A REVIEW PAPER ON ADAPTIVE MODIFIED ADVANCED ENCRYPTION STANDARD

[1]Vishal Goswami, [2] Sandeep Somkuwar
[1]Research Scholar, [2]Assistant Professor
Department of Electronics and Telecommunication Engineering
GD Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India

Abstract: Ensuring the security of the sensitive data from being accessed by unauthorized user is very important issue, especially while being transmitted or stored for the companies and end users. Multiple ways are used to do this job; one of the most famous is to use cryptography. Cryptography is used to transfer the data in a form that is not understood by anyone apart from the intended recipient. The advance standard encryption algorithm (AES) is one of the most secure encryption algorithms, but AES suffers from consumption of unnecessary time to achieve the necessary complexity needed to meet the security level, especially for real time application. In this research, a modified scheme is developed for the encryption/decryption algorithm by modifying the MixColumns stage.

The aim of new scheme is to increase the speed of the encryption/ decryption process while maintaining the complexity of the design by using IV vectors depends on true random number generator.

Keywords—Cryptography;AES;Encryption;Decryption.

Literature Survey:

Daemen, Joan, and Craig Clapp (1998) [4] presented PANAMA which is a module that can be utilized as cryptography hash function and in addition stream cipher. They have demonstrated that quick executions of programming could be possible utilizing inherent/innate parallelism on VLIW processor. Panama is basically based upon a machine which utilizes 8192 buffer and 544 bit state. These two are updated by utilizing loops/cycles/iterations. Panama utilizes hermetic hash function which must include: The normal workload of creating a collision is of the request of 2^(n/2),if n bit worth/value is given then expected workload of discovering the message is 2^n executions of hash function, when message and its hash value is given then expected workload of discovering the second message is of the request of 2^n executions of the hash function, Panama is likewise K secure if a key stream output alongside a given key and picked estimation of q is given then the compelling approach to get the learning of the key could be possible by doing exhaustive search. The future scope of panama is that it will be utilized as a part of set top boxes and digital televisions which will be utilized as a part without bounds in future that they utilize media processors for decompressing videos for performing different tasks. The panama gives high information/data rates.

Canright, David (2005) [3] defined more complex/intricate S-Box. In S-Box every subfield was filled by polynomial basis as well as ordinary basis which gave 432 cases altogether. The best case with the implementation of this algorithm gave 20 % change/improvement. They have shown optimizations in GF (2^8) inverter for best case. Implementations include two distinct representations of GF (2^8). The standard structure used the vector of 8 bits. The best approach to use these two methods is to encode/encrypt every block of plain text using AES algorithm and decrypting it in the reverse request. The above algorithm consumed smaller region in ASIC hardware versions of AES. So, this saved region which can adjust one more chip of S-

Box which works parallel in future. They have contrasted their work and 431 versions accessible yet have demonstrated that their algorithm is superior to all. This reduced S-Box can be used for some future hardware implementations of AES for many security applications.

Harrison, et al.(2007) [9] proposed novel encryption methodology for implementing AES Algorithm. An AES utilized block cipher method for encryption. By actualizing or implementing AES on GPU, various processes could be possible in parallel. First both electronic code book and chaining block cipher mode was connected to check the execution of the proposed implementation. In any case, chaining block cipher revealed the best results. At long last they have reasoned that the operating system reports 100 % burden amid GPU's task execution.

Key stream generators (A5/1, W7) (Zeghid, Medien, 2007) [17] are used to enhance the performance of AES for images which have reduced entropy. The researchers have implemented image encryption by vector quantization i.e. image is decomposed into vectors and then encryption and decryption is done vector by vector. After encryption the image is transformed into shadows which are not understandable to intruders. Image text encryption has also been achieved by chaotic algorithms by them. The chaotic algorithm used by them is based on Lorenz equations. They tried implementing DES (Data Encryption Standard) but it was so complex and involved very large computations. It was also not fast to process huge data formed by multimedia applications and hardware which was used to implement DES was so costly. So, the solution to all problems was solved with the introduction of AES .AES is used in those applications which requires fast processing. They have also done analysis of various security issues. Like statistical approach, key space analysis to prevent data from cipher text attack, statistical attack, plain text attack, brute force attack, etc. In histogram analysis, histogram of original image was showing so many peaks whereas that of the encryption image the histogram was fairly uniform without many ups and downs. Applying all above techniques the problem of textured zones was not solved. But when they applied W7 key stream generator the problem of textured zones was easily solved. W7 key generator was proved better than A5/1 key stream generator.

Block cipher mode (Morris Dworkin 2010) [5] is one of the mode upon which AES is implemented. The researchers have provided recommendation for the block cipher mode of AES. Mode is known as key wrap (KW). When the key wrap is done with the padding to provide interoperability then this is known as key wrap with padding (KWP). The triple idea key wrap (TKW) is used to support legacy applications. The above all techniques provide confidentiality as well as integrity to keys as well as data. Forward transformation is permutation of data is caused by the block cipher in conjunction with the key. The key used in forward transformation is called key encryption key (KEK). The inverse of forward transformation is known as inverse transformation. For key, the wrapping and the unwrapping functions are applied on the 3 or more blocks. But the resulted length of output is same as input for both functions. Prerequisites are KEK and K and 128 bit cipher block. Two types of algorithms are explained for the key wrapping.

The plain text is expanded in the authentication encryption function which provides the authenticity to the data. If the output is a plaintext then the cipher text is authenticated else it is not authenticated.

Hermassi, Houcemeddine et al. (2013) [10] proposed better versions of picture

cryptosystem by adjusting/modifying S-box as well as P-box of classical cryptography. By applying such modification the brute force attacks reduced and execution of encryption and decoding/decryption has increased. Problems confronted by previous chaotic cryptosystems were that they were not secure to attacks like chosen and known plain text. Two modifications done here are basically to S-Box and P-Box. They made plain text which is in connection with key stream. Therefore, at whatever point plain text changes key stream changes naturally. They used PWLCM map for shuffling which reduces the quantity of iterations to transform the rows as well as columns. Instead of using ECB they utilized CBC in which every plain text block gets Xored with previously used ciphered data block. Security was broke down using co-connection of adjoining pixels and histograms. In any case, the issue still exists in generation of key and in the permutation process. At last they concluded that attacker will be more confused when user will take the above described method. Subsequently it has shown better execution as contrast with DES, AES, and triple DES. Thus future take a shot at key stream and change could be possible.

Manoj B et al. (2012) proposed AES encryption and decryption on Xilinx ISE 12.4 tool coded in VHDL (Very High Speed Integrated Circuit Hardware Description Language). They have done symmetric key encryption because they are relatively easy to implement and are faster and consumes less power. Here implementation is done with AES 128.7-bit of data was shifted to 128 bit register to AES encryption algorithm and 128 bit encrypted image was produced and then this encrypted image was send to decryption algorithm to get back the original image. Performance of algorithm was calculated n stands for number of clock cycles.

Problems were encountered to them while implementing asymmetric key encryption because it was consuming so much power due to which its implementation was becoming harder. They have concluded that maximum frequency achieved using above technique is 164.562 MHz and the throughput value they observes was 252.132 Mbit/sec for encryption and decryption of the image. Hence they thought the symmetric key encryption a better approach. This same procedure or implementation can be very useful in forensics, Artificial intelligence system, Military communication etc.

Rashmi Ramesh Rachh (2014) [13] has introduced two different systems for hardware computation of AES. The first system for encryption used better S-Box, then implementing add round key and mix column transposition bit wise. And for decryption inverse S-Box, then implementing inverse mix column and inverse add round key bit wise. This architecture takes input if three blocks.

Second system involves encryption by combining block 3 of S-Box with mix-column and add round key. Block 3 of S-Box with inverse mix column and inverse add round key for decryption. These two methods were implemented in VLSI with lesser delay.

Wang, Jing et al. (2012) [15] proposed kerchofs standard for scrambling a picture by utilizing pseudo random permutations. Certain problems were faced when user utilized this encryption scheme. Those problems were if every line and section of the matrix is similar then collector can't decode the message accurately. Besides this each plain text word is connected with one cipher text word yet is not dependent of other cipher text. Consequently can't meet the diffusion and confusion property and if the quantity of iterations is small then statistical attacks can uncover visual data easily. At that point they made new algorithm which solved above problems. After various hypothetical analysis as well as simulations they demonstrated that proposed algorithm acquire better confusion and diffusion properties and is more secure to many attacks.

XTS-AES (Morris Dworkin 2012) [6] is utilized to maintain confidentiality of information stored in storage device. XTS-AES algorithm is an XES i.e. XOR then Encryption and then XOR again with the help of cipher text stealing to increase the data input size. It only provides confidentiality but not authentication. Because when there is no authentication then it gives more protection to the encrypted data. Three elements used in this procedure are a secret key, data unit of fixed length and the apparatus which implements XTS-AES encryption.

Benrhouma et al. (2013) [2] proposed modified technique to actualize partial image encryption. They perceived that today users need a swift response henceforth RSA, AES, DES, IDEA, and so forth algorithms are no more relevant to encryption because they consume huge time. Thus they implemented partial picture encryption based on spatio partial systems which encrypts just a small portion of the information/image to confuse intruder/attacker. Anyhow, when the matter comes to scramble the picture then cryptosystems develops each and every shading/color of picture. Yet at the same time issue was there i.e. there was weakness in security during key generation stream. Subsequently they have infer that when they utilized the same key for many communications like brute force attacks, chosen plain text attacks and so on. However, when they made key to be subject to plain text and infer halfway picture encryption (i.e. to scramble just some portion of the plain text) decreased various attacks.

Gnanaraj et al. (2013) [8] proposed a smart card application to get authentication or access in a specific system. They proposed validation scheme which asks user's identification and password before going into a system. The algorithm is executed in such a way that the processing delay is less when contrasted with the previous algorithms. In this improved version of remote based confirmation scheme has been connected. The secret information entered by the user acts as key and whole information of the user is kept inside server. At whatever point user enters key that information is contrasted with the information present inside server. The smart card first does the acceptance of user and then forwards the information to server for validation purpose. If valid user then is permitted to go into the system else it is rejected or said to login once more. Various attacks are possible such as man-in-the-middle assault/attack, mutual authentication, ID theft assault, and modification assault and so forth. In future other light weight algorithms can be used other than

Overwhelming AES or RSA. Additionally deal with blending the algorithms can also be finished.

Majid Babaei (2013) [1] described that in today's reality the security of picture is exceptionally essential and it has gotten to be extremely hard to secure the images using just a single method so keeping in mind the end goal to secure the picture another strategy for DNA encryption is produced. Various scientific problems were solved using DNA figuring. They used One Time Pad algorithm to solve the issue of picture encryption furthermore the chaotic map as input to one time pad. There are various complex numerical which are used as a device to build up the key and scramble the message so that another strategy is produced to encode the message used as DNA processing in which various DNA framework/matrix were made. As DNA can store substantial (large) measure of information furthermore can perform parallel response so it fastens and made the encryption stronger. In this chaos hypothesis is joined with the DNA computation and after that one time pad algorithm is connected over it to scramble the information or picture.

One Time Password (Ms. E. Kalaikavitha 2013) is key which is valid for 1 session only. The researchers have proposed secure login using encrypted one time password (OTP) and mobile of the user to provide authentication to the system. Their main idea was to increase security. They introduced technique because online based applications mainly use STATIC passwords which are more prone to attacks. Static password are easy to remember and easy to hack because generally users keep their passwords as their birthdays, anniversaries, etc. When user enters username and password, the pseudo random generator generates one time password (OTP) at the web server and encrypts it using AES algorithm. This encrypted OTP is send to the user’s mobile but the user is not able to read it because it is in encrypted form.

Conclusion

An altered variant of the AES for asset compelled conditions is given in this article. Another Substitution Box is presented which works on a solitary, relative change recipe through the Galois Field (24). MAES is recognized by expanding the battery life of low-fuelled gadgets by lessening vitality utilization. This methodology shows 18.35% productivity in transmission by means of the proposed MAES to the sink hub of the scrambled bundles and an expanded number of parcels transmitted. Along these lines, inertness is 29,983 milliseconds. For expansion, the wellbeing question and the unpredictability of room will be routed to make the proposed alteration progressively applicable. Along these lines, during the transmission of encoded information, we intend to examine the multi path way directing frame work In request to accomplish an equivalent proficiency as far as number of bundles transmission and inertness, we will additionally execute open key cryptography, specifically elliptic-bend (ECC), with better insurance.

Referenecs

[1] Babaei, Majid. "A novel text and image encryption method based on chaos theory and
DNA computing." Natural Computing 12, no. 1 (2013): 101-107.

[2] Benrhouma, Oussama, Houcemeddine Hermassi, and Safya Belghith. "Security
analysis and improvement of a partial encryption scheme." Multimedia Tools and Applications (2013): 1-18.

[3] Canright, David. "A very compact S-box for AES." In Cryptographic Hardware and Embedded Systems–CHES 2005, pp. 441-455. Springer Berlin Heidelberg, 2005.

[4] Daemen, Joan, and Craig Clapp. "Fast hashing and stream Encryption with PANAMA." In Fast Software Encryption, pp. 60-74. Springer Berlin Heidelberg, 1998.

[5] Dworkin, Morris. "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices." NIST Special Publication (2010).

[6] Dworkin, Morris. "Recommendation for block cipher modes of operation: methods for key wrapping." NIST Special Publication 800 (2012): 38F.

[7] Ganesan, K., and K. Murali. "Image encryption using eight dimensional chaotic cat
map." The European Physical Journal Special Topics (2014): 1-12.

[8] Gnanaraj, Jaspher Willsie Kathrine, Kirubakaran Ezra, and Elijah Blessing Rajsingh.
"Smart card based time efficient authentication scheme for global grid computing." Human-centric Computing and Information Sciences 3, no. 1 (2013): 1-14.

[9] Harrison, Owen, and John Waldron. "AES encryption implementation and analysis on
commodity graphics processing units." In Cryptographic Hardware and Embedded Systems-CHES 2007, pp. 209-226. Springer
Berlin Heidelberg, 2007.

[10] Hermassi, Houcemeddine, Rhouma Rhouma, and Safya Belghith. "Improvement of
an image encryption algorithm based on hyper-chaos." Telecommunication Systems
52, no. 2 (2013): 539-549.

[11] Norouzi, Benyamin, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, and Mohammad Reza Mosavi. "A novel image encryption based on hash function with only two-round diffusion process." Multimedia Systems 20, no. 1 (2014): 45-64.

[12] Rachh, Rashmi Ramesh, PV Ananda Mohan, and B. S. Anami. "Efficient implementations for AES encryption and decryption." Circuits, Systems, and Signal Processing 31, no. 5 (2012): 1765-1785.

[13] Rachh, Rashmi R., PV Ananda Mohan, and B. S. Anami. "Implementation of AES Key Schedule Using Look-Ahead Technique." Circuits, Systems, and Signal Processing (2014): 1-8.

[14] Wadi, Salim Muhsin, and Nasharuddin Zainal. "High Definition Image Encryption Algorithm Based on AES Modification." Wireless Personal Communications 79, no. 2 (2014): 811-829.

[15] Wang, Jing, Guoping Jiang, and Bing Lin. "Cryptanalysis of an image encryption scheme with a pseudorandom permutation and its improved version." Journal of Electronics (China) 29, no. 1-2 (2012): 82-93.

[16] Wang, Xingyuan, and Qian Wang. "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos." Nonlinear Dynamics 75, no. 3 (2014): 567- 576.

[17] Zeghid, Medien, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. "A Modified AES Based Algorithm for Image Encryption." International Journal of Computer Science & Engineering 1, no. 1 (2007).