Privacy Preserving Framework For Smart Home Using Attribute-Based Encryption

Ekeji, P.U. [#1], Bennett, E.O.[*2], Sako, D. J. S. [#3]

Department of Computer Science, Rivers State University
Port Harcourt, Nigeria

ABSTRACT

In computing sense, home security is becoming necessary nowadays as the possibilities of intrusion is increasing day by day. Safety from theft, leaking of raw gas and fire are the necessary requirements for home security systems. The primary focus of this paper is to provide security and access control to smart home using an attribute-based encryption system. Attribute-Based Encryption is a type of public key cryptosystem in which the secret key of a user and the ciphertext are associated with the attributes. The ciphertext is associated with some set of user attributes, such that the decryption of ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. The system was implemented using Hypertext preprocessor (PHP) along with MYSQL as database. Results show that the system was able to control access to smart home environment with the ability of detecting, preventing intruders from gaining access to smart home system.

Keywords — *Ciphertext, Security, Attribute Based Encryption, Smart Home.*

I. INTRODUCTION

Since the origin of man, the home had been a reliable place of rest after all human activities of the day. A home is termed to be a conducive environment for human living, and it could be in different forms like bricks, thatch, hut etc., and they are also in different designs like duplex, bungalow, flats, rooms etc. that possess a kind of security that keep it safe from intruders [1].

When a home is controlled with smart devices it will be called a smart home. According to one of the most recent definition provided in [2], a home which is smart enough to assist the inhabitants to live independently and comfortably with the help of technology is termed as smart home [3]. In a smart home, all the mechanical and digital devices are interconnected to form a network, which can communicate with each other and with the user to create an interactive space. [4] Defined the smart home as an application that is able to automatize or assist the users through different forms such as ambient intelligence, remote home control or home automation systems. The home security had been an issue ever the spread of human covetous act, and this has led human race into danger and loss of properties and life. In Attribute-Based Encryption (ABE), attributes are having importance as they determine public key for encrypting data and can be used as an access policy to control users' access. There are two types of access policy; key- policy and ciphertext-policy. The key-policy is the access structure on the user's private key, and the ciphertext-policy is the access structure on the ciphertext. [5] Proposed an attribute-based encryption (ABE) scheme and this was the first attempt at proposing the concept of the attribute-based encryption scheme. In this scheme, user's identity is used as attributes, and a set of attributes are used to encrypt and decrypt data.

Despite the benefits of a smart home and security put in place in smart homes, there is still an invading report which results in loss of properties and loss of lives. This could be due to the following:

1. Compromising or poor security system through the process of hacking.
2. Faulty sensors and wireless networks used in intrusion detection system which causes some security challenges.
3. Malfunctioning of smart home mechanism

It has become very critical to deploy optimized security-based intrusion detection systems in smart homes using privacy preserving framework together with encryption applications. The provision of effective and sustainable intrusion detection system in smart homes using attribute-based encryption technique will mitigate security challenges in smart homes

II. LITERATURE REVIEW

Many literature, techniques and methods have been written and adopted to protect smart homes from intruders:

A. Enhancing Security in IOT using Rivest Shamir Adleman (RSA) model: is mostly used for file and message encrypting with two encrypting capacities. The encryption function is the base of the security while the key generation is to reveal the private key but if the private key is known it will be needless to encrypt user input. [6]

B. Smart digital door lock system for home automation model: is a technology that uses digital information such as a secret code, semi-conductors, smart card, and finger prints as the method for authentication but it does not work alone except a ZigBee module is embedded in it. [7]

C. Password encryption using Data Encryption Standard (DES) model: is an algorithm that was formerly considered to be one of the most popular method for private key encryption. DES encryption algorithm encrypts passwords before it can be stored in the database or file. [8]

III. SYSTEM DESIGN

The behavioral and structural details of the system and its components are provided in Figure 3.1. The system architecture has four components; they are the smart home, the input source, the cloud and the Attribute-Based Encryption. The ABE is responsible for the security of the system, the smart home is the living environment, and the cloud is the source for network connection between the home and the input source.

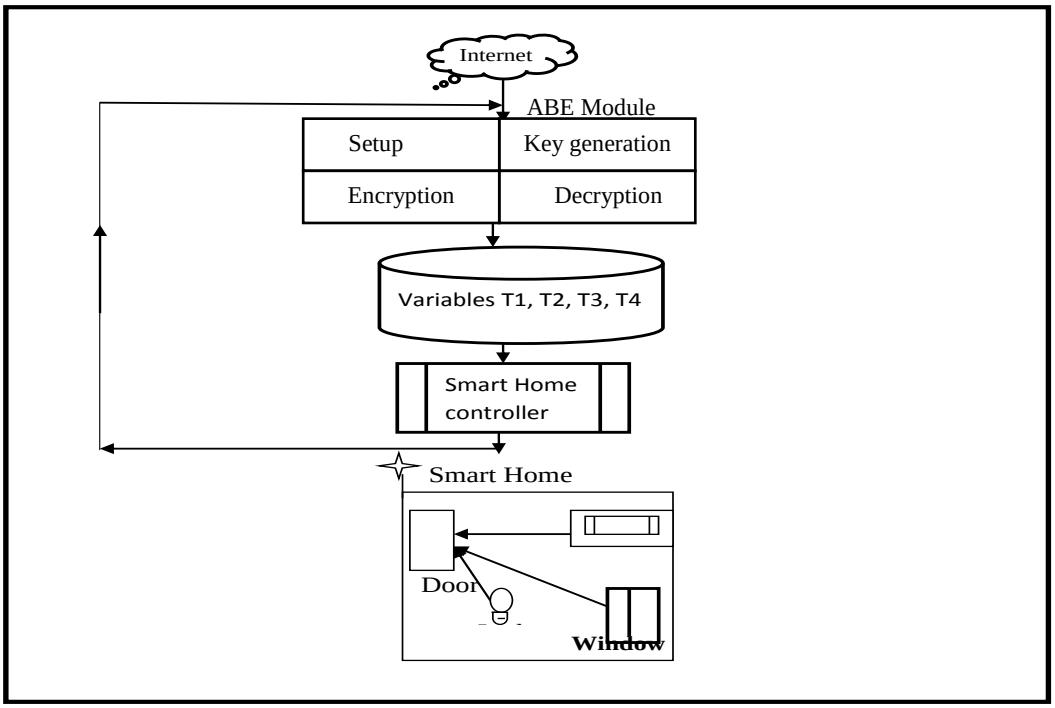

Fig 1: System Architecture

How the System Is Trained

The intrusion system is based on the Attribute based Technique that is used to predict intrusion in the smart home. The key default input parameter specifications used is tabulated in Table 3.1. These show the IP address, subnet mark, browser Type and IP address location with variable names from T1, T2, T3 and T4 for identification. The input parameter is trained to only recognize a particular variable. When any user tries to access the smart home, the system checks if the user's details are in link with the trained variable before it can grant access, else it sees it as an intrusion.

A. Input Parameters

Inputs are resources needed for executing the process as shown in Table 3.1. The networking environment is connected to the internet, and each driver has a unique id IP address to be trained and the subnet mark to the smart home**.**

TABLE I
Input Parameters

Serial number	Operative rule	Variable
1	IP Address Class type	T1
2	Subnet mark	T2
3	Browser Type	T3
4	IP Address location	T4

.This is where the users will check their access after proper registration by the home owner services. They will login using their username and password, the system always retrieve the IP address, country and city of any intruder and send to the system admin while working online but if it is working offline it will retrieve the local IP which is::1, so if their verification is successful they will have access to their various pages and if they are not registered they will be detected as an intruder.

TABLE 2
Input Criteria

Criteria	Rating (%)	Access
Unlocking a keycard lock	30	YES
Through unsecured Wi-Fi network	10%	YES
Sending phishing emails or messages	20%	YES
Access through Attribute Based Encryption	0%	NO
Penetration via vulnerable passwords	40%	YES

B. Description of ABE Process

ABE schemes usually consist of four fundamental processes. In basic ABE schemes, the user's secret key and the ciphertext are labeled with a set of descriptive attributes. A particular key can decrypt a particular ciphertext only if there are at least a specific number of attributes overlapped between the attributes of the ciphertext and the user's key. The decryption condition in a KP-ABE or CP-ABE schemes is that the attributes set satisfies the access structure specified in the secret key or ciphertext. The four algorithms are Setup, Encryption, Decryption, Key generation and it has a sender, an authority and some receivers as participants.

Setup: (K, U) -> (PP, MSK)

This algorithm takes as input a security parameter K and returns a public key PP and system master secret key MSK. PP is used by message senders for encryption. MSK is used to generate user secret key and is only known to the authority. Given a security parameter k, this algorithm calls the Setup algorithm of SM9 scheme and it sets the ABE scheme's master public key Mpk and the master secret key Msk.

(Mpk,Msk) → SM9. **Setup(1^k) …**……(1)

Key Generation: KeyGen (M_{pk}, M_{sk}, U) -> SK The authority executes this algorithm for the purpose of generating a secret key SK. The algorithm takes as inputs the public parameter PP, the master secret key MSK, set of attributes S and outputs a decryption key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Given the master public keyM_{pk}, the master secret key M_{sk}, and a set of attributes U, this algorithm converts the set of attributes U into an identity ID_U € $\{0,1\}^{|u|}$ by running the algorithm α', and then calls the Private-Key-Extract algorithm of SM9. It outputs the ABE's private key SK_U.

SK_U←SM9 .**Private-Key –Extract (** M_{pk}, M_{sk}, α'(U, u) ……..…(2)

Encryption: (M_{pk}, A_1, M_{sk}) -> CT this algorithm is performed by a sender who wants to encrypt a message M, with the public parameter PP, a set of attributes S, an access structure T. This algorithm outputs the ciphertext CT.

Given the master public key M_{pk}, an access structure A, and a message M, this algorithm converts the access structure A = {A_1, A2, An} into a set of identities by running the algorithm {, and then gets a set of ciphertexts C = {CT_1, CT_2, ……, CT_n}

C ← **Encrypt** (Mpk, £ (M_{pk}, A1, M_{sk}) -> CT ……... (3)

Decryption: (K, PP, SK, CT)->M This algorithm takes as the input the ciphertext CT and secret key SK for an attribute set. Returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

Given the master public key M_{pk}, a set of attributes U, the private key SK_U, and the set of ciphertexts C, this algorithm converts the set of attributes U into an identity ID_U { 0, 1 }^{u} by running the algorithm ' and then gets the plaintext M by running the encrypt algorithm.

M ←**ecrypt (**M_{pk},(U, u), SK_U,C)……..……..(4)

Encryption: We consider standard expansion.

N = **(**M_{pk},(U, u), SK_U,C) + (Mpk, £(A, u), M) + **(** M_{pk}, M_{sk}, α'(U, u) ……..(5)

TABLE 3
Notations used

S/N	Notation	Meaning	Description
1	K	Key	Key means secret code
2	PP	Public key	It is the user first input variables
3	M_{pk},	Master secret key	Master key is the key to access the final
4	S	Set of attributes	This represents the user attributes
5	SK	Secret key	These are the keys sent to the user
6	CT	Cypherte xt	Means the encrypted text
7	U	User	Admin

C. Algorithm: Attribute Based Encryption

1 Start
2 //Initialize IP address, Subnet mat,browser, location; 3 IF IP address € Subnet mat, browser € location
4 output ⊥ and terminate
5 else
6 t ← e(location)
7 If DEM is Stream cipher based on KDF
8 klen ← location + v
9 else
10 m ← e(IP address)
11 else If DEM is Block cipher combined with KDF
12 IP address ← Subnet mat + v
13 If Ip address is full zero
14 output ⊥ and terminate
15 else
16 output ⊥ and terminate
17 Block
18 Alert
19 End

D. Experimental Specification

This system will only grant a user access after every ciphertext is associated with a set of descriptive attributes and the user's secret key is issued by trusted authority which captures access structure also known as policy because it follows a routine process. This specifies which type of ciphertext the key can decrypt, i.e. a user is able to decrypt a ciphertext only if the set of attributes associated with the ciphertext satisfies the access policy associated with the user's private key. But if there is an intrusion attempt, the system will extract the intrusion date/time, IP Address, username, password, and the intrusion frequency. This will be saved at the intrusion page.

TABLE 4
Output Specification

System status	Conditions	Intrusion Levels
Minor intrusion attempt/No Access	valid username & invalid password	3
Intrusion detected/No Access	Invalid Password & Invalid username	2
Major Intrusion attempt/No Access (Access can be granted by administrator)	Valid username, valid password & Invalid attribute	1

IV. RESULTS AND DISCUSSION

The table 4. Shows the relationship between bit length and number of attempted intrusions.

TABLE 5
Bit Length Effect of Key on Security

S/N	Bit	Number of Attempt
1	0010	8
2	00000100	4
3	0000000000001000	2

As the bit length increases, more attempts are required which takes a lot of time recovering the key, and this leads to a decrease in the number of attempts. This means that security keeps on increasing as the key size increases but complexity of the system is also increased. So, there is a need to maintain tradeoff between key length and complexity of the system.

TABLE 5
Result presenting Intrusion outcome

Date (2019)	Time(Hrs.)	Ip Address	Username	Password	System IntrusionFrequency
Feb 14th, 2020	02:14	192.168.23.32	dogglegging@yahoo.com	Dog	1
Feb 19th, 2020	05:18	192.168.23.26	donpca@gmail.com	Don	1
April 10th, 2020	16:31	192.0.0.2	freedomfighter@hotmail.com	Freedom	2
May 14th, 2020	23:24	192.168.0.0	goldenbet@hotmail.com	Gold	2
May 23rd, 2020	12:16	192.168.23.27	janemany@yahoo.com	Jane	1
Nov 3rd, 2020	01:18	192.168.2.12	trybetv@yahoo.com	Try	2
Nov 4th, 2020	12:19	192.168.23.30	junior@come.com	Junior	1
Nov 14th, 2020	16:55	192.168.23.29	sampleinhope@yahoo.com	Sample	1
					12

A. Evaluation

Decryption Computation Time: The Encryption and Decryption computation time is the time taken by the algorithms to produce the plain text from the cipher text. The decryption time can be used to calculate the decryption throughput of the algorithms. Table 4.3 shows the decryption time of two previous algorithms against our approach.

TABLE 5

Encryption and Decryption Time Table for Different File Sizes

Input length in bits (2^n)	Encryption / Decryption execution time (S)		
	Rivest Shamir Adleman	Attribute-Based	Data Encryption Standard
2^2	3	1	4
2^3	6	3	8
2^4	9	5	12
2^5	12	7	16

For bit length of 22 character in bits in size the decryption execution time for Rivest Shamir Adleman (RSA), Data Encryption Standard (DES) and proposed algorithm are 3, 1 and 4sec respectively. This implies that our proposed algorithm consumes less time for all sizes of bit lengths.

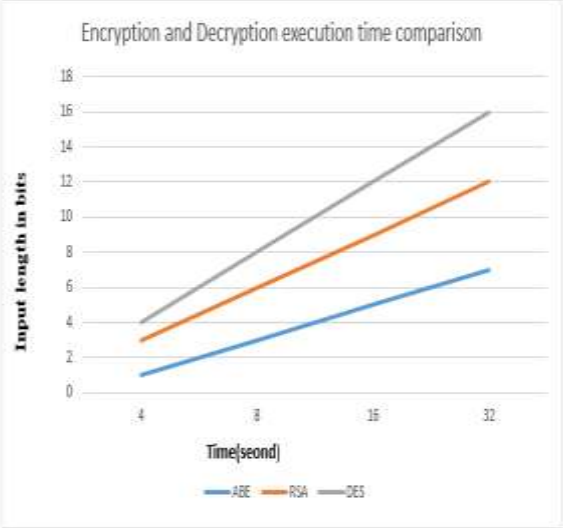

Fig 2: Comparing Encryption and Decryption Time between ABE, RSA and DES

The graph was generated from the Table 4.3, and shows the relationship between the number bits (bit length) and the runtime of our algorithms as compared with two previous approaches.

V. CONCLUSIONS

This research was centered on optimizing security of smart home intrusion detection systems using Attribute-Based Encryption. Username, password and user attributes are the primary and

secondary system security parameters used to checking for an intrusion by encrypting the user attribute. In other words, the proposed system is trained to extract the IP address, username, password, country and city of any intruder and store as indicating the sign of intruder. It does this after comparing the username and password to the real stored variables in the historical database prior to system access. With this aim in mind the system controls access of incoming details to check if they are real members of the smart home. This approach has been proven to be capable of avoiding security gaps and optimizes user's confidentiality by providing an extra level of protection.

ACKNOWLEDGMENT

My sincere gratitude goes to Dr. E.O. Bennett, My extend administrator whose direction, help, words of support and productive proposal has driven to the completion of this investigate work. I stay thankful to my father Mr. Collins Eke for his valuable commitments and proposal.

My significant appreciation goes to my lecturers: Dr. N.D. Nwiabu, Dr. Daniel and my Head of Department (HOD) Rd. I. E Anireh. For their words of support, helpful feedback, direction and motivation amid the course of ponder.

I am utilizing this medium to appreciate Mrs. Duke Daba, for her budgetary support.

Finally, to GOD All-powerful be the wonderfulness and honor for being my asylum and defender all through the period of this study.

REFERENCES

[1] Satpathy, L. Smart Housing (2009):*Technology to Aid Aging in Place*. New Opportunities and Challenges. Master's Thesis, Mississippi State University, Starkville, MS, USA, 2006. 9. Cook, D.J.; Das, S.K. *How smart are our environments*? An updated look at the state of the art. Pervasive Mob. Comput. *2007, 3, 53–73.* [CrossRef].

[2] Alam and Ali (2012) "A living laboratory for the design and evaluation of ubiquitous computing.vol 33, pp. -55.

[3] Rtylin , I., Barnett, K., Miller, E., Bailey, C. (2005). *Smart housing and social sustainability*: Learning from the residents of Queensland's Research House. Australian Journal of Emerging Technologies and Society; *3 (1): 43–57.*

[4] Ozkan, ND, Berardi, U, GhaffarianHoseini, A, Makaremi, N. (2013). *The essence of future smart houses*: From embedding ICT to adapting to sustainability principles. Renewable and Sustainable Energy Reviews; 24: 593– 607.

[5] Sahai and Waters (2005)Interfaces," in Extended Abstracts of the 2005 Conference on *Human Factors in Computing Systems, 2005, pp. 1941 - 1944.*

[6] Md. ShoaibAktherKiron,Le, Greichen, (2018)"*Value based home automation or today's market*," IEEE Transactions on Consumer Electronics, *vol. 38, no. 3, pp.34-38, Aug. 1992.* Article (CrossRef Link)

[7] G. Ho, D. Leung, P. Mishra,Sahai, Atkin B.(2016)Intelligent Buildings*: "Applications of It and Building Automation to High T echnology Construction Projects",* John Wiley & Son, New York. European Parliament. Directive *2010/31/EU* of the European Parliament and of the Council of 19 May 2010 on the Energy Performance of Buildings; Directive 2010/31/EU; The European Parliament and the Council of the European Uninion: Brussels, Belgium, *2010.*

[8] Aditi Dixit and Anjali Naik (2014) "*work on the use of Prediction Algorithms in Smart Homes*". IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 39, pp.240 – 245, Mar. 2009

[9] Sahar F. Sabbeh *"Privacy Preservation in the cloud: current solutions and open issues"*. International Journal of Computer Trends and Technology (IJCTT) V51(1):10-24, September 2017