Journal of Computations & Modelling, vol.4, no.2, 2014, 41-58
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2014

Fingerprint Biometric-Based Cryptographic System as A Security Approach in Grid Environment

Abdulraheem Muyideen[1], Aremu Dayo R.[2], Adewole Kayode S.[3] and Muhammed Kamaldeen J.[4]

Abstract

Interconnection of computer systems for the purpose of sharing resources in grid is increasing on the daily bases. Resource shared in grid is not limited to files alone but also includes computer resources such as memory, processors, etc. The security challenges resulting from this sharing is enormous including authentication, authorization, integrity, availability. These call for research attentions as evidenced from the reviewed literatures. Several researches have proposed cryptographic approaches as a promising solution to the various security challenges. However, issues surrounding the knowledge-based authentication approach motivate the researchers to be more innovative by proposing biometric-

[1] COMSIT Directorate, University of Ilorin, Ilorin, Nigeria.
E-mail: muyideen@unilorin.edu.ng
[2] Department of Computer Science, University of Ilorin, Ilorin, Nigeria.
E-mail: draremu2006@gmail.com
[3] Department of Computer Science, University of Ilorin, Ilorin, Nigeria.
E-mail: adewole.kayode@unilorin.edu.ng
[4] COMSIT Directorate, University of Ilorin, Ilorin, Nigeria.
E-mail: jimoh.km@unilorin.edu.ng

Article Info: *Received* : December 11, 2013. *Revised* : January 23, 2014.
Published online : May 31, 2014.

based cryptographic model to secure grid resources. This paper examines and analyses existing efforts to tackle these challenges. It also examines Grid Architecture where various components of a grid play major role in resource sharing and securing of grid. Biometric-based model was proposed that provides security for grid users using fingerprint for authentication and authorization in grid due to its ease of collectability.

Keywords: Grid, Resources; Biometrics; Architecture; Cryptography

1. Introduction

The computational and storage capacity requirement of users is never met by individual computer system. Users in the field of engineering models, economics, medicine, weather forecasting, cryptography, structural engineering and biology are only a few areas where there is an insatiable hunger for more computational power and storage capacity.

Computational grid is interconnection of computers for the sole purpose of sharing computer resources in order to achieve higher computational power. Ian Foster is the father of computational grids. He envisioned that computational grid be like power grids in which the users of electricity know nothing about generation and distribution of electricity he only make use of it. Computational grids is envisioned to have resources pooled together and make it available to the user who hook-ups with the grids.

Oracle describes computational grids in simple term, as the pooling of all IT resources into a single set of shared services for all enterprise computing needs. Ali et al. [1] described computational grids infrastructure as continually analyzes demand for resources and adjusts supply accordingly.

Ian et al. [2] define computational grid as a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities.

Grid computing enables the virtualization of distributed computing resources such as processing, network bandwidth, and storage capacity to create a single system image, granting users and applications seamless access to vast IT capabilities.

The need for computational grids arose due to high computational need of some complex computation that cannot be met by computational power of single computer. Secondly, more and more computers are being purchased due to advance in technology and crash in price but they are being underutilized. According to a study, more than 90% of computational power of individual computer is idle i.e computers are underutilized [3]. The idea to form grids is to pool idle resources together for better usage.

The main reason behind grids is to save costs by sharing resources. The resources can be advanced programs to solve some task, devices like sensors and computer power. It works because every user does not need the resources all the time. The challenge to make this to work is to get a large group or groups of people to share their resources. There must therefore be good scheduling. This people may not want to share their work with others so the grid must be secure against intrusion and not leak information. The system must be fault tolerance otherwise, people cannot do their job, which will cost the users less effectiveness and also lead to complain. There must also be some payment system so that those who use a resource pay for it.

1.1 Security Requirements of Computational Grids

Security is an important component in the grids computing environment. If you are a user running jobs on a remote system, you care that the remote system is secure to ensure that others do not gain access to your data. If you are a resource provider that allows jobs to be executed on your systems, you must be confident that those jobs cannot corrupt, interfere with, or access other private data on your system.

As good as computational grid is, the security challenges remain source of concern to users. Among the challenges are integrity, confidentiality, authentication, authorization and non-repudiation [4].

Integrity refers to the ability of the computer systems to ensure that the data is protected from unauthorized modifications. Confidentiality is the ability to keep information from being disclosed to unauthorized users. Authentication is the act of ensuring that someone is whom he claims to be. Authorization is the right to perform some actions. Non-repudiation refers to the inability of someone to deny an action taken [4].

Everyone involved in computational grid has concerns regarding security, although the specifics of the concerns may differ. Contributors of resources are concerned that the privacy and integrity of their systems be ensured; users of the systems are concerned that the integrity of their applications, data, and results be maintained; systems administrators are concerned that the resources be made available only to approved users. These necessitate the need for security policies for computational grid.

1.2 Biometrics

Biometrics is using unique physiological or behavioural characteristics (or identifiers) to ascertain and verify people's identity [5]. These unique identifiers include distinct features such as fingerprints, various iris patterns, blood vessel patterns in the retina, voice inflections in speech, and hand shape/geometry. It also includes the way we sign our name or use a computer keyboard. In biometric systems, a sensor measures biological feature of a person such as fingerprint [6].

Then the system compares this feature called the probe with a previously stored sample called enrolment. If the samples match then, the person is granted access otherwise, the person is deny access. Advantages of biometrics is that they neither be forgotten, nor guess.

There are a several biometric technologies available which includes Fingerprint recognition, Hand geometry recognition, Facial recognition, Iris and retina recognition, Voice recognition etc. Fingerprint recognition, hand geometry recognition and iris recognition are most prevalent among these technologies. Voice biometrics works by digitizing a profile of a person's speech to produce a stored model voiceprint or template [7].

2. Related Studies

Computational grid is becoming popular among researchers to solve complex computational problem ranging from Engineering, Mathematics to science application such as weather forecast. Security of the grid is one major obstacle against wide use of the grid. Several attempts and methods have been employed to provide adequate security for users and resources in the grid against unauthenticated and unauthorised users with appreciable level of achievement.

In the work of Jaspher et al. [8], the researchers emphasised that the existing grid security is based on OGSA which uses traditional PKI. They proposed authentication of the grid based on password, ID, biometric and position of the user. The results of the scheme provide enhance security and reduce operational time taken. Jaspher, W. K. & Kirubakaran, E. [8] also gave the advantage of their proposed scheme as a method for reducing disk space use during user authentication since reusability of the already authenticated biometric data will not be required for subsequent access to the grid resources. This, however will enhance the user identification process.

To improve encryption and decryption algorithm use in securing grid, Hisham & Khaled [9] used highly efficient scheme to accelerate RC4 algorithm, which is a stream cipher by about 873.52% when compared to other scheme to secure grid environment. Thus, time taken to identify and accept an authorised user is reduced while time taken to reject an unauthorised user also greatly reduced. The researchers only focused on how to improve encryption and decryption algorithm use in securing grid, however, a more efficient method for grid user authentication was not explored.

Research as shown that different methods of attacks are used on the grid ranging from injecting malcious code into the grids by users and resources to network attack by vicious application.The capability of biometric authentication for securing users authentication cannot be overemphasised as this was emphasised in the research work of [10]. The researchers outlined the capability of biometric authentication system and identified the weak links in the system. They proposed a solution to some of the identified weak links.

Baolin et al. [11] proposed a security for grid based on trust model that compute and compare trust worthiness of entities in the autonomous and different domain. Their model provides different methods to deal with the malicious attack of users and resources belonging to the same or different domains and simulates experiment to evaluate the trust model. While this research work provides protection for grid users and resources against malicious attack, it did not address the problem of user and resources authentication.

Sindhuja et al. [12] proposed identity based cryptography for grid security. The scheme was based on Hierarchical Identity Based Encryption and Hierarchical Identity Based Scheme. It was highly efficient and scalable when compared with previous similar scheme for grid security but not for grid user authentication.

Shengbao et al. [13] research is similar to Sindhuja et al. [12]. The researchers examined certificateless authentication and key agreement protocol for securing the grid based on Diffie Hellman key agreement protocol. The protocol provides mutual authentication among users and resources in the grid and secured communication using common shared session key.

Marty et al. [14] categoried activies to be secured in the grid to include naming and authentication; secure communication; trust, policy, and authorization; and enforcement of access control. The researchers then examined the available mechanisms in securing these activities and then proposed new methods for the security requirements of Grids.

Safieh et al. [15] proposed two level security for grid security based on trust model system. The benefit of this model over previous trust models are the posibility of adding new domains without compromising the security of the grid and choosing of provider that has closest to users.

Rather than using one server to store password, Ruckmani, V. & Sadasivam, S. G. [16] used two seperate servers; authentication server and backend server to store password for authenticating grid users. The protocol is based on the fundamental concept of trigon and the parameters of the trigon is used to authenticate the users of the grid. The user is assumed to be authenticated only when the two servers authenticate the user successfully. The main advantage of the model is that an adversary cannot achieve his aim by having access to one server and it is difficult to have access to the two servers by an adversary. The model involves the use of password for user authentication. However, if the password is compromised by any means, the two servers can therefore be accessed by an adversary.

Patrick et al. [17] stated that porting a complex secure application from one security infrastructure to another is often difficult or impractical. While Kerbrose security is founded on trusted third party with encryted ticket for grid users authentication, the Grid Security Infrastructure (GSI) is founded on public key infrastructure with X509 certificate for grid users authentication. The researchers proposed method to migrate a system from Grid Security

Infrastructure to Kerbrose V5 security and emphasized on the need for designers of network security software to accommodate Generic Security Services Application Program Interface (GSSAPI).

Wenbo et al. [18] proposed identity based signcryption scheme to meet the requirement of cross-domain authentication in computational grid. Based on their proposed scheme, the reserachers presented identity based authentication model for multi-domain and mutual entity authentication. Although the proposed scheme is efficient in term of communication and computational cost, it has to battle with key distribution and management among participating entites

Ming, Z. & Renato, J. F. [19] presented a Secure Grid File System (SGFS) which supports GSI-based authentication and access control, end-to-end message privacy, and integrity. Ming, Z. & Renato, J. F. [19] used user-level virtualization of NFS to provide transparent grid data access leveraging existing, unmodified clients and servers. The researchers' method supports user and application-tailored security customization per Secure Grid File System session, and leverages secure management services to control and configure the sessions. The system conforms to the GSI grid security infrastructure and allows for seamless integration with other grid middleware. A SGFS prototype is evaluated with both file system benchmarks and typical applications, which demonstrates that it can achieve strong security with an acceptable overhead, and substantially outperform native NFS in wide-area environments by using disk caching.

2.1 Appraisal of Literature Review

The various methods employed to provide security in the grid required the use of key either in a symmetric or asymmetric algorithm. Several researchers have used Certificate Based Authentication (CBA) and Certificate-less Based Authentication (CLBA) for grid security. The key could be memorised or kept somewhere for safe keeping. However, the key can be compromised. Hence, this paper explores the use of biometric scheme for protecting the computational grid against unauthenticated and unauthorised users.

3. Proposed Design

This research proposes authentication protocol for computational grid based on biometric fingerprint technology. The method comprises of three phases, which are initialisation phase, registration phase and authentication phase.

3.1 Initialization Phase

In the initialisation phase, CA request a card for user U_i, the manufacturer accepts the request order from the CA, it writes various security parameter into the cards and then send the card to CA as follows:

step 1.1 manufacturer randomly selects a large prime number p and determines its root α

step 1.2 generates a unique Authentication Number *AN*.

step 1.3 randomly selects a 128-bit string *K* as a key for symmetric encryption and keep (p, α, *AN*, *K*) secret.

3.2 Registration Phase

In this phase, the user registers with the CA and receives a card once the user identity has been confirmed by the CA. The registration steps are as follows:

step 2.1 suppose user U_i with identity ID_i is to register. The user chooses a card password PW_i and stored to the card which is protected by the encryption mechanism of the card.

step 2.2 the fingerprint image of the user U_i is obtained via a sensor and the minutiae are extracted from this image to form a fingerprint template F_i. The F_i is split into two parts F_{iA} and F_{iB} where F_{iA} and F_{iB} represents part A and part B of the fingerprint template respectively.

step 2.3 computes $EA_i = h(F_{iA} \oplus AN)$, $EB_i = h(F_{iB} \oplus AN)$ and $HEF_i = h(EA_i \cup EB_i)$ where $\cup$ is concatenation operation and h is a one way hash function

step 2.4 the parameter $(ID_i, hEB_i,\ p, \alpha, K,\ HEF_i)$ is sent and saved in the server where hEB_i is the part B of the user's fingerprint template.

step 2.5 the parameter (ID_i, PW_i, hEA_i) is stored in the card where hEA_i is the part A of the user's fingerprint template.

3.3 Authentication Phase

In this phase, user insert card containing partial authentication parameter into card reader and a login request is sent to the server. The fingerprint information is checked as follows:

step 3.1 user U_i inputs its password PW_i, if the password is valid, then the authentication number (*AN*) is extracted otherwise the user request is rejected.

step 3.2 the user provides fingerprint via a sensor and the fingerprint is then compared with that stored on the authentication server. Let F_{i*} represents the fingerprint minutiae extracted by the sensor. F_{i*} is separated into F_{iA*} and F_{iB*} and then computes $EA_{i*} = F_{iA*} \oplus AN$ and $EB_{i*} = F_{iB*} \oplus AN$. The two parts are then merged to generate the full biometric template of the user i.e.

$HEF_{i*} = h(EA_{i*} \cup EB_{i*})$. Then the server sends EB_i for comparison purpose in order to verify the user. If a match is obtained i.e. $EB_{i*} = EB_i$ the user authentication is successful and proceed to next step otherwise it terminates.

step 3.3 This step uses Diffie-Hellman algorithm to establish a session key for key exchange. The client randomly selects a number $X_A < p$, then computes $Y_T = \alpha^{X_A} mod\, p$ and $Y_A = ID_i \parallel Y_T$ where α and p are both stored already on the card. The client then sends Y_A to the server. Similarly, the server randomly selects a number $X_B < p$, then computes $Y_B = \alpha^{X_B} mod\, p$ and sends Y_B to the client.

step 3.4 The client uses Y_B to compute the session key $SK = (Y_B)^{X_A}\, mod\, p$. Similarly the server uses Y_A to compute the common session key $SK = (Y_A)^{X_B}\, mod\, p$.

step 3.5 The server generates a one-time symmetric key RK, then computes $M = E_{sk}(EB_i \parallel RK)$, and then sends M to the client. $E_{sk}(.)$ denotes a symmetric encryption function such as DES based on the session key SK.

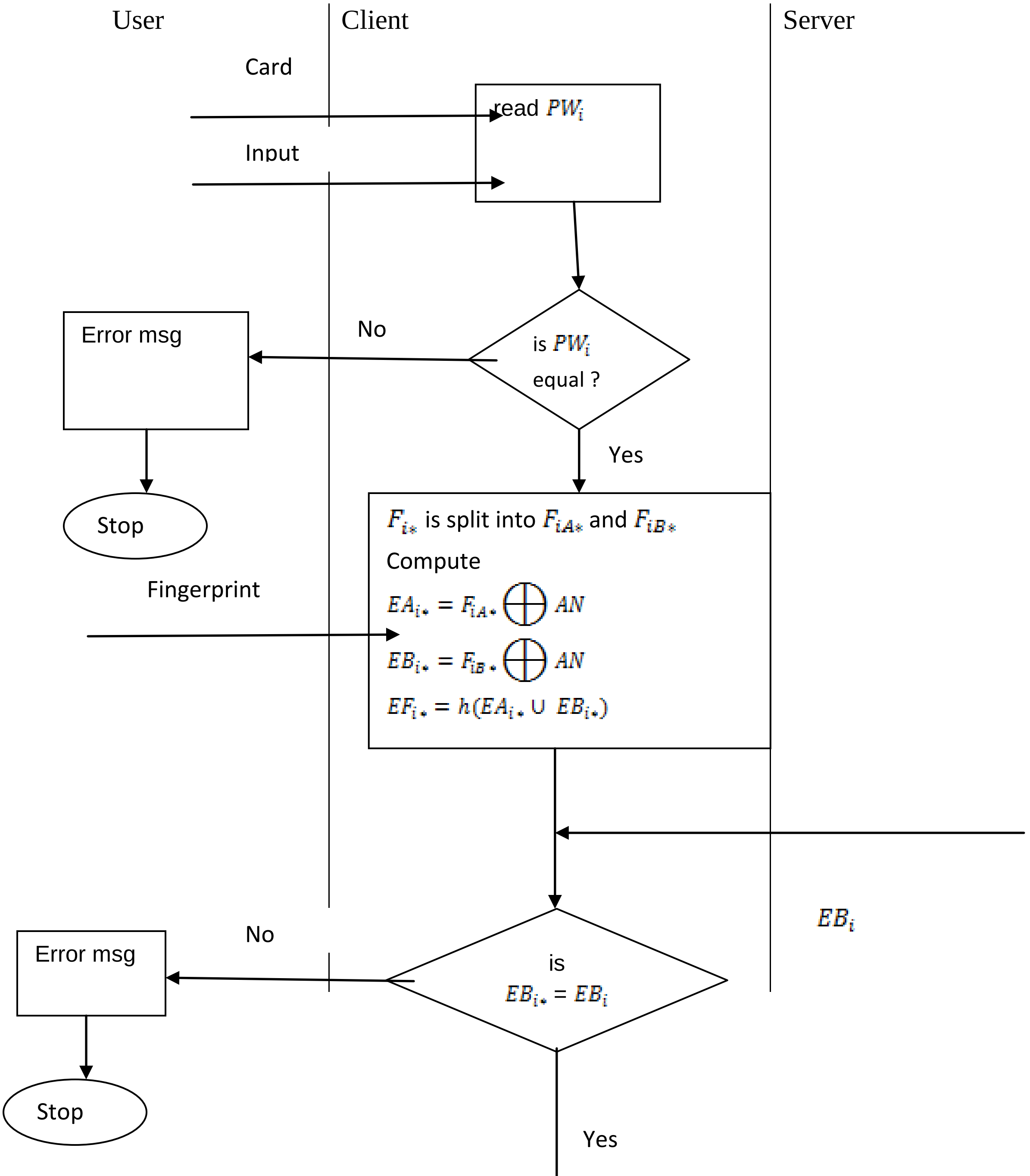
step 3.6 The client recover EB_i and RK by performing the decryption function $D_{sk}(M)$, and extract EA_i from the card. EA_i and EB_i are then merged to obtain $EF_i = EA_i \cup EB_i$. $D_{sk}(.)$ denotes a symmetric decryption function such as DES based on the session key SK.

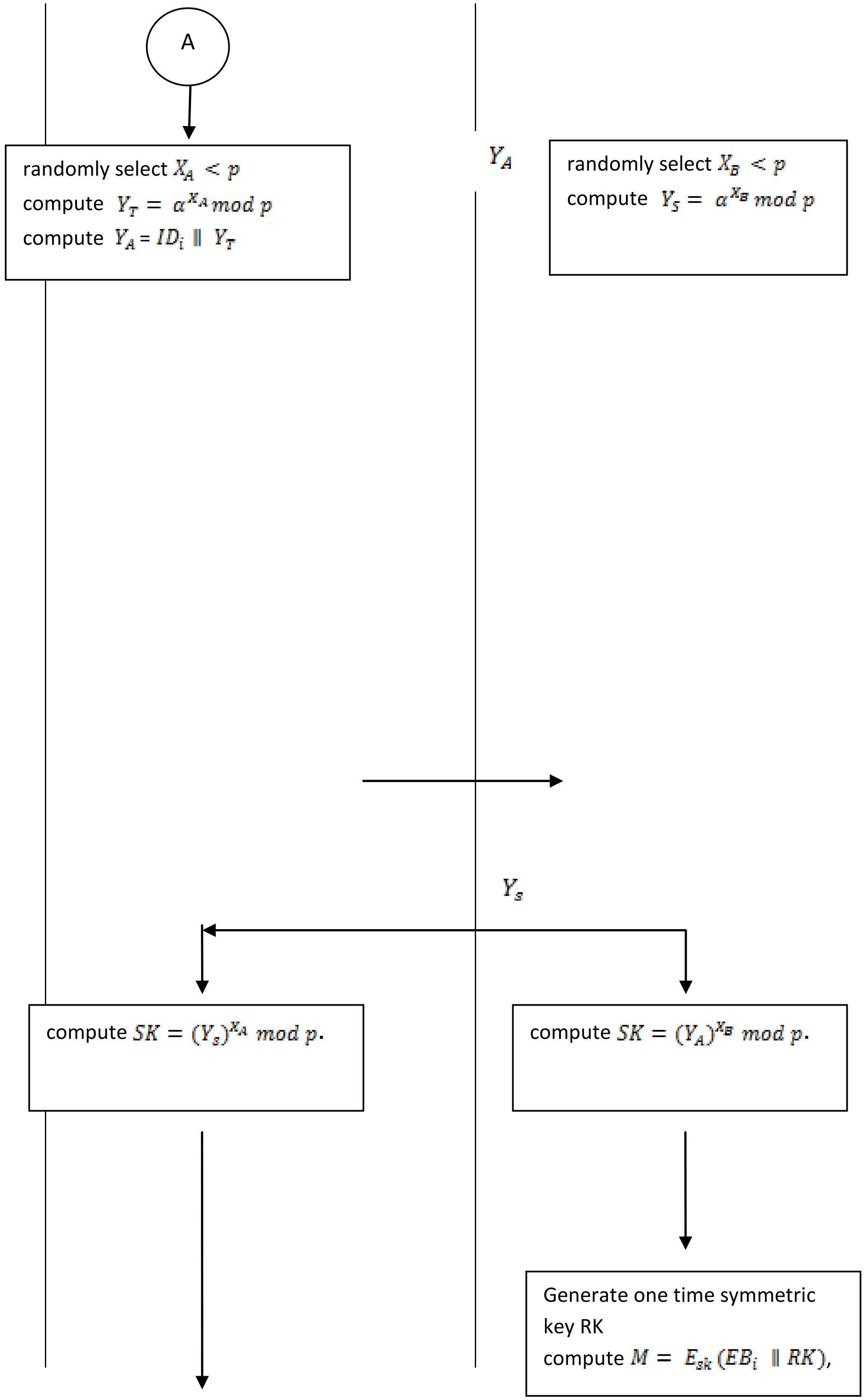
step 3.7 The client compares EF_i and EF_{i*}. If a match is obtained, the user is successfully authenticated else the client sends $RM = E_{Rk}(h(EF_i) \parallel CM)$ to the server for reconfirmation purposes. E_{Rk} is a symmetric encryption function based on the key RK and CM is a message indicating the matching result.

step 3.8 The server re-verifies the match $h(EF_i) = HEF_i$. If a match is obtained, the server accepts the login request of user U_i else it rejects the request.

3.4 Conceptual diagram of the proposed model

Below is the diagrammatic representation of the model outline above


User
Client
Server
Card
read PW_i
Input
No
Error msg
is PW_i equal ?
Yes
Stop
F_{i*} is split into F_{iA*} and F_{iB*}
Compute
$EA_{i*} = F_{iA*} \oplus AN$
$EB_{i*} = F_{iB*} \oplus AN$
$EF_{i*} = h(EA_{i*} \cup EB_{i*})$
Fingerprint
EB_i
No
Error msg
is $EB_{i*} = EB_i$
Stop
Yes


A
randomly select $X_A < p$
compute $Y_T = \alpha^{X_A} \mathit{mod}\ p$
compute $Y_A = ID_i \parallel Y_T$
Y_A
randomly select $X_B < p$
compute $Y_S = \alpha^{X_B} \mathit{mod}\ p$
Y_s
compute $SK = (Y_s)^{X_A}\ \mathit{mod}\ p$.
compute $SK = (Y_A)^{X_B}\ \mathit{mod}\ p$.
Generate one time symmetric key RK
compute $M = E_{sk}(EB_i \parallel RK)$,

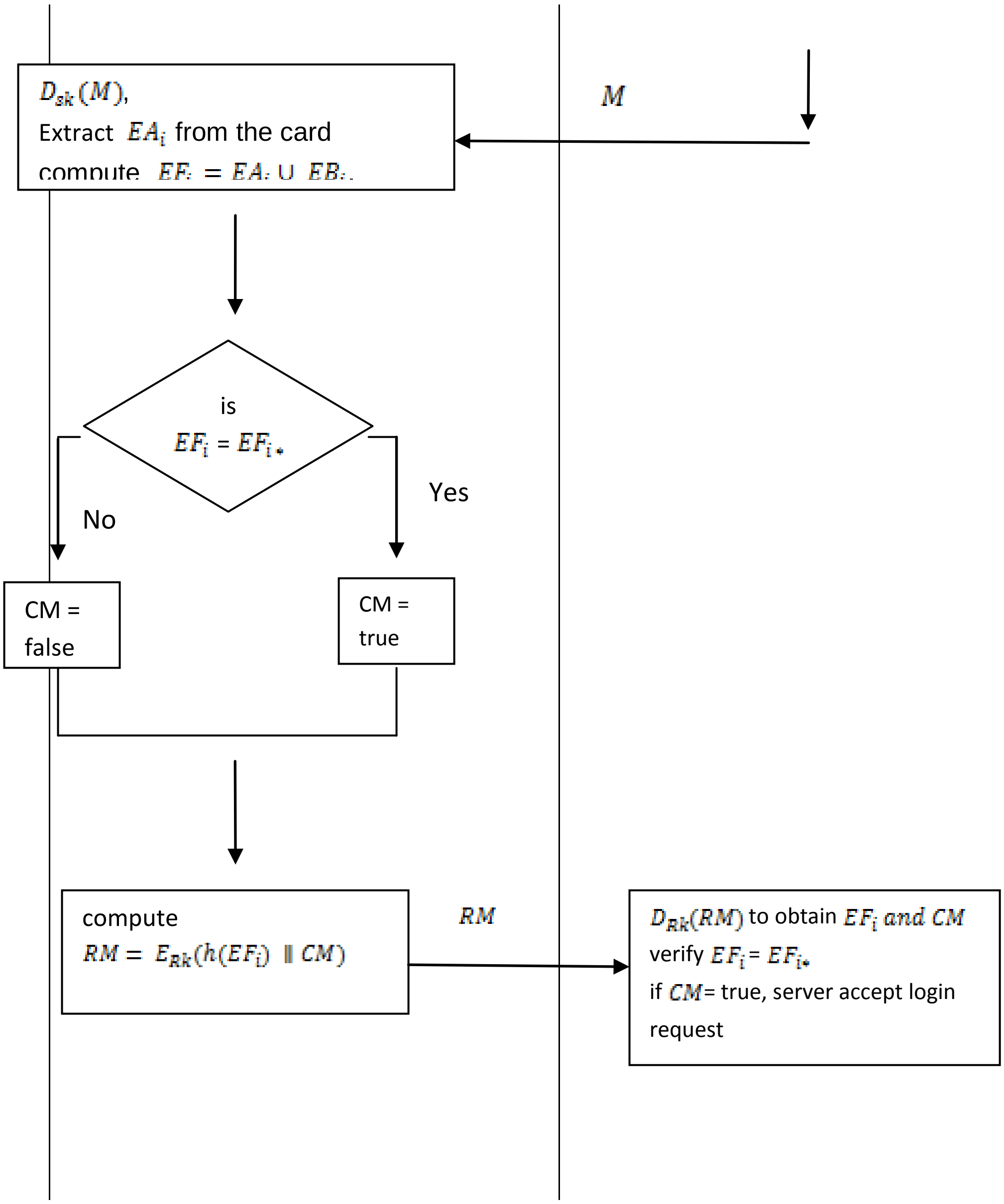

$D_{sk}(M)$,
Extract EA_i from the card
compute $EF_i = EA_i \cup EB_i$
M
is
$EF_i = EF_{i*}$
No
Yes
CM = false
CM = true
compute
$RM = E_{Rk}(h(EF_i) \parallel CM)$
RM
$D_{Rk}(RM)$ to obtain EF_i and CM
verify $EF_i = EF_{i*}$
if CM= true, server accept login request

Figure 1.1: Conceptual diagram of the proposed model

4. Analysis

An attacker attempting to attack the model will need the three factors used for the model i.e. the password, card and the fingerprint. The password and the card can be stolen but without the fingerprint, the attacker cannot succeed in his mission. The model separated the fingerprint into two parts, therefore the attacker cannot have the two separated parts from the card if stolen. It is extremely difficult for an attacker to obtain the three authentication parameters for a particular user and hence the model is safe. As explained that the fingerprint is separated into EA_i and EB_i and then encrypted before stored in a card and the server respectively, the user information and privacy is equally protected since the information are not in plaintext.

The model provide protection against network attack by the encryption of the data using 128-bit key symmetric algorithm and separation of the fingerprint stored in the card and the server. This provides adequate protection for the model. The use of Diffie-Hellman algorithm key exchange in the model provide protection for data when transmitted. The decryption process is further complicated by the fact that the session key is changed on periodic basis. The attacker also face the major challenge in determining the AN and the coding used to construct the partial authentication template EA_i.

5. Conclusion

This paper has presented an authentication model based on biometric fingerprint for computational grid security. The model has the advantage that the user chooses his own password for the card at will, the card and server store separate part of the whole fingerprint. The separate fingerprints are integrated when the users have successfully completed the login process in the authentication phase.

The model is robust toward authentication and network attacks. Therefore it provides efficient solution for enhancing the security of the grid computing.

References

[1] Ali, R. B., Sumalatha, A., Nirav, H. K., Rimato, F., Renato, F., & Jose, A. B Fine-Grain Access Control for Securing Shared Resources in Computational Grids, *Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS’02)*, IEEE *Computer Society*, (2002).

[2] Ian, F., Carl, K., Gene, T., & Steven, T., A Security Architecture for Computational Grids, *5th Conference on Computer and Communications Security*, San Francisco CA USA, ACM, (1998).

[3] Syed, I. A., Mustafizur, R., & Mukaddim, P., Policy Requirements to Ensure Security in Enterprise Grid Security Systems.

[4] Syd, C., Alistair, D., Peter, H. & Steven, N., OMII Grid Security Technology Overview, (2005).

[5] Ravi, D., An Introduction to biometric: A concise overview of the most important biometric technologies, *Keesing Journal of Documents & Identity*, **17**, (2006).

[6] Andrea, K. & Ziad, S., *Haptics and the Biometric Authentication Challenge, Advances in Haptics*, Mehrdad Hosseini Zadeh (Ed.), 2010, ISBN: 978-953-307-093-3, InTech, Retrieved 07 June, 2013 from: http://www.intechopen.com/books/advances-in-haptics/haptics-and-the-biometric-authentication-challenge

[7] Adewole, K.S., Abdulsalam, S.O. & Jimoh, R.G., Application of Voice Biometrics As An Ecological and Inexpensive Method of Authentication, *International Journal of Science and Advanced Technology*, **1**(6), (2011), 196-201.

[8] Jaspher, W. K., & Kirubakaran, E., Biometric Authentication and Authorization System for Grid Security, *International Journal of Hybrid Information Technology*, **4**(4), (2011), 43-58.

[9] Hisham and Khaled., A New Accelerated RC4 Scheme Using Ultra GradSec and HIMAN and use this Scheme to secure HIMAN data, *5th International Conference on Information Assurance and Security*, (2009).

[10] Ratha, N. K., Connell, H. J., & Bolle, R. M., Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal*, **40**(3), (2001).

[11] Baolin, M., Jizhou, S., & Ce, Y., Reputation-based Trust Model in Grid Security System, *Journal of Communication and Computer*, **3**(8), (2006).

[12] Sindhuja, R., Varsha, P., & Sumathi, G., An Improved ID Based Entitled Verifier Cryptography for Grid Systems, *International Journal of Recent Trends in Engineering*, **2**(1), (2009), 68-72.

[13] Shengbao, W., Zhenfu, C., & Haiyong, B., Efficient Certificateless Authentication and Key Agreement (CL-AK) for Grid Computing, *International Journal of Network Security*, **7**(3), (2008), 342-347.

[14] Marty, H., Mary, R. T., & Keith, R. J., Security for Grids, *Proceedings of the IEEE*, **93**(3), (2005).

[15] Safieh, S., Amir, M. R., & Mehran, M., Proposed platform for improving grid security by trust management system, *International Journal of Computer Science and Information Security*, **6**(1), (2009), 143-148.

[16] Ruckmani, V., & Sadasivam, S. G., A novel trigon-based dual authentication protocol for enhancing security in grid environment, *International Journal of Computer Science and Information Security*, **6**(3), (2009), 64-72.

[17] Patrick, C. M., Wilbur, R. J., & Richard, J. D., Adapting Globus and Kerberos for a Secure ASCI Grid, *Association for Computing Machiner*, (2001).

[18] Wenbo, Z., Hongqi, Z., Bin, Z., & Yan, Y., An Identity-Based Authentication Model for Multi-Domain in Grid Environment, *International Conference on Computer Science and Software Engineering*, (2008), 165-169.

[19] Ming, Z., & Renato, J. F., *A User-level Secure Grid File System*, 2007.