Security in Smart Houses

Popa Dan, Talas Andrei Florin

Politehnica University of Bucharest

dan.oct.popa@gmail.com, andreitalas@gmail.com

***ABSTRACT* – A smart home or a smart house is a building that has automated and highly advanced systems in order to monitor and control every existent function within it. Controlling temperature, lightning, air quality, multi-media, windows and doors operations, security or any other necessary tasks in order to perform comfort to the resident. With the rise of wireless computerization, remote-controlled devices are becoming smart just-in-time. Because of that, data existent in the context of a smart house could be vulnerable and the system should protect it.**

In this context, elasticity is understood as the property of a system to automatically provide resources when are needed, because of workload changes. For these there is a need of protection and security against unauthorized access.

Cryptography has always been an indispensable tool for computer security and data security, so it has been used everywhere.

For this we propose a mechanism which assure security for data stored within the smart house. Security is provided with multiple level encryption and hash values on files to provide extra security and tools for integrity verification.

***KEYWORDS* –smart house, elasticity, cryptography, storage**

I. INTRODUCTION

Although there is a low level of consensus on what the term Smart House should represent, we see its implementation being similar to a living organism. We have sensors that represent the sensory receptors of the body, actuators that represent the muscles, controllers that represent the brain.

Home automation systems are mainly used for increasing the comfort of the smart house inhabitants or to assess and help the seniors or cognitive/physical-ill residents. Building systems for elderly or disabled residents should be a priority taken into consideration the rapid growing numbers of elders (over 60) in comparison with the percentage of young and adult population. In 2000 the elders' percentage of the world population was around 10%, by 2050 it's expected to reach over 20% [1]. A study made in US by the Alzheimer's Association showed that one in nine elders of age 65 or older has Alzheimer's disease (11%) [2].

The concept of Smart House should refer to the system that is capable to:

- identify the environmental context: weather, weather prognosis, location, current time
- understand the current context factors: current weather and its implications on the residents well-being, the geographical position and the normal environment values for it
- recognize the human factor: understand the identity of the person and locate it indoor.
- identify human activities and behaviors
- understand the current activity and the behavior of the person and assess the implication of that activity.

Elasticity is a term that has originally been defined in physics as a property of a material to return to its original state after a deformation. In economics elasticity describe the sensitivity of a variable to changes in one or more variables [3].

Elasticity in a system is represented by the degree to which a system is able to adapt, at workload changes by allocating and deallocating resources. The allocation and deallocation of resources is made in an autonomic manner in order to match the demand of the point as close as possible in a short time [3].

Cryptography is a transformation technique used to transform the data in order to provide various security and services such as confidentiality, data integrity, authentication, authorization and non-repudiation [5].

Cryptography is formed by two basic components: an algorithm and a key. The algorithm is the way that data transform and the key is a factor used for data transformation. The algorithms provide security and protection to the data by using encryption to transform the original data in encrypted data and the reverse by decryption to transform the encrypted data back to the original data [5].

The cryptographic algorithms can be symmetric algorithms or asymmetric algorithms. Symmetric algorithms use a single secret key for both encryption and decryption. Some symmetric algorithms are: DES, 3DES, AES. Asymmetric algorithms or public key algorithms use a known key, called public key and a secret key, called private key. The keys are related to each other. Some examples of asymmetric algorithms are: RSA, DH (Diffie-Hellman keys), SSH, SSL [7].

We propose a system that uses multiple encryption to encrypt files and assure security. It is widely believed that multiple encryption provides better security. This is believed because even if we make assumptions of some components, or ciphers are broken or keys are compromised, the security and

confidentiality can still be maintained by the remaining levels of encryptions made [14].

We made this choice in order to assure long term security for files. We chose 2 levels for encryption, first with DES [4] and second with RSA [5]. And to assure data integrity we made hash value of plaint text and cipher text too because this way the point where data is decrypted is able to know if information has been altered. The hash value is calculated with SHA-384 algorithm [13], a truncated version of SHA-512.

II. RELATED WORK

Nowadays there are many applications in smart house environments which work with personal files and data. We want to make this work to be safe and to give assurance to user that his files are protected.

A. Smart house

Home automation algorithms have to be deployed into more than one smart home implementation and they have to be modeless and adapt to the system they are deployed to; because of this the majority of algorithms used in home automation emphasizes the use of artificial intelligence algorithms.

Home automation is supported by various types of algorithms:

- Activity Recognition – or pattern recognition, used for identifying human activities and the human responsible for a specific activity. The collected information can be used to create usability patters and predictions for specific individuals. In AAL can be used to issue reminders for seniors or cognitive/physical-ill residents.
- Context Modelling – the ability to represent all the information gathered from sensors the algorithm predictions into model of the current environment.
- Anomaly Detection – ability to detect unexpected behaviors. Especially used in AAL system implementations to detect possible hazards that could affect or be produced by seniors or cognitive/physical-ill residents.
- Resident Identification – ability to identify and locate the resident indoor.
- One of the most important functions of a smart home implementations used for AAL has to be the ability to understand and perceive new types of situations.

It has to interpret sensory information and recognize activities patterns even if they are new activities from the system implementation point of view. It has to analyze daily activities, interpret new activities and predict normal or abnormal resident behaviors [16].

B. Elasticity

Nowadays elasticity is found in the context of cloud computing and is considered to be one of the primary properties of cloud computing. [3]

In the paper [3] the authors say that elasticity in cloud is a degree of the system which indicates the ability of adapting to changes of workloads and provide resource allocation and deallocation on demand.

Often elasticity in cloud computing is thought to be the same as scalability, but scalability differs by not taking in consideration the actual demand over the resources.

We can think that elasticity can have the same role in a context of a smart house because there are numerous available resources for usage. Of course there are not as powerful as in cloud computing, but the demand is not as big as in cloud computing and the context of a smart house can be seen as a grid, such as cloud computing.

C. Cryptography

Cryptography is a way of technique of hiding information in order to protect it from being read. [4] There are 2 types of cryptography: symmetric and asymmetric. The symmetric cryptography it uses same length keys for encryption and decryptions, while in the asymmetric cryptography the length of the key differs and is called Public Key Cryptography because the encryption key is public.

1) DES

Data Encryption Standard, used since the ‘70s, is an encryption algorithm which uses a secret key with a length of 56 bits to operate a block of 64 bits of information. [4] The main concern on DES is the key length because is too short and it can be broken with brute force easily with a parallel machine where a node is able to try 50 million keys/sec. [5]

2) RSA

RSA (Ron Rivest, Adi Shamir and Leonard Adleman) is an asymmetric algorithm based on factoring the product of two large prime numbers. Information is encrypted with the public key and is decrypted with the private key. [5] RSA is a strong algorithm because is time consuming to find the factorization. [5]

In the paper [6] the authors present a modified RSA algorithm used for secure file transmission.

3) SHA-384

SHA-384 is a Secure Hash Algorithm, truncated version of SHA512. SHA-384 produces a digest over a message with the length of 384 bits, and has 80 rounds of operations on the message and operates on block with length of 128bits. [12]

SHA-384 truncates the final result of SHA-512 from 512 bits of digest to 384 bits of digest, reducing the memory storage for digest. [13]

D. Cryptographic chalenges

In order to assure security in smart houses there are three requirements that provides minimal security: privacy, integrity and verifiability. [8]

Privacy refers to confidentiality or limiting access to data and privacy for users.

Integrity refers to the property of data not being altered through time.

Verifiability is the option that user should have in order to verify that the results of computations are correct.

E. Security mechanism

In the paper [7] the authors propose a system based on 2 levels of encryption for text files in cloud computing. In the phase of encryption, the first level is encrypting with DES and the second level is encrypting using RSA. For the decryption phase the cryptographic algorithms are used in the reverse order.

We focus our goal in adapting this mechanism in order to assure security for data existent in a context of a smart house. We chose this mechanism because it offers a better confidentiality for data because of its two levels of encryption.

F. SEA

SEA stands for Scalable Encryption Algorithm and is a cryptographic algorithm based on a Feistel Structure. In the paper [9] the algorithm is detailed explicitly. The algorithm is made of following operations: bitwise XOR, substitution box, word rotation, bit rotation and addition.

In the paper [10] the authors present an implementation of SEA and in the paper [11] the authors measure the performance of SEA.

III. EXPERIMENTAL METHODOLOGY

We will make an algorithm with Open MPI which encrypts files on two levels. In the following lines we describe out steps in implementing the desired algorithm in our algorithm. Our application contains 5 big steps: [7] (Figure 1)

1. file generation
2. first validation
3. first level of encryption
4. second level of encryption
5. final validation

We chose to use multiple level encryption with DES and RSA in order to assure long term security [14] because multiple encryption is a technique that provides data security by performing the process of encryption multiple times, using the same or different algorithms [15].

A. File generation

In order to produce and measure elasticity through our application we will generate a big file. We simply did this by writing many lines in a file. After ending the file generation step we succeeded in creating a big file.

The size of the file is approximately 100 MB. We did this in order to test the elasticity in a smart house context, but it can be done with any size desired. The reason that we chose just 100 MB is that in a context of a smart house the volume of existent data is not huge.

B. First Validation

In this step of the algorithm we read the file and compute a hash algorithm on its data in order to validate the data. For this we chose to use the SHA 384 algorithm [12]. We compute a hash on the file because we want that the destination point to be able to certify that data have not been altered by somebody and to confirm that data is valid.

We chose this hash function because is fast, doesn't us to much memory to store, SHA-384 being a truncated version of SHA-512. [13]

C. The first level of encryption

In this phase of the algorithm we read the data in blocks of 64 bits length plain text and encrypt with DES algorithm with a 56 bits block of key resulting a 64 bits block of cipher text. [4]

We chose DES algorithm because is fast and has only 16 rounds of operations [5] and this way we provide the first level of security.

D. The second level of encryption

This is the second level of encryption of the algorithm we use. For this level we need a public key for who will be transmitted the file. The algorithm used in this phase is RSA algorithm. RSA algorithm [5] is applied on the output generated by the DES algorithm on the plain text.

With RSA we realize the second level of encryption and prove extra security for the files

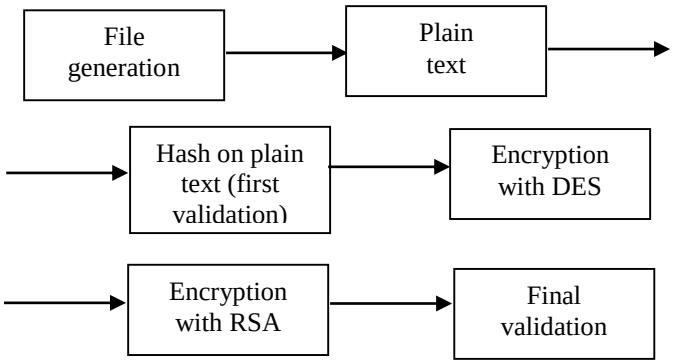

Figure 1. Algorithm phases

E. Hardware

We will make our tests on a cluster based on Linux virtual machines (1 core, 1 GB RAM) following the next procedure:

- We will make every test 5 times
- We will run our application with 1 to 8 machines
- We will measure every step of the algorithm

F. Measurements

We will test our algorithm on different number of machines. For every step of algorithm, we will select the optimal number of machines to run. This is the number of machine that executes the step in almost same time like a bigger number of machines

For every case of machine number, we will measure time of every step of the algorithm and show the results through graphs. For every number of machines and for every step we will calculate the average time of execution and show it.

IV. Experimental results

A. Step1 – File generation

Below are the results of the first step of the algorithm. We can observe that the time is shrinking with running on bigger number of machines (Figure 2). The optimal number of machines is 4 because from 4 to many the difference is too little.

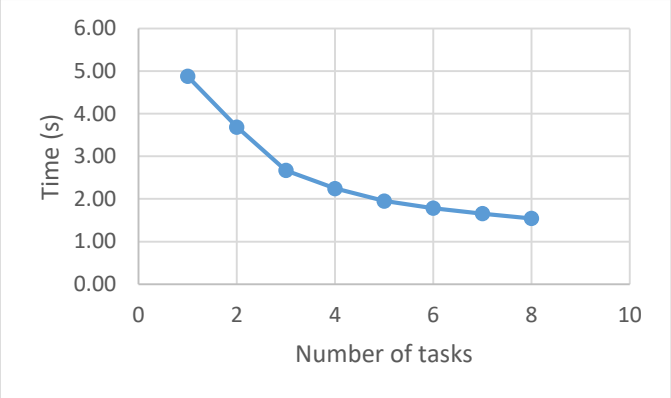

Figure 2 – File generation

B. Step2 – First validation

In this step we perform SHA-384 [12] on the file. In the Figure 3 we can observe that the optimal number of machines is 5 because from 5 to many the difference is too little.

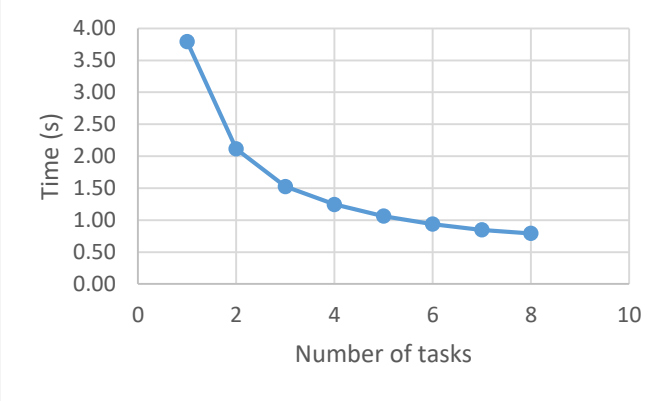

Figure 3 – First validation

C. Step 3 – First level of encryption

Below is the result of the first level of encryption. Encryption is made with DES [4] and the plain text is encrypted in blocks of 64 bits, so in this case the number of machines doesn't really make a change because the encryption is made in blocks. Every block is encrypted, so this encryption is not made on all of plain text. Basically you do the same iterations on 1 or more machines.

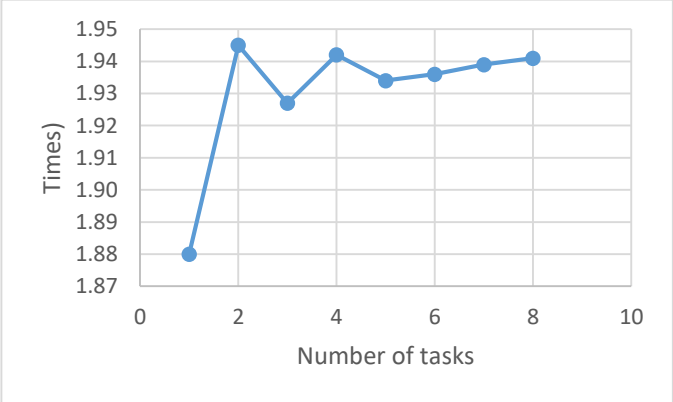

Figure 4 – First level of encryption

From we can observe that the difference of time depending the number of machines is the order of milliseconds, so is irrelevant. For this step the optimal machine number is 1.

D. Step 4 - Second level of ecnryption

Below are the results of the second level of encryption. The encryption was made with RSA [5] with 1024 bits public key. We observe in Figure 5 that the lowest time is with 3 machines, and after that is easily increasing and varying with2 milliseconds. This happens because the encryption with RSA the output has the same length of the modulus, so if we split data in many machines and encrypt each one part with RSA we will have 1024*number of machines bits of output. So it takes a little more time, but, as seen, the difference if about 2 milliseconds. So the optimal machine number is 3.

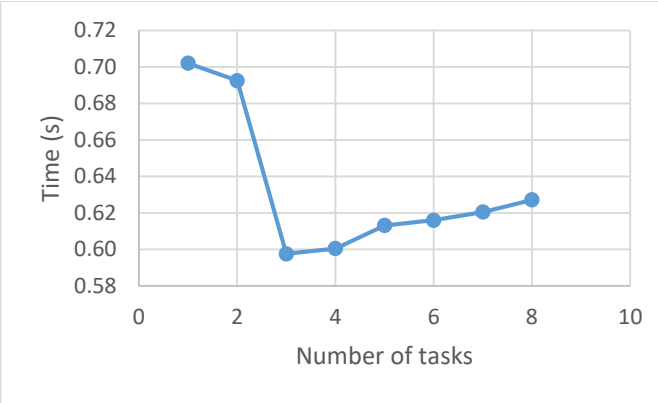

Figure 5 – The second level of encryption

E. Step 5 – Final validation

We decided to make another validation in order to make a better security for long term. This validation is another hash value performed with SHA-384 [12], but this time on cipher text. The reason we make this extra validation is to assure the destination point, at decryption, that data has not been altered.

Another reason we make this is to prevent destination point to decrypt for nothing. First the destination point calculates hash on cipher text and if the value is not the same than the decryption will not return all the plain text. So this way he can assure that doesn't encrypt for nothing.

In the figure below we see that from 5 machines to many the difference of time is too little, so 5 is the optimal machine number.

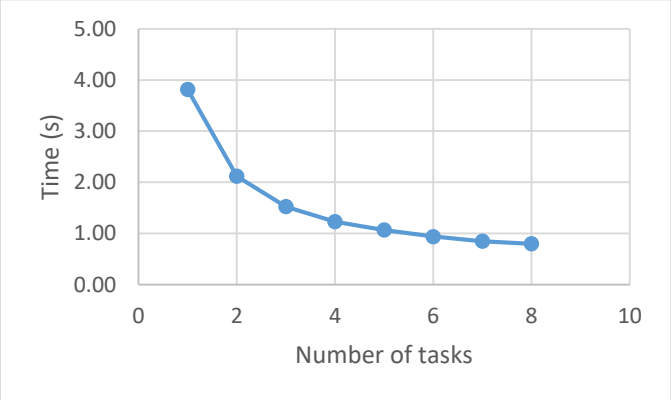

Figure 6 – The final validation

F. Elasticity

In the figure below we can observe the elasticity of the algorithm. The second and final steps have the same optimal number of machines because is the same operation, but is made on different data.

So our mechanism can be easily used with few resources in a context of a smart house because it doesn't need a big number of workers to process data.

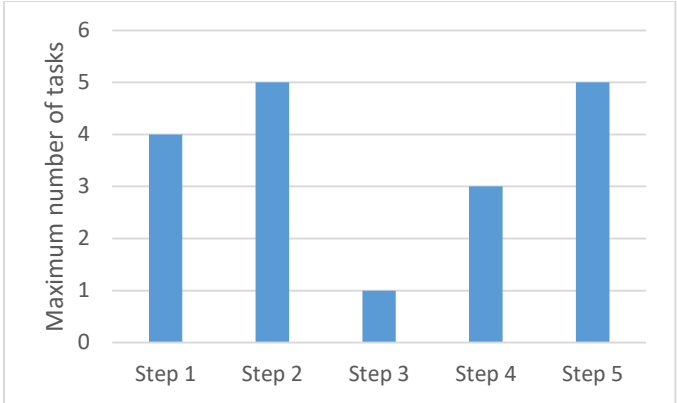

Figure 7 – Elasticity

V. Future Work

As a future work the cryptographic algorithms can be replaced with other algorithms that will scale even better than those ones. For example, the first level of encryption can be done with AES and the second level of encryption can be done with RSA or other public key algorithm. And the application can be done to go further and encrypt more than one file at a time.

VI. Conclusion

Our application is used to encrypt file with multiple level of encryption and gives tools to decryption point to verify data integrity. Our algorithm assures long term security with the use of multiple encryption.

The result of tests showed that our application scales and can be used, for example, for storage of sensitive data because it provides security and integrity with the advantage of multiple encryption used and hash values.

VII. References

[1] UN: World population ageing: 1950–2050. (2001).

[2] Alzheimer's Association: 2015 Alzheimers Disease Facts and Figures. (2015).

[3] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Elasticity in Cloud Computing: What It Is, and What It Is Not, ICAC (pages 23-27), June 2013

[4] Mohit Mittal , Performance Evaluation of Cryptographic Algorithms, International Journal of Computer Applications (0975–8887) Volume (2012).

[5] K. Kalaiselvi, Anand Kumar, Implementation Issues and Analysis of Cryptographic Algorithms based on different Security Parameters, International Journal of Computer Applications (0975 – 8887), International Conference on Current Trends in Advanced Computing (ICCTAC-2015)

[6] Rajan.S.Jamgekar, Geeta Shantanu Joshi, File Encryption and Decryption Using Secure RSA, International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013

[7] Shakeeba S. Khan, Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, International Journal of Innovative Research

in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015

[8] Sashank Dara, Cryptography Challenges for Computational Privacy in Public Clouds, Cloud Computing in Emerging Markets (CCEM), 2013 IEEE International Conference on (pages 1-5). IEEE.

[9] Francois-Xavier Standaert, Gilles Piret, Neil Gershenfeld, Jean-Jacques Quisquater, SEA a Scalable Encryption Algorithm for Small Embedded Applications, Smart Card Research and Advanced Applications, pp. 222-236. Springer Berlin Heidelberg, 2006.

[10] Francois Mace, Francois-Xavier Standaert, Jean-Jacques Quisquater, ASIC Implementations of the Block Cipher SEA for Constrained Applications, Conference on RFID Security 07, Malaga July 11-13

[11] M. Nagendra, M. Chandra Sekhar, Performance Modeling of Scalable Encryption Algorithm using Parallel Computation, International Journal of Simulation Systems, Science & Technology 14, no. 2 (2013)

[12] Khovratovich, D., Rechberger, C., & Savelieva, A. (2012, January). Bicliques for preimages: attacks on Skein-512 and the SHA-2 family. In *Fast Software Encryption* (pp. 244-263). Springer Berlin Heidelberg

[13] Gueron, S., Johnson, S., & Walker, J. (2011, April). SHA-512/256. InInformation Technology: New Generations (ITNG), 2011 Eighth International Conference on (pp. 354-358). IEEE.

[14] Zhang, R., Hanaoka, G., Shikata, J. and Imai, H., 2004. On the security of multiple encryption or CCA-security+ CCA-security= CCA-security?. In*Public Key Cryptography–PKC 2004* (pp. 360-374). Springer Berlin Heidelberg

[15] Gupta, H. and Sharma, V.K., 2011. Role of multiple encryption in secure electronic transaction. *International Journal of Network Security & Its Applications (IJNSA)*, *3*(6), pp.89-96

[16] Suryadevara, N., Mukhopadhyay, S.C., Wang, R., Rayudu, R.: Forecasting the behavior of an elderly using wireless sensors data in a smart home. Engineering Applications of Artificial Intelligence 26(10) (2013)2641–2652