RSA AUTHENTICATION MECHANISMS IN CONTROL GRID COMPUTING ENVIRONMENT USING GRIDSIM TOOLKIT

Saiful Adli Ismail[1], Md Asri Ngadi[2], Johan Mohd Sharif[2], Mohd Nazri Kama[1] and Haslina Sarkan[1]

[1]Advanced Informatics School, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, saifuladli@utm.my, mdnazri@utm.my, haslinams@utm.my
[2]Faculty of Computing, Universiti Teknologi Malaysia, Malaysia, dr.asri@utm.my, johan@utm.my

ABSTRACT. There are security concerns when our sensitive data is placed in the third party infrastructure such as in the Grid Computing environment. As such, it is difficult to be assured that our data is in the safe hands. Thus, authentication has become the most critical factor pertaining to this. There are several approaches has been discussed in the grid computing environment on the safeguard, scalable and efficient authentication that are either Virtual Organization centric or Resource centric. Most of the grid computing uses public key infrastructure (PKI) to secure the identification, but the vulnerability are still cannot be avoid. In order to satisfy the security need of grid computing environment, we design an alternative authentication mechanism using RSA algorithm to ensure the user identification, and carry out the experiment in the Gridsim toolkit simulator.

Keywords: grid computing, RSA, authentication, public key infrastructure (PKI), gridSim

INTRODUCTION

Grid computing has been growing and fitting as a common platform for many consumers. Virtual organization (VO) in a grid basically gathers as well as incorporates computing and data resources from different bodily organization for instance commercial companies, scientific libraries and academic institution. Thus, budding a reliable and effective access control mechanism for Grid is essential (Park & Chung, 2009). Most Certificate authority (CA) in a traditional public key cryptosystem (PKC) has to store large amounts of public key certificates, real-time public key certificate has to be transmitted and stored in the signature verifying process, which will raise unnecessary waste of bandwidth and time delay. In addition, identity-based authentication protocol does not demand to store big quantities of public key credentials, but key escrow becomes an inevitable problem, because the user's private key is generated by the key generation center (KGC).

To overcome the aforesaid problem, (Al-Riyami & Paterson, 2003) proposed certificate less public key cryptosystem (CL-PKC) in 2003. The KGC generates user's partial private key instead of whole private keys. Many certificate less signature schemes (Gorantla & Saxena, 2005; Liu, Au, & Susilo, 2007; X. Li, Chen, & Sun, 2005; Xiong, Qin, & Li, 2008; Yap, Heng, & Goi, 2006; Zhang & Mao, 2012; Zhang, Wong, Xu, & Feng, 2006) have been proposed, but some of them (Gorantla & Saxena, 2005; Liu et al., 2007; Li et al., 2005; Xiong

et al., 2008; Yap et al., 2006; Zhang & Mao, 2012; Zhang et al., 2006) suffer from the public key replacement attack, the other certificate signature schemes have short signature length and can provide higher computational efficiency (Zhang, Yao, Wang, & Takagi, 2013). Established along the design idea of little signature, we propose an authentication mechanism that carries the characteristics of public key replacement attack resistance as well as high computational efficiency. The new mechanisms provide mutual authentication and non-repudiation.

RELATED WORKS FROM THE PAST

There are many access controls from previous researches such as Attribute-based access control (ABAC), where Identity Providers responsibility to giving the related attributes. As such they authenticate in the VO their members and create the attributions declaration consecutively to deliver the essential identity information to assist on making authorization decision made by the resource and service provider (Park & Chung, 2009). Other than that, there is Policy-based access control, in which Globus Toolkit (GT2) mechanism is used; it is a resource management mechanism (Jin Wu, Leangsuksun, Rampure, & Hong Ong, 2006).

In 1984 Adi Shamir introduced the concept of Identity based Cryptography (IBC) and offered a signature scheme (Shamir, 1984). After 17 years, (Boneh & Franklin, 2001) in 2001 have proposed IBE from the Weil pairing which is more secure and practical. In 2002 (Gentry & Silverberg, 2002) proposed hierarchical IBC scheme and signature schemes. By default, authentication of users in the architecture of grid computing is using PKI certificates where weaknesses in the single point of Certificate Authentication (CA) server failure or compromise. Certificate management is very complex and throws a poor scalability, which determines the number of sessions of protocol 2 in GSI (Li & Sun, 2007; Mao, 2004a). Thus, the evolution of the use of IBC / PKI in a grid computing architecture is introduced by (Lim & Robshaw, 2004), in 2004 as an appropriate hierarchical IBC in grid environment. In the same year (Mao, 2004b) introduced the Identity-based non-interactive authentication framework for grid computing where, this framework is a certificate-free and show significant performance improvement.

In 2005, Lim H. W. and Robshaw propose hybrid approach combining IBC at the user level and PKI above the user level (Lim & Robshaw, 2005). This approach resolves the key escrow, but lose non-interactive authentication and certificate-free. In 2007 Chen, L. et al revisit grid security infrastructure (GSI) in the GT2 and improved the GSI architecture and protocol by proposing an alternative authentication framework (Chen, Lim, Mao, & others, 2007). The framework proposes by Chen, L., is still using certificate to do the authentication. Again in 2007 (Li & Sun, 2007) has proposed identity-based architecture for grid (IBAG) and identity- based authentication protocol. Later in 2008 (Zhang, Zhang, Zhang, & Yang, 2008) proposed identity-based signcryption scheme to meet cross-domain authentication. However, the architecture proposed and authentication mechanism is still not clear on how it to be implemented and the Certificate Authority (CA) are still not disappearing thoroughly. In this paper, we present our work on introducing RSA authentication mechanisms to secured user identification into the Gridsim simulation toolkit.

GRIDSIM ARCHITECTURE AND COMPONENT

GridSim is design as a multi layer architecture for extensibility, as shown in Figure 1 (Sulistio, Cibej, Venugopal, Robic, & Buyya, 2008). This allows new components or layers to be added and integrated into GridSim easily. In addition, the layered GridSim architecture captures the model of the Grid computing environment. GridSim is based on SimJava2, a general purpose discrete-event simulation package implemented in Java. Therefore, the first

layer at the bottom of Figure 1 is managed by SimJava2 for handling the interaction or events among GridSim components (Simatos, 2002). Therefore, SimJava2 manages the first layer at the bottom of Figure 1 for handling the interaction or events among Gridsim component.

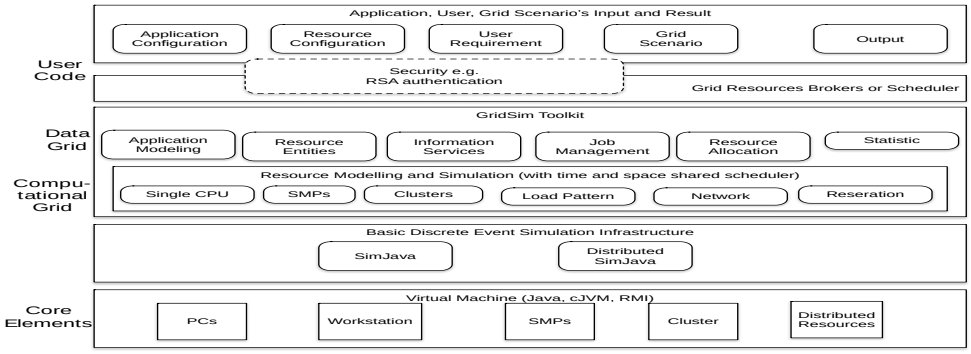

Figure 1. Gridsim Architecture with security layer

All components in GridSim communicate with each other through message-passing operations defined by SimJava. The second layer models the core elements of the distributed infrastructure, namely Grid resources such as clusters, storage repositories, and network links. These core components are utterly indispensable to create simulations in GridSim. The third and fourth layers are concerned with modeling and simulation of services specific to computational and data Grids, respectively.

In case of Data Grids, job management also incorporates managing data transfers between computational and memory resources. Replica catalogs, data services for files and data, are also specifically implemented for Data Grids. The fifth layer contains components that aid users in implementing their own schedulers and resource brokers so that they can examine their own algorithms and strategies.

METHODOLOGY

This section explains an operational framework used in conducting this research. The methodology is a set of procedures or methods used to conduct the research. The research strategy, design explains how the whole experimentation will be conducted is outlined. It is then followed by the detailed explanations of each phases involved in this research strategy. Each phase consists of outcomes that feed into the next phase of the research strategy.

There are three major phases that compose to three major strategies of the task:

Phase1: Reviewing current Grid Computing authentication framework implementation.

This phase analyses current implementation of Grid Computing authentication framework. After that, an analysis of current practice of implementation of Grid Computing authentication framework development phase is then conducted. In this phase, focused on authentication time for users to authentication server (e.g., broker, certificate authority (CA) and single-sign on server), communication time and computation time. A matrix will be developed to match or tailor between the security and performance of existing and current authentication framework.

Phase2: Designing and implementing a prototype version of the RSA authentication framework.

Based on the list of existing and current authentication framework mechanisms, a new authentication framework will then be designed and implemented. This phase will use a small

set of data, such as users, routers, network and resources as an input for Gridsim simulator using Java program as an initial implementation.

Phase3: Evaluating an RSA authentication framework using Gridsim simulator.

The evaluation will use the existing and current authentication framework parameter to be compared to the developed prototype authentication framework. A controlled Grid Computing authentication framework will be conducted in a simulation environment using the GridSim simulator with Java programming.

IMPLEMENTATION RSA AUTHENTICATION MECHANISM IN GRIDSIM

Rivest, Shamir, & Adleman, (1978) originally proposed the RSA algorithm construction at MIT 1978 conferences. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In this section, we describe the implementation of RSA authentication mechanisms in GridSim toolkit.

WHY GRIDSIM?

There are numerous Grid simulators that provide various functionalities. Based on (Klusáček, Matyska, & Rudová, 2008; Klusáček & Rudová, 2010) articulated that Bricks is designed for simulation of client server architectures in Grid computing, SimGrid is used for the simulation and development of distributed applications in heterogeneous and distributed environment. Simbatch allows evaluating scheduling algorithms for batch schedulers and MicroGrid can be used for systematic study of the dynamic behavior of applications, middleware, resources, and networks. In this work, our simulator is a Java based simulator GridSim toolkit. This toolkit is flexible and universal and it delivers really good documentation. It also provides functionality to simulate the basic Grid computing environment and its behavior. GridSim provides a simple implementation of common entities such as computational resources or users and also allows to simulate simple jobs, network topology, data storage and others useful functionalities.

RSA AUTHENTICATION NETWORK ARCHITECTURE

In this section, we briefly describe RSA authentication mechanism network architecture. From the Figure 2 we can see that RSA authentication network architecture is composed of three entities, which are users, broker server and resources. The authentication is done, as depicted in Figure 2 where it's called asymmetric key cryptography because the key used for performing encryption and decryption are different and are normally referred to as public and private keys.

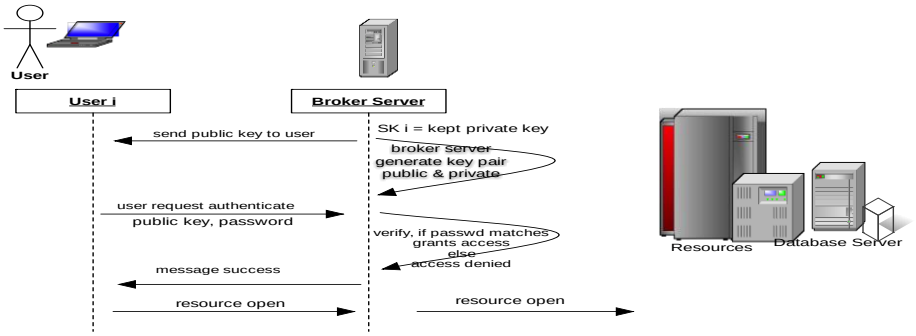

Figure 2. RSA Authentication mechanism

Firstly, broker server generated pair key such as public and private key. The broker server kept the private key and sends the public key to the grid users. The authentication process begins with a user authenticate to the broker server with password encrypted with the public key that corresponds to the pair key generated by broker server. Secondly, the broker server decrypted the user password and verifies the password. If the password matches, the broker server grants access to the network to use the resources. If not, access is denied.

Finding

The platform for simulation experiment is GridSim, which is based on Java. Since GridSim is based on SimJava which is a discrete event simulation tool, and simulates various entities by multiple thread. This aligns well with the grid-computing environment. In a simulation environment special users and resources can be generated by reconfiguring these interfaces and connected the network link through two routers.

The experiments were performed on Intel Core i7 2.9GHz machine with 8GB 1600MHz DDR3 RAM. The tests were run for a different number of available machines with different CPU ratings. We have run tests for 100 jobs with release dates, RSA authentication time, computation time, communication time and authentication time. All the data are generated into log file using log4j in Java after running the simulation. The output file is depicted in figure 3

```
2014-04-27 23:48:34,230  - Starting Log
2014-04-27 23:48:36,418  - (type,usr,compcost,simtime),RSA,33,25.0,70.0
2014-04-27 23:48:36,418  - (type,usr,authcost,simtime),RSA,33,5.0,70.0
2014-04-27 23:48:36,418  - (type,usr,commcost,simtime),RSA,33,4.0,70.0
2014-04-27 23:48:36,421  - (type,usr,compcost,simtime),RSA,29,25.0,70.0
```

Figure 3. RSA log file

In this experiment we create one scenario where the total grid users are 5 to simulate the concurrent request and uniformly distributed them among the two trust resources. In our simulation setup, some parameters are set identically for all network elements, such as the maximum transfer unit (MTU) of a link and the latency. The detail parameter of the simulation in the experiment is shown in table 1 below.

Table 1. Simulation Parameter

Parameter	Value
Number of users	5
Number of resources	2
Number of gridlet	100
Baud rate	1000 bits/sec
Propagation delay	10 ms
MTU	1500 bytes

Result Analysis and Simulation

In this section, we analyses average RSA authentication performance is firstly discussed. Then simulation experiment gives precise result.

Authentication Cost

For this experiment, the execution of authenticated users from the user to the resources through broker server has been done. The figure 4 indicates that the result starts at 2.8 milliseconds and drop significantly to 1.5 milliseconds. This is due to the fluctuation of the processor CPU time. After that the average of RSA authentication time is around 1.55 milliseconds per simulation time.

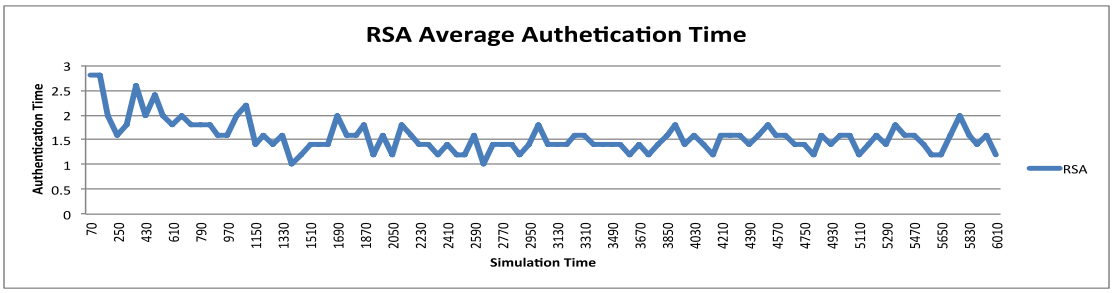

Figure 4. Authentication cost vs Simulation time

Communication Cost

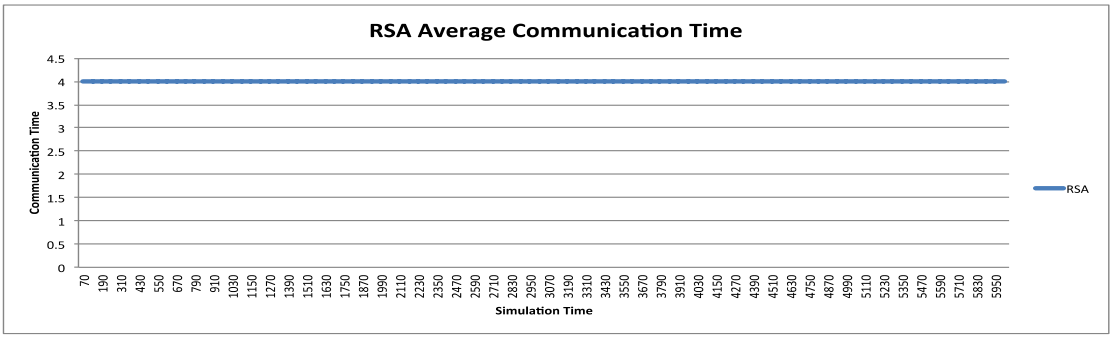

Figure 5. Communication Cost vs Simulation time

Based on Figure 5, it was found that average communication cost from the user to the resource would take around 4 millisecond over simulation time. We can see that the result shown in the simulation is significantly fast.

Computation Cost

As a result, execution computation cost time; the average time for RSA computation time for task on each 5 users is shown in Figure 6. The graph illustrates the average computation time for RSA is approximately 25 milliseconds.

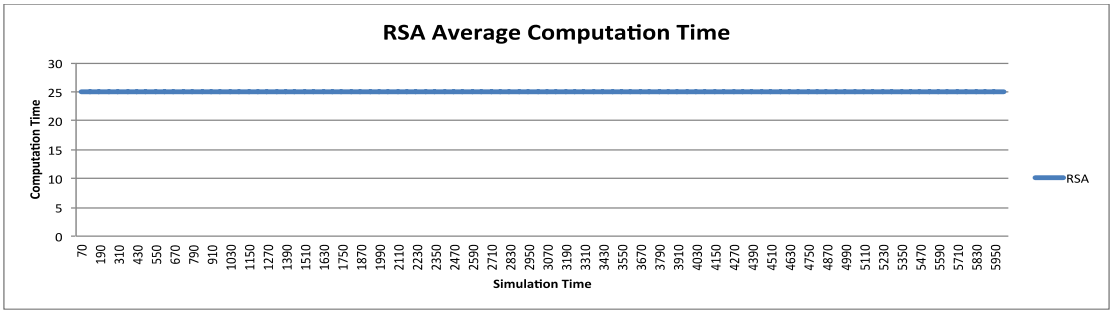

Figure 6. Computation Cost vs Simulation time

CONCLUSION

In conclusion, in this paper we are proposing a security in grid computing simulation to be implemented in authentication administration of grid computing environment as an extension to GridSim simulator. With this extension, GridSim has the ability to handle basic Grid security functionality. The most important point to implement this is the ability to control user management in a virtual organization (VO), whereas to protect the final manage of permission to share resources by the resource provider. In summation, we test the average communication time between users to resources through broker, computation time in the server and authentication time from server or broker. The result shown in this experiment are not very surprising, but the describe simulation was used as an example of the different functionality of the simulator. We hope that this study can help researcher make an important finding and help solve problems arising in data grid computing security. In the future, we are contriving to look at the other authentication mechanism comparison with other crypto algorithm such as DSA, HMAC ECC and IBI in a control grid computing environment using the GridSim toolkit simulator.

ACKNOWLEDGMENTS

We would like to thank to Universiti Teknologi Malaysia (UTM) and Ministry of Education Malaysia for their financial support. Also to Advanced Informatics School and Faculty of Computing staffs that have been involved in the study.

REFERENCES

Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In *Advances in Cryptology-ASIACRYPT 2003* (pp. 452–473). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-40061-5_29

Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. In J. Kilian (Ed.), *Advances in Cryptology — CRYPTO 2001* (Vol. 2139, pp. 213–229). Springer Berlin / Heidelberg. Retrieved from http://dx.doi.org/10.1007/3-540-44647-8_13

Chen, L., Lim, H. W., Mao, W., & others. (2007). User-friendly grid security architecture and protocols. *Lecture Notes in Computer Science*, 4631, 139.

Gentry, C., & Silverberg, A. (2002). Hierarchical ID-Based Cryptography. In *Advances in Cryptology — ASIACRYPT 2002* (pp. 149–155). Retrieved from http://dx.doi.org/10.1007/3-540-36178-2_34

Gorantla, M. C., & Saxena, A. (2005). An Efficient Certificateless Signature Scheme. In Y. Hao, J. Liu, Y.-P. Wang, Y. Cheung, H. Yin, L. Jiao, … Y.-C. Jiao (Eds.), *Computational Intelligence and Security* (pp. 110–116). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/11596981_16

Jin Wu, Leangsuksun, C. B., Rampure, V., & Hong Ong. (2006). Policy-Based Access Control Framework for Grid Computing (pp. 391–394). IEEE. http://doi.org/10.1109/CCGRID.2006.80

Klusáček, D., Matyska, L., & Rudová, H. (2008). Alea–Grid scheduling simulation environment. In *Parallel Processing and Applied Mathematics* (pp. 1029–1038). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-68111-3_109

Klusáček, D., & Rudová, H. (2010). Alea 2: job scheduling simulator. In *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques* (p. 61). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). Retrieved from http://dl.acm.org/citation.cfm?id=1808220

Li, H., & Sun, S. (2007). Identity-Based Cryptography for Grid. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007. SNPD 2007. Eighth ACIS International Conference on (Vol. 2).

Lim, H. W., & Robshaw, M. J. B. (2004). On Identity-Based Cryptography and Grid Computing. In *Computational Science - ICCS*, 474–477.

Lim, H. W., & Robshaw, M. J. B. (2005). A Dynamic Key Infrastructure for Grid. *Lecture Notes in Computer Science*, 3470, 255.

Liu, J. K., Au, M. H., & Susilo, W. (2007). Self-Generated-Certificate Public Key Cryptography and Certificateless Signature/Encryption Scheme in the Standard Model: Extended Abstract. In *Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security*, 273–283. New York, NY, USA: ACM. http://doi.org/10.1145/1229285.1266994

Li, X., Chen, K., & Sun, L. (2005). Certificateless signature and proxy signature schemes from bilinear pairings. *Lithuanian Mathematical Journal*, 45(1), 76–83. http://doi.org/10.1007/s10986-005-0008-5

Mao, W. (2004a). An identity-based non-interactive authentication framework for computational grids. *Technical Report HPL-2004-96*. Hewlett-Packard Laboratories.

Mao, W. (2004b). An identity-based non-interactive authentication framework for computational grids. *Technical Report HPL-2004-96*. Hewlett-Packard Laboratories.

Park, S. M., & Chung, S. M. (2009). Privacy-preserving attribute distribution mechanism for access control in a grid. In *21st International Conference on Tools with Artificial Intelligence*, ICTAI'09, 308–313. IEEE.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology*, 47–53.

Simatos, C. (2002). Making simjava count. *MSc. Project Report*. The University of Edinburgh.

Sulistio, A., Cibej, U., Venugopal, S., Robic, B., & Buyya, R. (2008). A toolkit for modelling and simulating data Grids: an extension to GridSim. *Concurrency and Computation: Practice and Experience*, 20(13), 1591–1609. http://doi.org/10.1002/cpe.1307

Xiong, H., Qin, Z., & Li, F. (2008). An Improved Certificateless Signature Scheme Secure in the Standard Model. *Fundamenta Informaticae*, 88(1), 193–206.

Yap, W.-S., Heng, S.-H., & Goi, B.-M. (2006). An Efficient Certificateless Signature Scheme. In X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, … C.-Z. Xu (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing* (pp. 322–331). Springer Berlin Heidelberg.

Zhang, J., & Mao, J. (2012). An efficient RSA-based certificateless signature scheme. *Journal of Systems and Software*, 85(3), 638–642. http://doi.org/10.1016/j.jss.2011.09.036

Zhang, M., Yao, J., Wang, C., & Takagi, T. (2013). Public Key Replacement and Universal Forgery of SCLS Scheme. *International Journal of Network Security*, 15(1), 115–120.

Zhang, W., Zhang, H., Zhang, B., & Yang, Y. (2008). An Identity-Based Authentication Model for Multi-domain in Grid Environment. In *International Conference on Computer Science and Software Engineering*, 3, 165–169. Los Alamitos, CA, USA: IEEE Computer Society. http://doi.org/http://doi.ieeecomputersociety.org/10.1109/CSSE.2008.1281

Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006). Certificateless Public-Key Signature: Security Model and Efficient Construction. In J. Zhou, M. Yung, & F. Bao (Eds.), *Applied Cryptography and Network Security* (pp. 293–308). Springer Berlin Heidelberg.