Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Akinduro, P. A, Alese, B. K, Alowolodu, O. D, Thompson, A. F, & Akinwonmi, A. E. (2015). Development of a secured shared processing system. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* pp. 29-41. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p029-041Akinduro1555.pdf

Development of a Secured Shared Processing System

P. A. Akinduro, B. K. Alese, O. D. Alowolodu, A. F. Thompson, and A. E. Akinwonmi
Computer Science Department, Federal University of Technology, Akure, Nigeria

deronkeakinduro2006@yahoo.com; bkalese@futa.edu.ng; odalowolodu@futa.edu.ng; afthompson@futa.edu.ng; aeakinwonmi@futa.edu

Abstract

The most common way of ensuring confidentiality of data or documents by individuals, governments, and institutions such as banks, hospitals, and other commercial enterprises is by consigning their secrets to a computer system. But this has not solved the problems of upholding security, instead they are more compounded due to the fact that secrets sharing is generally desired but only in a tightly controlled manner. This could be resolved by the introduction of a secured shared processing system. Secured shared processing system is a system that comprises of several computers whereby one stands as a secured, trusted system while the other systems are connected to it. The system do not divide up a memory or a clock; the computers only communicate with each other by exchanging messages over a communication channel; and each computer has its own memory and operates on its own operating system. This is achieved with the aid of Cryptographic mechanisms in which EI Gamal model was adopted as a Public-key cryptography scheme which will be applied on a workstation distributed System.

Keywords: Cryptography, Shared Processing, Parallel Computing, El Gamal Principle

Introduction

A shared processing system is a computer processing method in which different parts of a program are run in parallel on two or more computer systems that are communicating with each other over a network in which one computer stands as trusted system while the rest stand as untrusted systems. According to Attiya et al, (2004); Nadiminti and Dias, (2006;), Shared computing is a type of segmented or parallel computing, but the latter term is most commonly used to refer to processes in which different parts of a program run simultaneously on more than one processors that are part of the same computer. While both types of processing require that a program be segmented into sections that can run simultaneously. Shared processing computing also requires that the division of the program

Editor: Eli Cohen

take into account the different environments on which the different sections of the program will be running. For example, two computers are likely to have different file systems and different hardware components.

Individuals, governments, and institutions such as banks, hospitals, and other business enterprises will only entrust their secrets to a computer system if they can be sure of confidentiality. The glitches of maintaining security are further compounded because the sharing of secrets is generally preferred but only in a tightly controlled manner. In the simplest case, an individual can choose other individuals or groups with whom he wishes to share his private information. This type of controlled sharing is called discretionary security because it is permitted at the discretion of the individual. (Rushby, 1983).

Secured shared processing system is a system which consists of several computers in which one stands as secured, trusted system to which all other systems were connected with. They do not share the same memory or clock; the computers communicate with each other by exchanging messages over a communication channel; and each computer has its own memory and runs on its own operating system. The resources that reside ,owned and controlled by a computer are said to be local to it, while the resources that reside, owned and controlled by other computers and can only be accessed through the network are said to be remote. Typically, to access a remote resources is more expensive than accessing local resources because of the communication delays that occur in the network and the CPU overhead incurred to process communication protocols. The reasons behind the development of shared processing systems are the availability of powerful microprocessors at low cost as well as noteworthy advances in communication technology. The availability of powerful yet affordable microprocessors has led to the development of powerful workstations that satisfy a single user's needs. The main advantage of a secured shared processing system is the availability of a decisive price/performance advantage over more traditional time-sharing systems.

A secured shared processing system is to provide a general-purpose distributed computing system that is not only secure but also highly efficient, cost-effective, and user-friendly. The approach involves interconnecting small, specialized, provably trustworthy systems and a number of larger, untrusted host machines. The trusted system which will be referred to as the reference monitor controls the behavior of the untrusted system components. The trusted components will facilitate access and communications between the untrusted hosts; they will also make available specialized services such as a multilevel secure file store and a means of changing the security partition to which a given host belongs. The secured shared processing system is achieved by Cryptographic mechanisms in which EI Gamal model was adopted as a Public-key cryptography scheme which applied on a workstation distributed System.

Related Works

Applications and security are multi-faceted, from e-commerce and payments security to private communications and password protection. An important way to ensure secure communications is cryptography and it could be defined as the science of encoding and decoding messages over a communication channel especially over an insecured channel . In data and telecommunications, cryptography is normally used to secure the data and the communication channel especially if it is over any untrusted medium, which includes just about any network, especially the Internet. (Gary, 2013). There are some characteristics and requirements of any secured application-to-application communication, and these include: Authentication, Privacy/confidentiality, Integrity and Non-repudiation. This goes to show that Cryptography not only protects data from theft or alteration, but can also be used for user authentication. There are three general types of cryptographic schemes namely:

1. **Secret Key or symmetric Cryptography (SKC):** this makes use of a single key for both encryption and decryption
2. **Public Key or asymmetric Cryptography (PKC):** needs one key for encryption and another for decryption
3. **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information.

As stated in the work of Gary (2013), Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:

- RSA (Rivest Shaman and Adleman)*:* uses a variable size encryption block and a variable size key.
- Diffie-Hellman: D-H is used for secret-key exchange only, but not suitable for authentication or digital signatures.
- Digital Signature Algorithm (DSA)*:* The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.
- El Gamal: Designed by Taher El Gamal, a Public Key Cryptography (PKC) system similar to Diffie-Hellman and used for key exchange.
- Elliptic Curve Cryptography *(ECC):* A PKC algorithm based upon elliptic curves.

Rosly et al. (2013) used El Gamal algotithm for cryptographic computation in 32 – bit computing system. The analysis of El Gamal was used for securing data communication through the computer system. An experiment was carried out to devaluate the maximum of integers that a 32 – bit computer can compute using the standard 32 – bit GCC compiler. This was collected on three different occasions to measure up performances. The research concluded that data in real time were not suitable as a reference to be implemented because the work was not implemented in real time mode. Real time mode output includes other processing time, so the output time is not accurate. The actual times for the specific process are counted by using a combination of time in user mode and system mode.

Babatunde et al (2014) proposed a system that provides a secure platform for encrypting and decrypting user's key. This made use of El Gamal as a network – based key exchange cryptography. Although the system has some drawbacks due to the algorithms show speed, message expansion by one or two factors during encryption. It is sematically insecure and require randomness during operation. The research concluded that a further research could be done in the area of hybridization to improve the efficiency and application of the system in the area of data security and information.

Khaled and Abdelazziz 2012, presented a voice encryption method called "DES with Random permutation and Inversion. This is used to increase the security of the exchanged data in Global System for Mobile Communications (GSM). Their work was based on current voice channel, which overcomes data channel's insufficiencies and solves the problem of penetrating the regular Pulse Excitation-Long Term Prediction (RPE-LTP) vocoder by the encrypted voice. The proposed method fulfils an end-to-end secured communication in the GSM; ensures a good compatibility to all GSM networks, and provide easy implementation without any modification in the systems. The encryption method has the advantages of suiting the RPE-LTP compression module requirements, good compatibility to GSM networks, and suitable implementation without any adjustment in current GSM signalling system

A multi-tier model for secured computing as a teaching method platform was designed and developed by Iliya and Ivo (2001). The model was based on establishing the credibility and role of

each component in a distributed computing environment. The components in the environments are but not limited to trusted users, servers, administrators, untrusted client, communication media and intermediate systems. This work addressed the issue of computer system security in an organized and systematic way by utilizing a basic model, which simplifies the analysis of whether the security requirements (both technical and social) are satisfied or not. The major disadvantages are replication of kernel-mode operating system security, significant processing speed reduction, and increased vulnerability to expert cryptanalytic attacks.

Rupa, et al (2012) used cryptography and steganography to secure communicated messages. The original message was encrypted by using Prime numbers and Gray code Algorithm (PGE) i.e cipher text, which is a first layer of security. In the second layer of data security, cipher text is embedded into an image using Linear Block Parity coding (LBP) approach. This method satisfies all security services such as improved authentication through new encryption algorithm PGE and improved confidentiality by LBP steganographic approach and less chances to retrieve or modifying the messages in middle of the process i.e. non repudiation, integrity and availability, but the method has undesired impact on the legitimate flows.

Sanjay et al, (2011) presented dynamic replication management architecture to improve the performance and dependability of distributed system. Improved performance is realized by evading the re-computation for all replicas from preliminary stage and placement of replicas uniformly over all distant nodes. Improved dependability is achieved by placing the replicas over totally distant set of computing nodes. From the result of their experiment, the approach takes lesser time as compared to simple non adaptive placement approach that computes the placement from initial stage if number of replica changes rapidly or new nodes joins the distributed system. Their approach is adaptive to change in number of replicas of each process or some process. In case of new nodes arrival, the disjoint module only compute placement for new nodes replicas without doing much computation for all existing replicas. It takes less bandwidth and latency since only fewer numbers of replicas in distributed system joins to the distributed system. Fault tolerance capability is also improved since placements of replicas are done on disjoined nodes. In case of several nodes failure of same link, disjoint replica placement increases dependability of distributed system as well.

System Design

In this work, the secured shared processing system is enhanced by Cryptography mechanisms in which EIGmal model was adopted as a Public-key cryptolography scheme which will be applied on a workstation distributed System.

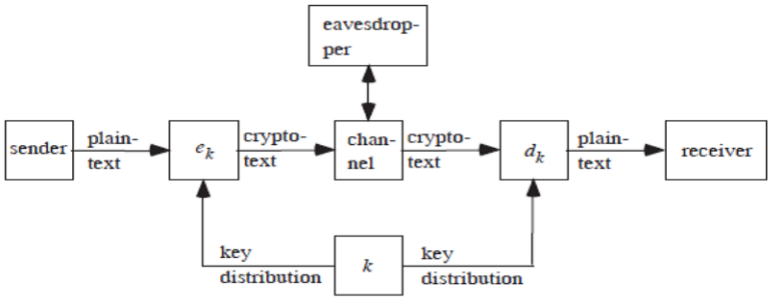


Figure 1. The general working principle of cryptography

The security of the El Gamal depends on the difficulty of computing discrete logs in a large prime modulus. The El Gamal is being used for this system because, when the paramters are chosen in

the right way, it achieves the weaker notion of indistinguishability under chosen plaintext attacks. Another efficiency of El Gamal is that it is probabilistic, meaning that a single plaintext can be encrypted to many possible ciphertexts, with the consequence that a general El Gamal encryption produces a 2:1 expansion in size from plaintext to ciphertext. Cryptosystem which can be defined as the 5-tuple (M;C;K;E;D) where $M \in \sum^*$ is the plaintext message Alice intends to transmit to Bob. The plaintext message can be divided into multiple blocks denoted as m_i. The ciphertext C $\in \sum^*$ is the result of an encryption function $E_K(P) : C$, which takes the plaintext and an additional key K, and computes the ciphertext. Bob, who receives C, uses it with a decryption function $D_k(C) : P$, under application of the key K and resulting into the plaintext. The message has been transferred, and Eve was not able to read it.

Table 1. Entities and their Keyparts

Persons	Private Key	Public Key
Alice	A	$g^a \bmod p$
Bob	B	$g^b \bmod p$

According to Andreas, (2005) There are four (4) procedures to follow when using El Gamal cryptography

I. Key Generation
II. Encryption Procedure
III. Decryption procedure
IV. El Gamal signature

Key generation

With El Gamal, the receiver only needs to generate a key in advance and publish it. Following these steps:

-Private key naming scheme: from above, Bob has to generate the key-pair

-Prime and group generation: Bob needs to create a large prime p and the generator g of a multiplicative group Z_p^* of the integers modulo p.

-Selection: Bob selects an integer b from the group Z by random and with the constraint $1 \leq b \leq p-2$. This will be the private exponent.

-Public key assembling: From this, the public key part $g^b \bmod p$ is computed. The public key of Bob in the El Gamal cryptosystem is the triplet (p; g; g^b) and the private key is b.

- Public key publishing: The public key now needs to be published using some dedicated key-server or other means, so that Alice is able to get hold of it.

Encryption Procedure

To encrypt a message M to Bob, Alice needs to obtain Bob's public key triplet (p; g; g^b) from a key server or by receiving it directly via unencrypted electronic mail. There is no security issue involved in this transmission, as the only secret part, b, is sent in g^b. Since the core assumption of the El Gamal cryptosystem says that it is infeasible to compute the discrete logarithm, this is safe. For the encryption of the plaintext message M, Alice has to follow these steps:

1. Obtain the public key

Alice has to acquire the public key part (p, g, g^b) of Bob from an official and trusted keyserver.

2. Prepare M for encoding

Write M as set of integers (m_1, m_2)in the range of $\{1,....,p-1\}$. These integers will be encoded one by one.

3. Select random exponent

Alice selects a random exponent *k* that takes the place of the second party's private exponent in the Diffie-Hellman key exchange. The randomness here is a crucial factor as the possibility to guess the *k* gives a sensible amount of the information necessary to decrypt the message to the attacker.

4. Compute public key

To transmit the random exponent *k* to Bob, Alice computes $g^k \bmod p$ and combines it with the ciphertext that is sent to Bob.

5. Encrypt the plaintext

Alice encrypts the message *M* to the ciphertext *C*. For this, the set created in step 2 is iterated and calculated for each of the m_i: $c_i = m_1 * (g^b)^k$

The ciphertext *C* is the set of all c_i with $0 < i \leq |M|$.

The resulting encrypted message C is sent to Bob together with the public key $g^k \bmod p$ derived from the random private exponent.

Even if an attacker would listen to this transmission, and in a second step would also acquire the public key part g^b of Bob from a keyserver, g^{b*k} would still be difficult to derive as can be seen from the Discrete Logarithm problem.

El Gamal advises to use a new random k for each of the single message blocks m_i. This greatly improves security, as knowledge of one message block m_j does not lead the attacker to the knowledge of all other m_i. The reason for this ability is that if $c_1 = m_1 * (g^b)^k \bmod p$ and

$$c_2 = m_2 * (g^b)^k \bmod p,$$

from knowing only m_1 the next part of the message m_2 can be calculated by the following formula: $\frac{m1}{m2} = \frac{c1}{c2}$

Decryption Procedure

After receiving the encrypted message C and the randomized public key g^k, Bob has to use the encryption algorithm to be able to read the plaintext M in the following steps:

1. Compute shared key

The El Gamal cryptosystem helped Alice to define a shared secret key without Bobs interaction. This shared secret is the combination of Bobs private exponent b and the random exponent k chosen by Alice. The shared key is defined by the following equation:

$(g^k)^{p-1-b} = (g^k)^{-b} = b^{-bk}$

2. Decryption

For each of the ciphertext parts c_i Bob now computes the plaintext using

$m_i = (g^k)^{-b} * c_i \bmod p$ After combining all of the m_i back to M he can read the message sent by Alice.

El Gamal Signatures

The El Gamal cryptosystem does not only support encryption and decryption, but also the electronically signing of messages M. A signature scheme has three main characteristics:

1. Creation

Alice needs to be able to find the signature for M by using her private key a, then send the message together with the signature as the pair (M; S) to Bob.

2. Verification

Bob has to be able to verify the signature by using the public key g^a. The verification of the signature assures Bob that Alice has signed the message as he received it. It does not deliver information about if Alice wrote the message herself or if she intended to send it at all. The second information Bob can draw from the verification is that the message has not been altered on the transmission path between him and Alice.

3. Forgery prevention

It should not be possible for a malicious user to use the public key g^a of Alice to create a signature for an arbitrary message. A signature in the El Gamal cryptosystem is the pair (r, s) with $0 \leq r; s < p-1$ defined by the equation $g^M = (g^a)^r r^s \bmod p$. The procedure of signing follows similar steps as the encryption procedure:

1. Choose random $k \in G$

2. Compute $r = g^k \bmod p$

3. Fill the signature equation from above as $g^M = g^{ks}$ g^a gargks mod p and solve it for s using

$m = ar + ks \bmod (p-1)$.

This has a solution for s if k is chosen such that gcd (k, p -1) = 1. Bob received (M, r, s) and wants to verify the signature now. For this, Bob only needs to compute both sides of the equation check for equality.

Table 2. Parameters of the proposed System

PARAMETERS	**MEANING**
MEP	Ministry of Employment and Productivity
CSC	Civil Service Commission
TSC	Teaching Service Commission
ESTAB	Office of Establishments, training and service

The slim vacant position in the public service has given now to inequality and favoritism because everyone wants their own to be given a place in the little available position declared vacant in various Ministry and government agencies.

The proposed secured share processing System will involve five Ministries, namely

- Ministry of Employment and Productivity: The only trusted Ministry while the other four Ministries will be untrusted.
- The Civil Service Commission: The recruiting arm of Civil Service for senior civil Servants from grade level 07 and above.
- The Establishment Department: Caters for the recruiting of Junior Civil Servants from grade level 01 to grade level 06 will be another untrusted Ministry.
- The Teaching Service Commission: Caters for the recruitment of staff in the Teaching Service will be another untrusted Ministry, and the last among the untrusted Ministries.

Any recruitment that is to be made either from the Civil service be it senior or junior or the Teaching service Commission, request will be made via Ministry of Employment which is the only trusted System through their log in details which already would have been given to the respected untrusted system/Ministries.

The Ministry of Employment and Productivity, the only trusted Ministry already has the data of all the unemployed graduates of Ondo state origin in its database, the Ministry of Employment will now sieve out the names from their database and send to the respected Ministries of agencies which vacancies had been declared. The Ministry /Agencies can now communicate to the concerned unemployed graduates based on details sent to them from Ministry of employment for exams and interview. The successful candidates will be issued letters of employment, After which these names will be declared open for Ministry of Employment and Productivity to be removed from its database while the names will be declared for the concerned Ministry for viewing and Printing by all other Ministries,

The proposed System to be designed will contain two log in details:

- The executive log in and
- The Administrative log in

The Ministry of Employment and Productivity which is the only trusted Ministry/System will be given the executive log in, the Administrative Log in will be given to Civil Service Commission, Teaching Service Commission and office of Establishments.

System Implementation

The system was implemented on a .NET framework (Murach, 2010) using visual studio as an IDE (Integrated Development Environment) which offers multiple-document-interface feature that makes it suitable for application development (Nagel et al, 2008) as well as C# programming language to code the model. Microsoft SQL server 2005 was also used as the backend. The System environment is made up of a single system that is capable of executing both the trusted and the untrusted application. It is configured with the following specification: Window 7, 4.00GB RAM size, Intel(R) Core(TM) i3 CPU M330 @ 2.13GHz processor.

Result and Discussion

The implementation procedure involves some stages of which few is mentioned.

(a) Login session
(b) Received message/ Home page for MEP
(c) Decrypted message page by MEP
(d) Session for message to be encrypted by MEP
(e) Encrypted message page by MEP
(f) List of unemployed applicant's page by MEP
(g) Decrypted message page by CSC

Login Session

This page authenticates each ministry to have access to the secured system. At the login session, there are three menus namely: select ministry which has submenu of all the names the four ministries; enter password and enter ministry code. The submit button enables each ministry to gain access to its own home page.

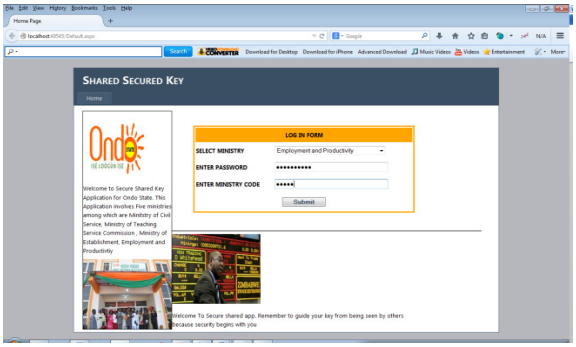


Figure 2 login session

Received message /Home page for MEP

This page is known to be the Home page for Ministry of Employment and Productivity. Here, there are sub menus like send message which allows the Ministry to send messages, also the view message sub menu allows the Ministry to view messages sent from different Ministries, while the view list applicant sub menu allows the Ministry to view all the registered unemployed graduates within the State.

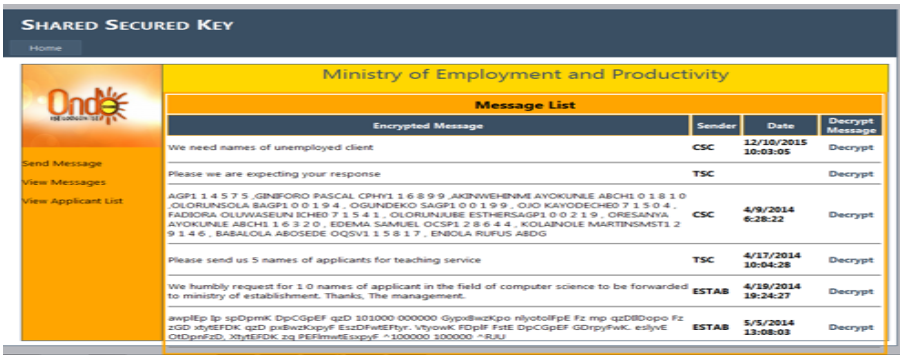


Figure 3 The received /Home page for MEP

Session for message to be encrypted by MEP

The page to displays send message menu, view massage menu and view applicants list menu. The send message menu displays where the ministry of Employment and productivity (MEP) types message which will be seen by the user as a plaintext and key needs to be generated automatically by clicking on generate key which is the first step in El Gamal encrypted procedure. After generating the key, a submenu Recipient code which has the code of the particular ministry you are sending the message to needs to be selected. A Recipient submenu identifies the destination ministry, then the message needs to be encrypted using the encrypt message submenu which

automatically changes the plaintext to ciphertext and the send submenu takes the message to the appropriate destination.

Figure 4 Message to be encrypted by MEP

Encrypted message page by MEP

This page shows the encrypted message to be sent by Ministry of Employment and Productivity also known as cyphertext.

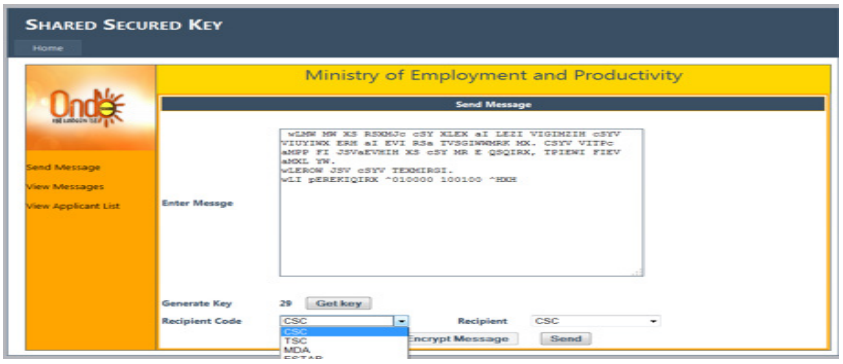


Figure 5 Encrypted message by MEP

List of unemployed applicant's page

This page allows the trusted system that is the Ministry of Employment and Productivity to view the list of all the registered Applicants. Figure 6 shows the list of all unemployed applicants.

Figure 6 list of unemployed applicant page

Decrypted message by CSC

Also this page performs the same function as in 4.3.4 and it also applies for all other Ministries.

Figure 7 decrypted message by CSC

Conclusion

Knowing fully that security is the degree of resistance to or protection from harm and it applies to any vulnerable and valuable assets in which computers, programs are not left out, it is not enough to have country or State with Ministry of Employment and Productivity and not have a proper and secured way of employing Staff who are competent for the job without a biased mind. At the implementation level, the information is been secured using El Gamal encryption which simplified the Diffie Hellman key exchange algorithm by introducing a random exponent k which is the replacement for the private exponent of the receiving entity. The study has also identified various methods and techniques through which competent personnel can be employed in the State Civil Service with the proposed secured System without sentiment. As security of lives and properties is important so also the security of information or messages in order to have a better and advanced country that is free from corruption and sentiment when it comes to employment, the proposed method can be used to secure information that is being shared among multiple systems. Therefore, this system is recommended for both Government and non-Government Organizations/Agencies for proper recruitment processing. Security is for everybody.

References

Attiya, H., & Welch, J. (2004). *Distributed computing: Fundamentals, simulations, and advanced topics*. Wiley Interscience. ISBN 0471453242.

Babatunde, A. O, Adewole, K. S., Abdulraheem, M., & Oniyide, S.A. (2014). A network-based key exchange cryptosystem using El Gamal algorithm. *African Journal of Computing and ICT, 7*(2).

Deswarte, Y., Blain, L., & Fabre, C-J. (1991). Intrusion Tolerance in Distributed Computing Systems. In *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium* (pp. 110-121). IEEE.

Georgiev, I. K., & Georgiev, I. I. (2001). A security model for distributed computing. *The Journal of Computing in Small Colleges,17*(1).

Kessler, G. C. (2013). *An overview of cryptography*. Retrieved from http://www.garykessler.net/library/crypto.html

Lenhtonen, S., & Prssinen, J. (2002), A pattern language for cryptographic key management. *EuroPLoP Proceedings*, pages 245-258.

Meier, A. V. (2005). *ElGama Cryptosystem. Joint advanced students seminar.* TUM Informatic.

Murach, J. (2010). *Murach's C# 2010*. Mike Murach & Associates.

Nadiminti, K., De Assunçao, M. D., & Buyya, R. (2006). Distributed systems and recent innovations: Challenges and benefits. *InfoNet Magazine*, *16*(3), 1-5.

Nagel, C., Evjen, B., Glynn, J., Skinner, M., Watson. K. (2008), wrox Professional C#: ISBN 978-0-470-19137-8

Rosly, N. A., Zafran, A. A. M., Habibah, H., Farid, S. A. S., & Anua, M. I. M. (2013). Cryptographic computation using ElGama algorithm in 32-bit computing system. In *Proceedings of the Third International Conference on Control, Automation and System Engineering* (CASE, 2013) pp. 63-67.

Rupa, C., Avadhani, P.S, E., Srinivas, R. (2012). An efficient security approach using PGE and parity coding, *International Journal of Distributed and Parallel Systems (IJDPS), 3*(6).

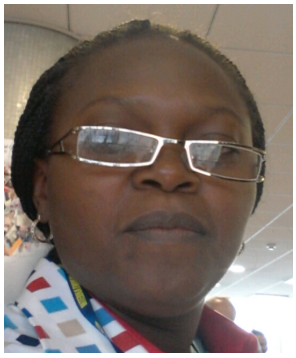
Rushby, J. M., & Randell, B. (1983). *A distributed secure system*. tech. report 182, Computing Laboratory, University of Newcastle upon Tyne, England.

Biographies

Mrs. Akinduro Peace Aderonke is a graduate student of the Department of Computer Science, Federal University of Technology, Akure, Ondo State Nigeria. Her areas of interest include Cryptography and Distributed Systems. She has been able to attend some local conferences and workshops.

Dr. Alese Boniface Kayode is presently an Associate Professor with the Computer Science Department of the Federal University of Technology Akure, Ondo State, Nigeria. He holds a Ph.D. degree in Computer Science from The Federal University of Technology Akure, Ondo State, Nigeria in 2004. He has several awards of excellence. His areas of research include, Computer and Network Security, Quantum Computing and Digital Signal Processing. He is the current holder of the First Bank Professorial Chair in Computer Science of the Federal University of Technology, Akure, Nigeria.

Mrs. Alowolodu Olufunso Dayo is a Lecturer in the Department of Computer science, Federal University of Technology, Akure. She is rounding up her PhD programme in the same institution. She has attended many workshops and conferences and has published papers in conferences and journal of international repute. Her area of interest spans Genetic Algorithm, Cloud Computing and Cryptography.



Dr (Mrs) A.F Thompson is working as a Senior Lecturer in the Department of Computer science, Federal University of Technology, Akure. She finished her PhD in the year 2014. She has attended numerous international conferences and workshops where she presented papers that had appeared in reputable journals. Her areas of research interest spans Biometrics, Network Security and Image Processing Algorithms.

Akinwonmi, Akintoba Emmanuel lectures at the Computer Science Department of the Federal University of Technology, Akure. He had earlier joined the University in 1997 as a systems programmer. He rose to the post of a Chief System Programmer before joining the Computer Science Department in 2010 as a lecturer, from where he had earlier obtained a PGD and a Master of Technology degree in 2007. He is on the Ph. D programme and his area of research crosses artificial intelligence, DSP and NLP.