SECURE HOME AUTOMATION: PROACTIVE SECRET SHARING SCHEME AND ADVANCED ENCRYPTION STANDARD

Bombay Bhavya Sree[1], **Nalla Pranitha**[2], **Shamlet Paul Raj**[3]

Department of Information Technology[1], Sreenidhi Institute of Science and Technology[1]

Department of Information Technology [2], Sreenidhi Institute of Science and Technology[2]

Department of Information Technology[3], Sreenidhi Institute of Science and Technology[3]

ABSTRACT— *the drawbacks of today's home automation system using IOT are eavesdropping, trespassing, data security. The home automation has monitoring control over remote surveillance and pivotal locking system. Therefore, this issue of data security and privacy will be addressed by using Proactive Secret Sharing Scheme. Using Proactive Secret sharing we can replace centralization with decentralization and give the players some specific powers, so that they can operate the system. This scheme is decentralized where in the power is distributed among group of players. The issue of trespassing and malicious attacks will be addressed using cryptographic algorithms-Advanced Encryption Standards.*

KEYWORDS— *Advanced Encryption Standards (AES), bi-variate polynomial, Encryption, Internet of things (IOT), Privacy, Proactive Secret sharing technique, Security, Threshold cryptography, Decryption*

1 INTRODUCTION

1.1 IOT-Internet of Things

The Internet of Things (IoT) is a concept that describes a future where every day physical objects can be connected to the Internet and also be able to identify themselves to other devices. IoT is closely identified with RFID, sensor technologies, wireless technologies. It allows objects to be sensed and controlled remotely across existing network infrastructure. Internet is a medium that connect people across the world for emailing, gaming, conferencing, online trading and so on. IoT includes, for example, Cameras connected to Internet that allow you to post pictures online with a single click, changing the lane while driving safely, switching off the lights automatically in a room when no one is around. Internet of things can be able to transfer data over the network without human interaction. [1]

1.2 IOT basic characteristics

Internet of things is a collection of physical objects which is has ability to capture information for physical world. IoT is an intelligent system, which has computing and communicating ability [6]. Internet of things has three basic characteristics such as

Comprehensive awareness: Comprehensive awareness is due to the sensors, RFID and M2M terminal. These are used to get information of the object.

Reliable transmission: The main aim of reliable transmission is high accuracy and real time.

Intelligent processing: The main aim of intelligent processing is to analyse and collect the useful information to meet the user expectation. [1]

1.3 Shamir secret sharing

In this secret sharing scheme, we show how to divide data D into n pieces in such a way that D is easily constructible from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. [4] This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

1.4 Proactive Secret Sharing

In proactive secret sharing scheme the shares distributed during the distribution phase are renewed periodically without changing the secured data and reconstructs the corrupted shares if any.

Proactive Secret sharing consists of the following four phases:

– Setup of participants
- Share Distribution
- Share Verification
- Share Reconstruction
- Share Renewal
- Share Aggregation
- Subgroup formation

The above phases will be discussed in detail in section 3

1.5 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size [3].

2 HOME AUTOMATION

A Home Automation is an automation that helps us create the facilities of a smart home by providing access and control to light setup, temperature, humidity, security and many more requirements in a remote fashion through Internet access.

2.1 Facilities of Home Automation

1) To facilitate control and access to describe and monitor the lighting, air-conditioning, ventilation, temperature and humidity through automated schedules and devices.
2) To provide the features of security for automated homes through secure door locks and gates.
3) To coordinate with the home appliances in a smart way for better living.

4) For provision of interoperability and ability to upgrade itself.
5) Commitment to provide energy savings and also cost effective.

2.2 Drawbacks of Existing Home Automation

The current home automation system has certain drawbacks such as the loss of private data, eavesdropping and so on. The possible security threats in a smart home are Distributed Denial of Service (DDoS) attacks and leakage of information, etc. Smart home networks are threatened by unauthorized access. [1]

Monitoring the system and personal information leakage: As the authority of monitoring the data and information is centralized. If the centralized authority turns out to be a malicious person then there is a threat of leakage of information.

Trespass: If the smart door lock is effected by malicious codes or it is accessed by an unauthorized party, the attacker can trespass on smart home without smashing the doorway. The result of this effect could be in the form of loss of life or property. [1]

The rectification of these issues will be addressed in Section 3.

3 OUR PROPOSAL

3.1 To rectify the issue of centralization for data security

This issue of home automation can be rectified by Proactive Secret sharing.

3.1.1 Setup of participants

A group of n participants is set up and each player is assigned a symmetric polynomial.A threshold value t is set, where only t or more shares are required to reconstruct the secret. Let $f(x, y)$ be the bivariate polynomial with x, y being the two variables symmetric about both x, y axis. Let n be the group of the players and t be the threshold scheme.The degree of the variables x,y in the bivariate polynomial is such that it is at most equal to $t - 1$. P is the group of players.

3.1.2 Share distribution

Every player receives shares of the secret. To obtain the respective partial share,For suppose P_i denotes the bivariate polynomial say $f(x,y)$ and P_j denotes another bivariate polynomial $f(x,y)$ then ,the partial share of P_i with respect to P_j is obtained by substituting the value of i as y in both the polynomials. Add both the polynomials. We thus generate a polynomial in a single variable x.Similarly the value of j is substituted as y in both the polynomials and they added to generate the partial share of P_j.

3.1.3 Share Verification

After every participant P_j (for $j \in P$) has received a partial secret s_j, the node P_j can verify its partial share s_j in the following way:

Each participant $P_j \in n$ receives commitment c^{ij} and share $f_{ij}(h(P_j), z)$ from all other shareholders $P_i \in P$. $c^i_{ad} = b^i_{ad} * P \in G$

Where b^i_{ad} is the co-efficient multiplying $x^a z^d$ in $f_i(x, z)$.$c^{ij} = \Sigma c^i_{ad} * h(P_j)^d$. Each participant P_j calculates $\Sigma b^j_d * F$, where b^j_d is a coefficient of z^din share $s_{ij} = f_i(h(P_j), z)$. Participant verifies share s_{ij} by comparing $c^{ij} = \Sigma b^j_d * F$. If all s_{ij} holds true share s_j received is correct.

3.1.4 Share Recovery and Aggregation

In Share Recovery any player $P_i \in P$ that had lost it's partial secret s_i can recover it's partial share by authenticating itself to t the group of players$\in P$. This allows the node P_i obtain its lost partial share. Following the same protocol that a new node joining the network performs as in Share Distribution phase.

3.1.5 Share Renewal

It is important for the player P_i to update the partial share s_i without disturbing the original secret s. This can be achieved in the following manner:

Every Player $P_i \in P$ chooses a new polynomial f '$_i$ (x, z) for f '$_i$ (0, 0) = 0. Now every player $P_i \in P$ secretly sends the value $f'_{ij}(h(P_j), z)$ to all others player in the group $P_j \in P$.

Every player P_i receives n values of $f'_{ji}(h(P_i), z)$ which includes $f'_{ii}(h(P_i), z)\ for\ n_i \in N$.Then every node n_i computes $f_i(z) = f'(h(P_i), z) = \Sigma_{j \in k} f'_{ji}(h(P_i), z)$ and $s'_i = f_i(h(P_i), 0) = f_i(0)$

The new secret equation of $P_i \in N$ is $f(h(P_i), z) = f''(h(P_i), z) + f'(h(P_i), z)$

The new partial secret share $s_i = s_i + s_i$ for $s_i = f_i(0)\ and\ s'_i = f_i(0)$.

Finally every player $P_i \in n$ has a new partial secret s''_i and a new secret polynomial $f_i(z)$.

3.1.6 Secret Reconstruction

Select threshold number of updated shares and apply Lagrange's interpolation. $F(x) = \Sigma\, j \in t\ \mathbf{S}'_j(x)\ \mathbf{l}_j(x)\ l_j(x) = \Pi m \in t(x - x_m)/(x_j - x_m)$ where m 6= j. Secret is reconstructed by substituting zero in the polynomial obtained $(I) = S$

3.1.7 Subgroup formation

A subgroup of players can be formed from the exixting group to reconstruct the secret. The number of players in the subgroup must be greater than or equal to the threshold value t.

3.1.8 Example

Proactive Secret Sharing (Example)

The Prerequisites required to proceed through the example. The initial group of players $P_M = P1, P2, P3, P4$

An additive group G of order 29, i.e $q = 29$

The Curve used is $y^2 = x^3 + 1$

The Generator P = (520, 3392) q=4019 F = GF (q) k1 = 233 F1 = GF (k1)

P=E (117,122)

Each Player chooses its own bivariate polynomial: P1.¡x, z¿=PolynomialRing (F1, 2, order='lex')

P2. < x, z>=PolynomialRing (F1, 2, order='lex')

P3. < x , z> =PolynomialRing (F1, 2, order='lex')

P4. < x, z>=PolynomialRing (F1, 2, order='lex')

P5. < x, z>=PolynomialRing (F1, 2, order='lex')

3.1.8.1 Initialization Phase

$P1 = 3*x^2*z + 3*z^2*x + 8*x*z + 5*z + 5*x + 5$

$P2 = 5*x^2*z + 5*x*z^2 + 3*x*z + 8*z + 8*x + 9$

$P3 = 8*x^2*z + 8*x*z^2 + 5*x*z + 3*x + 3*z + 6$

$P4 = 2*x^2*z + 2*x*z^2 + 4*x*z + 8*z + 8*x + 4$

The implicit polynomial formed by the player is:

$F(x, z) = P1 + P2 + P3 + P4 = 18x^2z + 18xz^2 + 20xz + 24x + 24z + 24$

The secret *s* of the Home Automation is F (0, 0) = 24. All the Players exchange their secret by using hash value.

The hash values are calculated using hash function:

```
import hashlib
def hfun(id,k): h = int(hashlib.sha224(str(id)).hexdigest(),16)
Val = mod (h, k) ; return Val;
```

The hash values of the players are:

h_p1 = hfun ('party1', k1) = 31

h_p2 = hfun ('party2', k1) = 82

h_p3 = hfun ('party3', k1) = 196

h_p4 = hfun('party4',k1) = 157

3.1.8.2 Share Distribution

Each Player sends the following values to the other node:

P1 sends the following values to P2, P3, P4

$P11 = P1(x, hp1) = 93x^2 + 107x + 160$

$P12 = P1(x, hp2) = 13x^2 + 96x + 182$

$P13 = P1(x, hp3) = 122x^2 + 88x + 53$

$P14 = P1(x, hp4) = 5x^2 + 182x + 91$

P2 sends the following values to P1, P3, P4

$P21 = P2(x, hp1) = 155x^2 + 13x + 24$

$P22 = P2(x, hp2) = 177x^2 + 89x + 199$

$P23 = P2(x, hp3) = 48x^2 + 218x + 179$

$P24 = P2(x, hp4) = 86x^2 + x + 100$

P3 sends the following values to P1, P2, P4

$P31 = P3(x, hp1) = 15x^2 + 157x + 99$

$P32 = P3(x, hp2) = 190x^2 + 149x + 19$

$P33 = P3(x, hp3) = 170x^2 + 52x + 128$

$P34 = P3(x, hp4) = 91x^2 + 163x + 11$

P4 sends the following values to P1, P2, P3

$P41 = P4(x, hp1) = 62x^2 + 190x + 19$

$P42 = P4(x, hp2) = 164x^2 + 37x + 194$

$P43 = P4(x, hp3) = 159x^2 + 35x + 174$

$P44 = P4(x, hp4) = 81x^2 + 72x + 95$

The corresponding share at each player

$S1 = P11 + P21 + P31 + P41 = 92 * x^2 + x + 69$ and share at $P1 = 69$

$S2 = P12+P22+P32+P42 = 78*x^2-95*x-105$

And share at $P2 = 128$

$S3 = P13 + P23 + P33 + P43 = 33 * x^2 - 73 * x + 68$ and share at $P3 = 68$

$S4 = P14 + P24 + P34 + P44 = 30 * x^2 - 48 * x + 64$ and share at $P4 = 64$

3.1.8.3 Share Verification and Share Renewal

If the four players P1, P2, P3, P4 want to renew their shares then they choose a bivariate polynomial with free term 0

The polynomials are:

$P1_1 = x^2 * z + x * z^2 + 5 * x * z + 2 * x + 2 * z$

$P2_1 = 2 * x^2 * z + 2 * x * z^2 + 20 * x * z + 4 * x + 4 * z$

$P3_1 = 3 * x^2 * z + 3 * x * z^2 + 12 * x * z + x + z$

$P4_1 = 4 * x^2 * z + 4 * x * z^2 + 8 * x * z + 3 * x + 3 * z$

After choosing the polynomials, the players again undergo share distribution, share verification as above mentioned.

3.1.8.4 Share Aggregation

The new Polynomial

$P5. < X, z >= PolynomialRing\ (F1, 2, \text{order} =^0 lex^0) = 3*x^2*z + 3*z^2*x + 8*x*z + 5*z + 5*x + 5$

Again the P5 requests to all the players P1,P2,P3,P4 to share the secret and the above share distribution and share verification process is repeated.

3.1.8.5 Subgroup formation

If the players have to take up an event or has to undergo an event and if all the parties doesn't want to form a group. Then the interested or the minimum required players to acquire secret will form a subgroup and executes the event.

The polynomial is $P = P1 + P2 + P3$

The Players P1, P2, P3 will share their shares among them. And then the players will find their equivalent share. $SR1 = SP1_1 + SP2_1 + SP3_1$ $SR2 = SP1_2 + SP2_2 + SP3_2$ and $SR3 = SP1_3 + SP2_3 + SP3_3$

Then the subgroup key is recorded.

3.2 To rectify the issue of trespassing and malicious attacks

The issue of trespassing and malicious attacks will be addressed using cryptographic algorithm - Advanced Encryption Standard (AES)

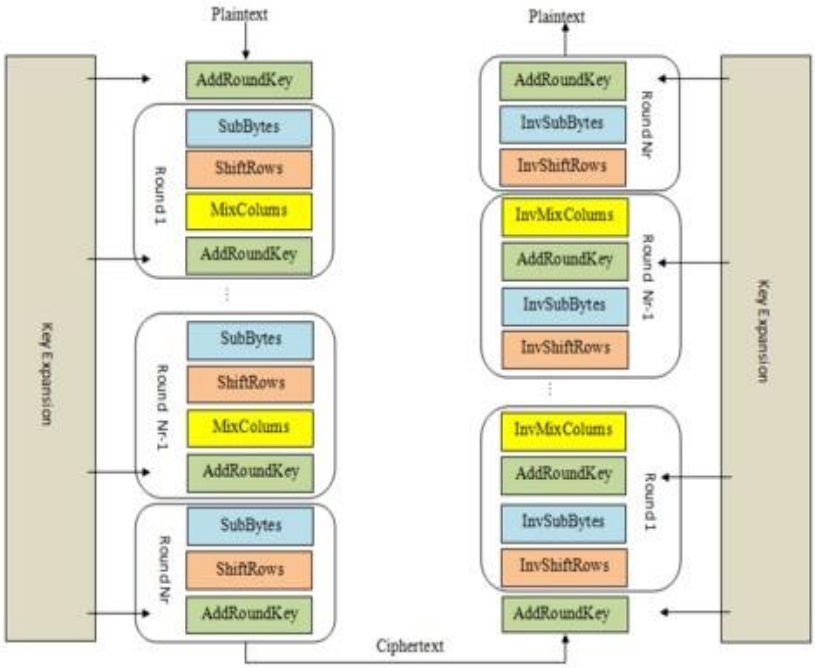
3.2.1 Framework of AES Algorithm

The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption as well as for decryption. The length of data blocks is fixed to be 128 bits, while the length can be 128, 192, or
256 bits. [10]

The AES algorithm, a symmetric block cipher can encrypt as well as decrypt the data. Encryption translates data to a secret form called cipher-text. Encryption of the cipher text then converts the data back into its original form, which is known as plain-text as is also reversible as most of the encryption algorithms. This helps us to understand that almost the same steps with some simple changes are performed to complete both encryption and decryption in reverse order. [10]

3.2.2 Process of Encryption and Decryption -AES

Fig. 1. Process of Encryption and Decryption-AES [10]



3.2.2.1 Steps for Encryption

1). The Sub Bytes is the first step of the AES Encryption process. This stage is depends on nonlinear S-box to substitute a byte in the state to another byte. According to diffusion and confusion Shannon's principles for cryptographic algorithm design it has important roles to obtain much more security. [3]

2). The Shift Row transformation comprises of four basic steps as mentioned below: i). keeping the first row of the state array unchanged ii)Shifting the second row circularly by one byte to the left (iii) Shifting the third row circularly by two bytes to the left iv). Shifting the last row circularly by three bytes to the left. The input block is written column-wise not row-wise. [10]

4)**.** The Mix Column transformation replaces each byte of a column by a function of all the bytes in the same column. More precisely, each byte in a column is replaced by two times that byte, plus three times the next byte, plus the byte that comes next, plus the byte that follows. [10]

5). AddRoundKey is the most vital stage in AES algorithm. Both the key and the input data (also referred to as the state) are structured in a 4x4 matrix of bytes.AddRoundKey has the ability to provide much more security during encrypting data. This operation is based on creating the relationship between the key and the cipher text. The cipher text is coming from the previous stage. The AddRoundKey output exactly relies on the key that is indicated by users. Furthermore, in the stage the subkey is also used and combined with state. The main key is used to derive the subkey in each round by using Rijndael's key schedule. The size of subkey and state is the same. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR. [3]

Fig. 2. S-Box for AES [10]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 3. ShiftRows Transformation [10]

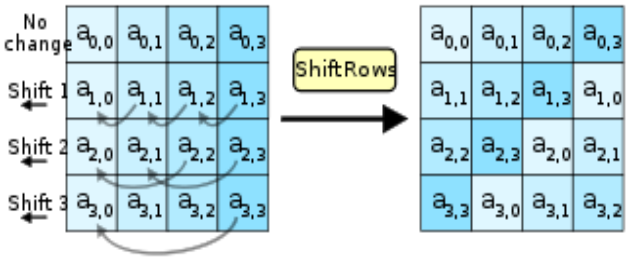
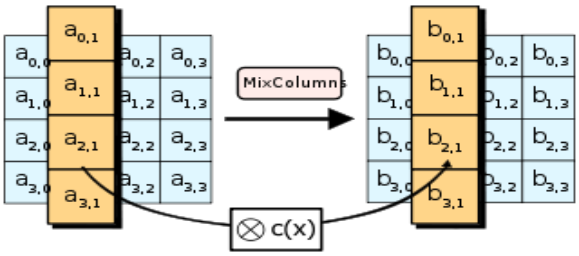


Fig. 4. Mix Column Transformation [10]



3.2.2.2 Steps for Decryption

1). Inverse Shift Rows

2). Inverse Sub Bytes

3). Add Round Key

4). Inverse Mix Columns

3.2.3 Example

Consider we have to secure the password which will lock and unlock the security gates of a smart home.

Let us consider the password to unlock the gates of a smart home is “AUTOMATION.” As the need to protect it from being prone to vulnerability. Hence we address this issue by encrypting and decrypting the password using AES Algorithm. The components required for the AES algorithm are secret key and password.

Initially we convert the secret key in character format to binary format. Key = bin.encoding (”SN”). The converted binary format of the key is : 0101001101001110

Next we have to convert the password to binary format P = bin.encoding (”AUTOMATION”). The converted binary format of the password is:

0100000101010101010101000100111101001101010000 0010101010001001001010011110100111 0

Now by using the encryption algorithm we pass the secret key and password as parameters to encrypt the password. C = maes(P, key, algorithm =”encrypt”)

The encrypted binary format of the password is

1110101111000110011001001000000001001001101000 1010100010010000011011111010100101 1

Now by using decryption algorithm and passing the encrypted password and secret key as parameters we decrypt the password.

Decryptedvalue = Maes (C, key, algorithm=”decrypt”)

Thedecryptedbinary format of thepassword is:

0100000101010101010101000100111101001101010000010101010001001001010011110100111 0

Next we will have to convert the decrypted binary format of the password to character format.

fromsage.crypto.utilimportbin$_t$o$_a$scii

Plaintext = bin$_t$o$_a$scii (decrypted$_v$alue)

The password obtained is: AUTOMATION

4 SECURITY ANALYSIS

4.1 Security analysis of Proactive Secret of Sharing

In this section, we discuss the security and correctness of our scheme. We assume that at any time in the lifetime of the Automation, the number of corrupted nodes is at-most t-1 and maximum value of t=n/21as we are using a (t, n) threshold secret sharing scheme.

Theorem 1: The secret s is always secure even if the are at-most t-1 corrupted nodes.

Proof: To construct the secret s, at-least t nodes have to co-operate. Since we employed a (t, n) threshold scheme, where in at-least t partial shares of nodes are required to reconstruct the secret using Lagrange interpolation. If t1 corrupted nodes try to reconstruct the secret, they can not generate the original polynomial because at least t points are required to generate actual polynomial.

Theorem 2: If a corrupted node has access to a partial share of one other node of the Home Automation, the corrupted node can only take advantage of the other nodes partial share only till the next renewal. After the share renewal phase the old shares become invalid.

Proof: In the share renewal phase every node chooses a new random symmetric bi-variate polynomial with constant zero, and adds this polynomial to the old polynomial thus creating a completely new polynomial from the existing one. If the initial polynomial of node n_i is f_i then in share renewal phase it chooses a new random bi-variate polynomial $f_i^{'}$ with $f_i^{'}(0,0) = 0$. The nal polynomial formed is $f_i^{''} = f_i + f_i^{'}$.The Automation lifetime is divided into different time periods and at the end of each of it, the nodes will renew their shares. Since the corrupted node has to get t shares with in the given time period, it can not take advantage of the share of just one other node. Once the nodes renew their shares then old shares are obsolete for the corrupted node [2]

4.2 Security analysis of AES

This section talks about the security and correctness of of AES.

The AES algorithm is often prone to Brute-force attack, Bicliques attack and also differential and linear attacks. [13] [12].AES is also exposed to attacks at various levels of adapting to the round key .But this issued has been addressed and the AES algorithm is made resistant to it. [14]

5 CONCLUSION

In this paper, we have addressed certain issues that occur in Home Automation. Cryptographic techniques are useful to protect the data in any of the above mentioned issue or attacks.Using AES and proactive secret sharing,we tried to secure the data by dividing the power among the users (n players) and let the secret key to be reconstructed collectively without it being susceptible to any outsider or attacker. In other words, power is not centralized but distributed to make sure that the secret key is protected even if one the players is corrupted. Proactive secret sharing complemented to Advanced Encryption Technique will pave a way to reduce the attacks and data loss in Home automation.

REFERENCES

[1] Security issues in the Internet of Things (IoT) : A Comprehensive Study - Mirza Abdur Razzaq,Sajid Habib Gill,Muhammad Ali Qureshi,Saleem Ullah-International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[2] Proactive Secret Sharing For Long Lived MANETs Using Elliptic Curve Cryptography N Chaitanya Kumar, Abdul Basit, Priyadarshi Singh, V. Ch. Venkaiah,DOI: 10.1109/ICICI.2017.8365362 Conference: International Conference on Inventive Computing and Informatics 2017, At coimbatore, chennai

[3] Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data- Ako Muhamad Abdullah-IEEE Paper, 2017 [4] A. Shamir, How to share a secret, Communications of the ACM 22 (1979) 612613.

[5] A Survey on the Internet of Things Security -KaiZhao,LinaGe-IEEE paper,2013

[6] Internet of Things and Security Issues -Suchitra.C, Vandana C.PIJCSMC, Vol. 5, Issue. 1,January 2016

[7] IoT System Security Issues and Solution Approaches-Shinsuke Tanaka,Kenzaburo Fujishima,Nodoka Mimura, Dr. Eng.,Tetsuya Ohashi,Mayuko Tanaka,Hitachi Review Vol. 65 (2016), No. 8

[8] IoT Vulnerability Analysis and Its Security Controls K.Nakao, K.Yoshioka, D.Inoue, ASM Science Journal, Special Issue 2017(1) ICT-Bio.

[9] A research Paper on Cryptography Encryption and Compression Techniques-Sarita Kumari,International Journal Of Engineering And
Computer Science ISSN: 2319-7242, Volume 6 Issue 4 April 2017, Page No. 20915-20919

[10] Design and Simulation of AES Algorithm for CryptographyRadhika D.Bajaj1,Dr. U.M. Gokhale-M.Tech VLSI1,ISSN 2321 33612016 IJESC

[11] AES Algorithm Based Secure Data Transmission for Wireless Sensor Networks-Dr. R. Prema-International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) pp 3670-3674-Research India Publications.

[12] AES: Current Security and Efficiency Analysis of its Alternatives Herman Isa, Iskandar Bahari, Hasibah Sufian, Muhammad Reza Zaba Cryptography Lab, Advanced Analysis and Modeling (ADAM) -2011 7th International Conference on Information Assurance and Security (IAS) 2011 7th International Conference on Information Assurance and Security (IAS)

[13] Study of Attacks in MANET,Attacks on AES ,Cryptographically Generated Addresses(CGAs) Methods and Possible Alleviation in IPv6 over MANET Area-International Journal of Computer Applications (0975 8887) Volume 96 No.1, June 2014

[14] Low Data Complexity Attacks on AES-Charles Bouillaguet, Patrick Derbez, Orr Dunkelman,Nathan Keller, Vincent Rijmen, and

Pierre-Alain Fouque-IEEE Transactions on Information Theory (Volume: 58, Issue: 11, Nov. 2012)

[15] Internet of Things: Features, Challenges, and VulnerabilitiesEbraheim Alsaadi,Abdallah Tubaishat- International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol. 4, No. 1, 2015, Page: 1-13, ISSN: 2296-1739.