Communication (using steganography and cryptography)" in International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.4, Special Issue (01), March 2015 ISSN-2319-8354(E).

[12] ShraddhaSoni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES Cryptographic Algorithm" in International Journal of Engineering and

Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012 ISSN: 2277-3754.

[13] Sugitha,G A.Albert raj, A "CNLRA : Critical node and Link reconnect algorithm for wireless adhoc networks using graph theory" Asian Journal of Research in Social Science and Humanities Vol 6,no 8 , 2016,pp 1953-1963.

[14] Yashwantkumar, Rajatjoshi, Tameshwarmandavi, Simranbharti, Miss Roshni Rathour "Enhancing the Security of Data Using DES Algorithm along with Substitution Technique" in International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 10 Oct. 2016.

[15] Maria Jessi ,A,Albert Raj " A newfangled method to maintain Infrastructure and Mobility of Nodes by weigh based Clustering and Distributed Scheduling , International Journal of Printing & Packaging Allied Science,Vol 5, no 1 , 2017,pp 24-33 ISSN 2320- 4287.