International Journal on Emerging Technologies **10**(2): 150-155(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Secure Migration of Mobile Agent using AES & Secret Sharing Approach

***Uttam Upadhyay*[1]*, Pradeep Kumar*[2] *and Deepti Aggarwal*[2]**
[1]PG Student, Department of Computer Science & Engineering,
JSS Academy of Technical Education, Noida, India.
[2]Assistant Professor, Department of Computer Science & Engineering
JSS Academy of Technical Education, Noida, India.

(Corresponding author: Uttam Upadhyay)

(Received 03 May 2019, Revised 10 July 2019 Accepted 17 July 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: As a mobile agent migrates from one host to different host in an open network, the security concern of mobile agent shouldn't be neglected. For this sender and receiver to authenticate one another before agent migration use a powerful authentication method. The security additionally aims to ensure the integrity and confidentiality of the mobile agent whereas it is in transit. Each party should certify one another exploitation public. Several approaches are planned for the migration method of mobile agent. This paper provides associate degree up-to-date survey of migration method of mobile agent analysis. In this research paper we use AES (Advanced Encryption Standard) and Shamir's secret sharing approach to provide the security of mobile agents during the migration process. Advanced encryption standard (AES) algorithmic rule is one on the foremost common and wide parallel block cipher algorithmic rule employed in worldwide. This algorithmic rule has Associate in Nursing own specific structure to encipher and decode sensitive knowledge and is applied in hardware and code everywhere the planet. It's very tough to hackers to urge the real knowledge once encrypting by AES algorithmic rule. Until date isn't any proof to creak this algorithmic rule. Second approach which we use for providing security to mobile agent is Shamir's secret sharing; this technique is used for hiding a secret which is needed in many situations. One possibly ought to hide a password, an encryption Key, a secret formula, and etc. data is secured with encryption, however the requirement to secure the secret key used for such encryption is important too. Consider, we tend to cypher our necessary files with one secret key and if that secret key is lost then all the necessary files are going to be inaccessible. Thus, secure and economical key management mechanisms are needed. One of them is secret sharing theme (SSS) that enables to separate the key into many shares which is able to get distributed to any or all the participants. The key are often recovered once these parties collaborate in some way. This survey paper can study these schemes and make a case for the requirement for the key sharing and their security.

Keywords: Network Security, Encryption, Decryption, AES, Shamir's secret sharing scheme

I. INTERODUCTION

Internet communication is taking part in the necessary role to transfer large amount of information in numerous fields. a number of information could be transmitted through insecure channel from sender to receiver. Completely different techniques and ways are victimization by non-public and public sectors to safeguard sensitive information from intruders owing to the protection of electronic information is crucial issue. Cryptography is one of the most important and widespread techniques to secure the information from attackers by victimization two very important processes that's encoding and decoding. Encoding is that the method of cryptography information to stop it from intruders to browse the first information simply. This stage has the power to convert the first information (Plaintext) into unreadable format referred to as Cipher text. The next method is that has performed by the authorized person is decoding. Decoding is contrary of encoding. It's the method to convert cipher text into plain text while not missing any words within the original text. To perform this method cryptography depends on mathematical calculations beside some substitutions and permutations with or whiles not a key. Modern cryptography gives the confidentiality, integrity, non-repudiation and authentication [1]. These days, there are variety of algorithms are on the market to encode and decode sensitive information that area unit usually divided into 3 varieties. Initial one is symmetric cryptography that is the same key is used for encoding and decoding information. Other is asymmetric cryptographic. This variety of cryptography depends on 2 completely different keys for encoding and decoding. Finally, cryptographic hash function victimization no key instead key it's mixed the information [2]. The symmetric key is rather more effective and quicker than asymmetric. a number of the common symmetric algorithms is Advance encryption standard (AES), Blowfish, Simplified data encryption standard (S-DES) and 3DES. The main purpose of this paper can offer a detail data concerning advanced encryption standard (AES) algorithm for encoding and decoding knowledge. Fig. 1 represent the migration process of mobile agent system.

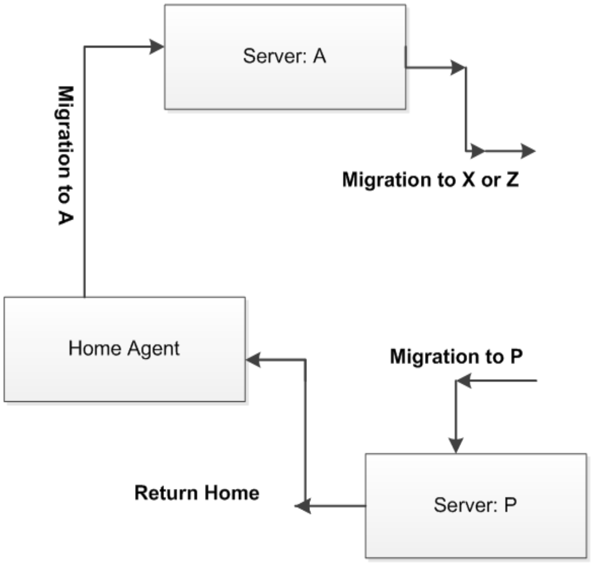


Fig. 1. Migration Process for Mobile Agent.

II. RELATED WORK

Equipment and programming usage of the AES calculation is a standout amongst the most significant territory to alluring inquires about to complete an exploration on it. As of late various research papers have been distributing on AES calculation to give significantly more unpredictability and looking at the exhibition between the famous encryption algorithms to scramble and decode information.

In Lu [16], etal proposed another engineering technique to reduce the multifaceted nature design of AES algorithm when it is executing on the equipment, for example cell phone, PDAS and smart card and so forth. This technique has comprised of coordinating the AES encoded and the AES decoded to give an ideal utilitarian AES crypto-engine. To do that they concentrated on some significant highlights of AES particularly (Inv) SubBytes and (Inv) Mixcolumn module.

An examination in [17] has directed on various mysteries key calculations to recognize which calculation can be given the best execution to scramble and unscramble information. To do that there was led on four regular calculations, for example, Blowfish, AES, DES and 3DES. In this paper to assess this calculation substance and sizes of encoding input records were changed and two distinct stages were utilized to test these calculations, for example, P-II 266 MHz and P-4 2.4 GHz. As per the outcomes Blowfish can give the best execution contrasted with different calculations and AES has a superior execution than 3DES and DES. It additionally give that 3DES 1/3 throughput of DES.

In this paper [18] assess the presentation of three algorithms, for example AES, DES, and RSA to encode content documents under three parameters like calculation time, memory use, and output bytes. Encryption time was figured to change over plaintext to figure message at that point contrasting these calculation with discover which calculation sets aside more effort to scramble content document. As per the outcomes they have gotten RSA takes additional time contrasted with different calculations. For second parameters RSA needs a bigger memory than AES and DES calculations. At long last, the yield byte of every calculation has considered. DES and AES produce a similar dimension of yield byte while RSA has a low dimension of yield byte.

III. AES ALGORITHM

AES Stands for Advanced Encryption Standard and is a united state encryption standard defined in federal information processing standard. AES is that the most up-to-date of the four current algorithms approved for federal us in the United States. AES could be symmetric cryptography algorithmic program process information in block of 128 bits. AES is symmetric since identical key is used for cryptography and also the reverse transformation, decryption [3]. The only secret necessary to stay for security is that the key. AES might organized to use totally different key-lengths, the quality defines three lengths and also the ensuing algorithms are named AES-128, AES-192 and AES-256 severally to point the length in bits of the key. The older standard, DES or data encryption standard. DES is up to 56bits only [4]. To beat the disadvantages of DES algorithmic program, the new standard is AES algorithmic program. This standard explicitly defines the allowed values for the key length (Nk), block size (Nb), and number of rounds (Nr).

A. AES Algorithm Specifications

AES is AN repetitive rather than Feistel cipher. It's supported two common techniques to cipher and decipher information known as substitution and permutation network (SPN). SPN could be a range of mathematical operations that square measure disbursed in block cipher algorithms.

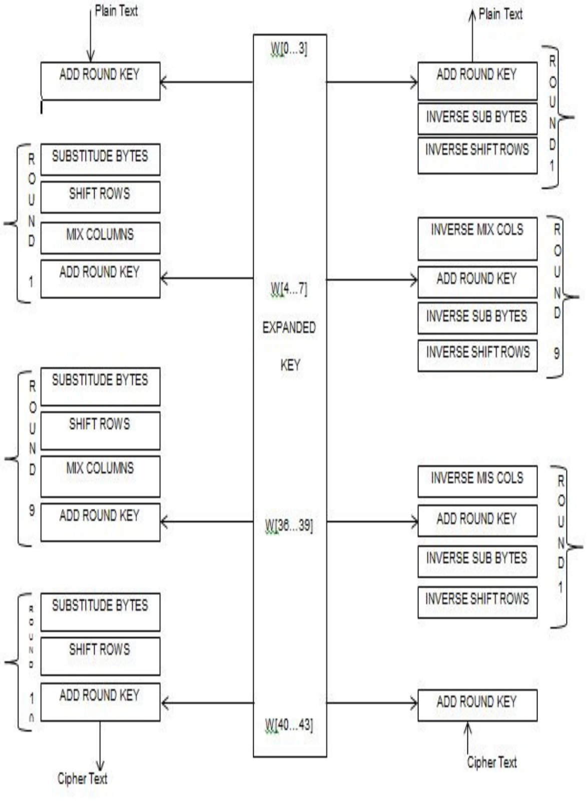


Fig. 2. General Structure of AES Algorithm.

AES has the flexibility to manage 128 bits (16 bytes) as a set plaintext block size. These sixteen bytes square measure depicted in 4x4 matrixes and AES operates on a matrix of bytes. Additionally, another crucial feature in AES is range of rounds. The number of rounds is relied on the length of key. There are 3 completely different key sizes are employed by AES rule to write and rewrite information like (128, 192 or 256 bits). The key sizes attempt to the quantity of rounds like AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Fig. 2 Represents the General Structure of AES Algorithm. An implementation of the AES algorithm shall support a minimum of one in every of the 3 key lengths: 128, 192, or 256 bits (i.e., Nk = 4, 6, or 8, respectively). Implementations might optionally support 2 or 3 key lengths, which can promote the ability of algorithmic rule implementations. For the AES algorithm, the length of the Cipher Key, K, is 128, 192 or 256 bits. The key length is pictured by Nk = 4, 6, or 8 that reflects the quantity of 32-bit words within the Cipher Key. For the AES algorithm, the quantity of rounds to be performed throughout the execution of the algorithmic rule is dependent on the key size. The number of rounds is represented by Nr, where Nr = 10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8. The only Key-Block-Round combinations that conform to this standard are given in Table 1.

Table 1: Key-Block-Round Combinations.

Bit Pattern	Key Length (NK Words)	Block Size (NB Words)	No. of Rounds (NR Words)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

B. Encryption Process

In encoding mode, the initial keys added to the input value at the terribly starting, that is termed an initial spherical. This is followed by 9 iterations of a traditional spherical and ends with a rather changed final spherical.

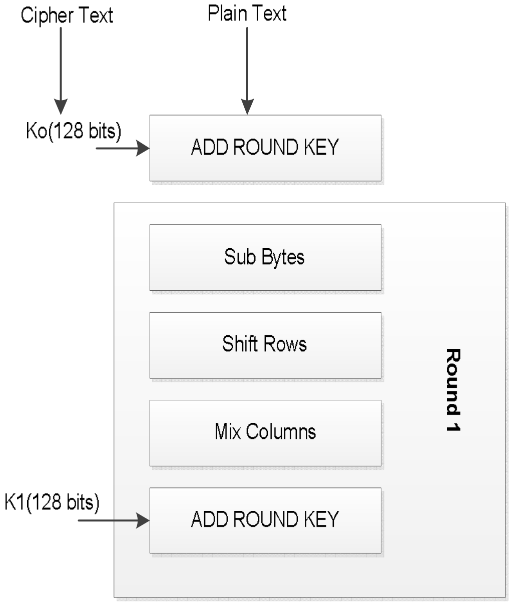


Fig. 3. General Structure of Encryption.

Throughout one traditional around the following operations are performed within the following order: Sub Bytes, Shift Rows, combine Columns, and Add round key. The ultimate spherical may be a traditional spherical while not the mix Columns stage. The first round process is depicted in Fig. 3.

Byte Substitution (SubBytes). The first stage of every spherical starts with SubBytes transformation. This stage is depends on nonlinear S-box to substitute a byte within the state to a different byte. Consistent with diffusion and confusion Shannon's principles for cryptographic algorithm design its vital roles to get far more security. for instance in AES if we've got hexa 53 within the state, it has to exchange to hexa ED. ED created from the intersection of 5 and 3. For remaining bytes of the state need to perform this operation.

Shift Rows. Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right aspect of row. Shift is dispensed as follows-

- First row isn't shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted 2 positions to the left.
- Fourth row is shifted 3 positions to the left.
- The result's a replacement matrix consisting of equivalent sixteen bytes however shifted with relevancy one another.

Mix Column Transformation. Each column of 4 bytes is currently reworked employing a special mathematical relation. This function takes as input the four bytes of 1 column and outputs four fully new bytes that replace the initial column. The result's another new matrix consisting of sixteen new bytes. It ought to be noted that this step isn't performed within the last spherical.

ADD Round Key. The sixteen bytes of the matrix are currently thought-about as 128 bits and are XORed to the 128 bits of the spherical key. If this is often the last spherical then the output is that the cipher text. Otherwise, the resulting 128 bits are understood as sixteen bytes and that we begin another similar round.

C. Decryption Process

In decryption mode, the operations are in reverse order compared to their order in encryption mode. Therefore it starts with associate degree initial spherical, followed by nine iterations of an inverse traditional spherical and ends with an AddRoundKey. An inverse traditional spherical consists of the subsequent operations during this order: AddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes. an initial spherical is an inverse traditional spherical while not the InvMixColumns. Fig. 4 represent the general structure of Decryption.

The decryption is the process to obtain the original data that was encrypted. This process is based on the key that was received from the sender of the data. The decryption processes of an AES are similar to the encryption process in the reverse order and both sender and receiver have the same key to encrypt and decrypt data.

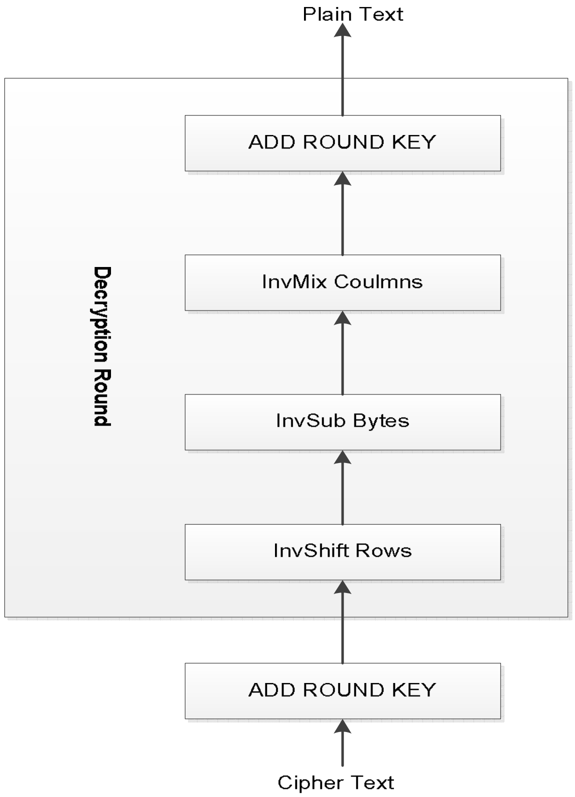


Fig. 4. General Structure of Decryption.

IV. SHAMIR'S SECRET SHARING SCHEME

Concept of secret sharing first off fictitious by Adi Shamir and George Blakley in 1979 severally. theme planned by each relies on completely different ideas. Shamir's theme relies on polynomial technique whereas Blakley's theme supported hyper plane idea. Secret sharing includes 2 main sections particularly share construction and secret reconstruction phase. Shamir's theme works as follows.

A. Share Construction

For share construction, threshold (k, n) and secret value S is needed. Then polynomial operate of an order (k-1) is constructed as shown in equation.

$$f(x) = d_0 + d_1x + d_2x^2 + \ldots + d_{k-1}\,x^{k-1}\ (modp) \qquad (1)$$

In above equation, constant term d0 is replaced with secret value S. the opposite coefficients like, d1, d2 , …, dk-1 are any random values. Secret shares are the pairs of values (xi ,yi), where yi=f(xi) for 1 ≤ i ≤ n and 0 < x1 < x2 . . <xn< n -1.

B. Secret Reconstruction

During secret reconstruction any k shares are collected. Then, secret worth is computed exploitation Lagrange's interpolation formula. Equation shows the Lagrange's interpolation formula which supplies polynomial operates.

$$f(x) = \sum_{j=1}^{k} \left(y_{ij} \Pi_{1<-t<-k, t\neq j} \frac{x - x_{it}}{x - x_{it}} \right) modp \qquad (2)$$

The constant term in equation f(x) is our original secret value. Equation (2) can be further simplified as whole equation is not needed. Simplified equation is shown in equation (3) which directly gives constant term i.e. secret value S

$$f(x) = \sum_{j=1}^{k} \left(y_{ij} \Pi_{1<-t<-k, t\neq j} \frac{x_{it}}{x - x_{it}} \right) modp \quad (3)$$

V. COMPARISON OF SECRET SHARING SCHEMES

Following Table represents the comparison of secret sharing scheme

Table: 2 Comparison table for Secret sharing scheme.

Type	Shares	Representation	Reconstruct	Advantages
Traditional SSS	n	k=n	k=n	It is terribly effective for fewer variety of participants
Threshold SSS	n	k, n	K out of n	It permits solely few shares (threshold) to reconstruct the secret
Threshold Changeable SSS	n	t, n	T=t'	It permits to alter the threshold within the absence of channel
Verifiable SSS	n	k, n	k, n	It is used as an answer to cheating issues

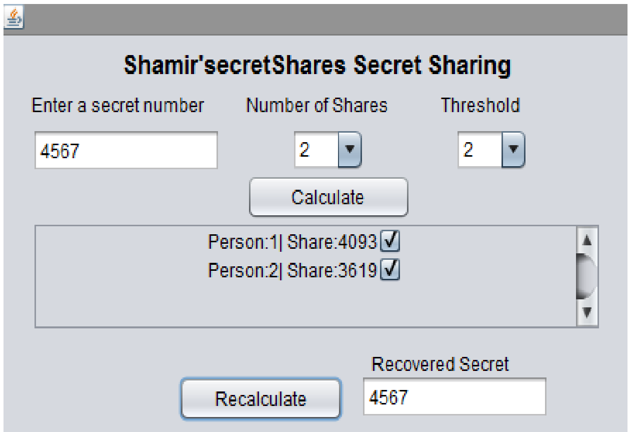
VI. IMPLEMENTATION OF SECRET SHARING

The Java execution of Shamir's plan includes two projects. The first make a Swing structure with marked Java Text Fields that will acknowledge a key, the limit estimations of n and t, and the prime number p that will characterize the modulus where the program will work. The program will at that point create a polynomial function s(x) of degree m-1 with arbitrary coefficients where the steady term is the mystery key. This should be possible utilizing the basic irregular capacity for whole numbers and putting away the coefficients into an exhibit. For BigIntegers, Java gives a constructor that will create arbitrary qualities. When the polynomial is fabricated, the m shares (x, y) will be developed by picking x=1… N and y being s(x).The program will at that point print out all m shares and the polynomial into a Java Text Area. Apparently the vendor would then be able to take the offers and disseminate them electronically or face to face. The second program will be the supplement to this one. It will start by showing Java Text Area that will acknowledge the prime number p alongside the base number of offers, t, expected to remake the message. It will at that point show m Java Text Area where every member can enter their offer.

The program will at that point play out the important counts and return the estimation of the key/mystery.

A. Program Name: SecretShare.

Description: This program creates mystery shares from an entered number dependent on Shamir's calculation. The program starts by giving the client a GUI isolated into left and right parts. On the left side is an information section board where the client can supply the mystery key (an enormous number), a prime number (q) for playing out the essential modulus arithmetic, the number of offers wanted, and the base number of offers required to reproduce the mystery. The section board likewise incorporates a catch that enables the client to peruse the key and prime number from a record. The document ought to have the key on the main line and the prime # on the second. The correct portion of the GUI holds a yield board that shows the prime number and the offers created. Underneath the yield region is a catch that gives the client a chance to compose the offers to a catalog with one offer for each document. This disentangles share dissemination on the grounds that the client can encode each record and send it to the fitting party. The prime number is additionally kept in touch with its own record so it very well may be sent to all members. Update: The encoder has been modified so that if a checkbox is empowered on the information section board, the program will produce a record that empowers offers to be assessed utilizing Feldman's technique. This document contains an enormous prime number p to such an extent that p-1 is different of q, an esteem g, and g raised to the intensity of every one of the Shamir polynomial coefficients. This last advance is utilized to shroud the coefficients utilizing the know trouble of taking care of the tactful log issue. The program has likewise been changed so the client no longer needs to enter a prime number. On the off chance that one isn't provided, the program will produce one bigger than the key and compose it to the yield region and the record. Squeezing the submit catch will make the underlying GUI be supplanted by one where the offers can be gone into a lot of content fields. The quantity of fields is dynamic and is set by the quantity of offers required to revamp the key. For comfort, every one of the offers can likewise be perused from a document by choosing the catch alongside every one. Once entered, one can press the unmistakable, restart, or discover key catches.



Shamir'secretShares Secret Sharing

Enter a secret number: 4567

Number of Shares: 2

Threshold: 2

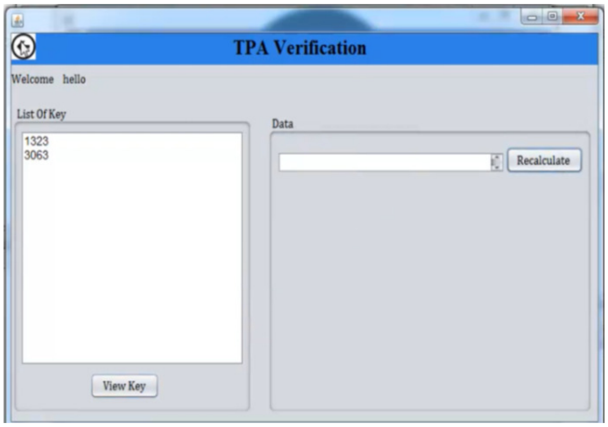
Person:1| Share:4093 ☑

Person:2| Share:3619 ☑

Recovered Secret: 4567

Fig. 5. Secret Number Sharing.

The unmistakable catch exhausts every one of the fields and the restart catch reestablishes the underlying screen with the goal that the program can be utilized for an alternate arrangement of offers. In conclusion, the discover key catch will register the mystery key dependent on the offers gave. It will dependably give a key, however on the off chance that any of the offers isn't right; at that point the key will not be right. In the event that one approved the offers, the program will check every one preceding processing they key and caution clients of any mix-ups. It will obviously show what share was mistaken so that the user(s) can make a move.



TPA Verification

Welcome hello

List Of Key

1323
3063

Data

Fig. 6. Secret Number Verification.

VII. CONCLUSION AND FUTURE WORK

This paper has focused on providing secure medium to the mobile agents during their migration process. For providing security we have used two approaches first one is Advanced Encryption Standard and second one is Shamir's Secret Sharing Methodology. Advanced encryption standard (AES) calculation is one of the productive calculation and it is generally supported and embraced on equipment and programming. This calculation empowers to manage diverse key sizes, for example, 128, 192, and 256 bits with 128 bits block cipher. In this paper, clarifies various significant highlights of AES calculation and shows some past investigates that have done on it to assess the exhibition of AES to scramble information under various parameters. As indicated by the outcomes acquired from explores demonstrates that AES can give substantially more security contrasted with different calculations like DES, 3DES and so on.

A secret sharing plan begins with a mystery and after that gets from it certain offers which are dispersed to certain clients. The secret might be recuperated just by certain foreordained gatherings which have a place with the entrance structure. secret sharing plans have showed up as a rich answer for the issue of protecting cryptographic keys however their applications incorporate now edge cryptographic conventions and some e casting a ballot or auction conventions. We have assessed the most significant mystery sharing plans for various access structures (general, limit, on the web, proactive,). Some fascinating and helpful broadened abilities have been additionally reviewed with the goal that the applications can be effectively conceivable.

ACKNOWLEDGEMENT

The authors acknowledge with thanks to the JSS Academy of Technical Education for the support and motivation in completing this study.

REFERENCES

[1]. Abdullah, A.M., & Aziz, R.H.H. (2016). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography algorithm. *International Journal of Computer Applications,* Vol. **143**, No. 4 pp. 11-17.

[2]. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, **67**(19).

[3]. Daemen, J., & Rijmen, V. (1998). The block cipher Rijndael. In *International Conference on Smart Card Research and Advanced Applications*, pp. 277-284. Springer, Berlin, Heidelberg.

[4]. Nikov, V. and Nikova, S. (2004). On Proactive Secret Sharing Schemes, SAC'04, LNCS 3357, pp. 314-331.

[5]. Kaur, Swinder and Vig, Renu (2007). Efficient Implementation of AES Algorithm in FPGA Device. *International Conference on Computational Intelligence and Multimedia Applications*, pp. 179-187.

[6]. Shivendra, Katiyar, Kullai Reddy Meka, Ferdous A. Babhuiya and Sukumar Nand (2011). Wireless sensor network System Powered By Sensor Security Using Steganography. *Proceeding of IEEE Transaction, Second International Conference on Emerging Applications of Information Technology,* pp. 288-291.

[7]. Shamir, A. (1979). How to share a secret?. *Communications of the ACM*, **22**(11), 612-613.

[8]. Wang, Z.H., Chang, C.C., Tu, H.N., & Li, M.C. (2011). Sharing a secret image in binary images with verification. *Journal of Information Hiding and Multimedia Signal Processing*, **2**(1), 78-90.

[9]. Pramstaller, N., Gurkaynak, F.K., Haene, S., Kaeslin, H., Felber, N., & Fichtner, W. (2004). Towards an AES crypto-chip resistant to differential power analysis. In Solid-State Circuits Conference, ESSCIRC 2004.

[10]. Nadeem, H. (2006). A performance comparison of data encryption algorithms. *IEEE Information and Communication Technologies,* pp. 84-89.

[11]. Hussien, H., & Aboelnaga, H. (2013). Design of a secured e-voting system. In *2013 International Conference on Computer Applications Technology (ICCAT)* pp. 1-5. IEEE.

[12]. Patil, S., & Deshmukh, P. (2014). Verifiable image secret sharing in matrix projection using watermarking. In *2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)* pp. 225-229. IEEE.

[13]. Rachh, R.R., Anami, B.S., & Mohan, P.A. (2009, January). Efficient implementations of S-box and inverse S-box for AES algorithm. In *TENCON 2009-2009 IEEE Region 10 Conference* pp. 1-6. IEEE.

[14]. Lu, C.C., & Tseng, S.Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In *Proceedings IEEE International Conference on Application-Specific Systems, Architectures, and Processors*, pp. 277-285. IEEE.

[15]. Nadeem, A., & Javed, M. Y. (2005). A performance comparison of data encryption algorithms. In *2005 international conference on information and communication technologies*, pp. 84-89. IEEE.

[16]. Berent, A. (2013). Advanced Encryption Standard by Example. Document available at URL http://www.networkdls. com/Articles.

How to cite this article: Upadhyay, U., Kumar, P. and Aggarwal, D. (2019). Secure Migration of Mobile Agent using AES & Secret Sharing Approach. *International Journal on Emerging Technologies*, **10**(2): 150-155.