Enforcing anti-breaching of Security in Cloud Computing by Applying multiple Methodologies to enhance protection of Cloud based Grids/Servers

Ihssan Alkadi

Ghassan Alkadi

Kuo-Pao Yang

Matthew Gill

Department of Computer Science & Industrial Technology
Southeastern Louisiana University
Hammond, LA 70042, USA

Abstract

This paper covers introduction of new methodologies that will enforce cloud computing security against breaches and intrusions. The business benefits of cloud computing, and the cloud architecture and its major components is that it orchestrates many different usages for the governmental. Educational and business sectors. This paper will also give the readers an insight on companies using cloud computing technology. In addition, the paper will discuss the future outlook for cloud computing based on leading IT. Much light will be shed on existing methodologies of security on Grid/Servers used for cloud computing and storage of databases. A several methods will be presented in addition to the already existing methods of security in Grids/Server cloud-based systems.

Keywords: *Cloud, Cloud Computing, Security, Web 2.0, Biometrics*

Overview

The term "*Cloud*" has been around since the early 1960's. John McCarthy was the first person to propose it. Later on, with the introduction of Google, Yahoo, and Web 2.0 (Facebook, YouTube, LinkedIn, Twitter, and MySpace) in the 1990s people then started their particular interest in the term the "C*loud*". In 2006 the term "*Cloud Computing*" was launched and research started to expand in this topic. As [1] defines the term as "*Cloud computing is a specialized form of distributed computing that introduces utilization models for remotely provisioning scalable and measured resources*." So the Cloud is mainly an IT virtualization setting and network that is accessed remotely with resources in a scalable manner. [2] Refers to Cloud computing as "Pay as you go". It is a self-service on demand which the user can provision computing capabilities without having to interact with a human. So Sever software does not have to be installed on your machine. It also allows greater [2] "Broad Network Access". The Cloud also allows resource pooling. Resources can be shared and accessed without having to have you in a special physical location or install special software to access them. [2] Refers to Rapid Elasticity in the Cloud since at peak times the Cloud excels at that. The elasticity expectation rests on the cloud provider to locate and allocate resources on the cloud servers so that the application software locally can do its job. It can handle the load of access and there are enough algorithms that preside on the Cloud server to handle such incredible requirements not as like Busy or try again. The Internet allows you to open access to lot if sites while cloud is usually are privately owned. So people still have issues in comparing the term "*Grid Computing*" with "*Cloud Computing*". Grid Computing became a desirable and popular in the 1990's where you combine a pool of high performance and loosely coupled resources such as networked powerful computers with a sophisticated number of CPU's and hardware that will help in resilient computing. Cloud computing is a descendant of the previous model of Grid Computing. In the Cloud model you have a Cloud provider, Cloud consumer, and a cloud service owner. The cloud provider is the organization that writes the ***SLA* (*S*ervice *L*evel *A*greement)** to make the Cloud resources available to the Cloud consumer is the organization that accesses the resources remotely on the cloud. *Cloud* is used to reduce Costs, elevate scalability, increase performance, availability and reliability. While the cloud service owner can be either one. So what is exactly is benefited from the Cloud? 1) On-demand Access, 2) ubiquitous usage, 3) scalability, 4) flexibility, 5) Reduce costs, 6) convenience 7) portability and access time reduction, 8) higher productivity, 9) Rapid Elasticity, and 10) Resource Pooling, 11) Faster implementation, 12) Energy Efficiency, 13) Geographic Distribution, 14) Massive storage and scale, 15) Resilient computing, and lastly 16) Homogeneity

The Cloud delivery models are *IaaS, PaaS*, and *SaaS*. IaaS is Infrastructure-as-a-service, PaaS is platform-as-a-service, and SaaS is Software-as-a-service. The IaaS is the IT hardware and middleware, resources, the IT environment that are packaged into the virtual cloud. The PaaS is the engine providing the hosting and the as "ready-to-use", [1] environment and back end. SaaS are the services and software such as LinkedIn and Facebook on the Cloud.

The Cloud installation and use differ primarily by ownership, size, access, and environment. The types of Cloud deployment are: 1) Public Cloud where it is a third party Cloud services, 2) Community Cloud is a Cloud services that is public but limited to certain companies/individuals, 3) Private Cloud is owned by a single organization, and 4) Hybrid Cloud is a combination of two or more different deployment models. Risks in using the cloud are incremental security holes and control which poses a threat to the cloud being accessed, and reliable. We next discuss the advantages of current security methods enforced.

Advantages to Current Methodologies

In current securities advantages in the Cloud are: 1) Confidentiality, 2) Integrity, 3) Authenticity, 4) and Availability. It is accomplished through 1) Symmetric Encryption, 2) Asymmetric Encryption, 3) Hashing, 4) Digital Signature, and 5)

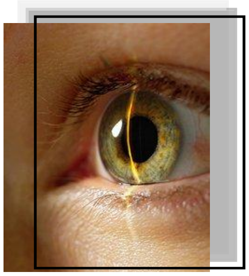
Public Key Infrastructure (***PKI***). The latest methodology that exists is the ***I***dentity and ***A***ccess ***M***anagement (IAM). It has four components: 1) Authentication, 2) Authorization, 3) User management, and 4) Credential management. Also, there is ***S***ingle ***S***ign-***O***n (SSO). X.805 [2] Has concerns with 1) Management Plane Security Objectives of availability Dimension, 2) Control Plane Security Objectives of availability Dimension, and 3) End User Plane Security Objectives of availability Dimension. Access control, network security policies and scope can keep threats at bay currently with the status of the cloud.

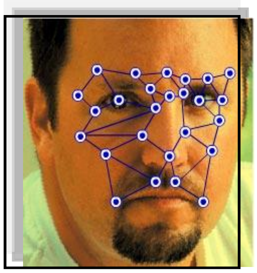
Disadvantages to Current Methodologies

Current Cloud suffers from: 1) Threats, 2) Risk, 3) Security Controls, 4) and Breaches. The type of current Methodologies that deal with simply a user Id and passwords and possibly random security questions that are preset you would have a: 1) Anonymous Attacker, 2) Malicious Service Agent, 3) 4) Trusted attacker, 5) Malicious Insider, 6) Traffic Eavesdropping, 7) Malicious Intermediary, 8) DoS Denial of Service, 9) insufficient Authorization, 10) Virtualization Attack, and 11) Overlapping Trust Boundaries [1]. Also, there is the reduced operational control and visibility and reduced provisioning of computation at the source of the cloud. Currently, Denial of service attacks and Destruction of information or other resources as well as interruption of services are the most fearful blows to the Cloud. Currently, the cloud existing on Amazon, Google, Microsoft, File Locker, iCloud, and Dropbox use ***I***ntrusion ***D***etection/***P***revention ***S***ystems *(IDPS)*. We recommend our own methodology next.

Suggested Methodologies: The Cloud **Mist**.

We present the Cloud Mist. We named it a Mist since it involves a various types of security methodologies. The first three techniques are being used and suggested in many books and articles on the internet. First we recommend the Eye retina scan before accessing a cloud server or account. Second we can use the pin number on a touch screen before accessing your sign on screen. See figures1 & 2 below. Third, we suggest using the facial recognition software. It is now available in many computers for sale these days. All previous methods are being used nowadays so there is nothing new here but using them can beef up the security of using biometrics to make sure that the cloud server does not get accessed by wrong hackers. So walking to a IT room or online trying to access a Cloud account can be stopped by the above three methods. So DoS attacks can be limited with the first line of defense utilized by the above three methods. Sometimes budgets and finances will play role in limiting the biometrics technology use that is why we will present our unique and new methods of adding security to the accessing of the Cloud server or account. The techniques suggested here can be easily setup so it can beef up security in companies and governmental sites. Some of them are being used already. It is a matter of budgeting and having to revamp the IT infrastructure to accommodate the technology.





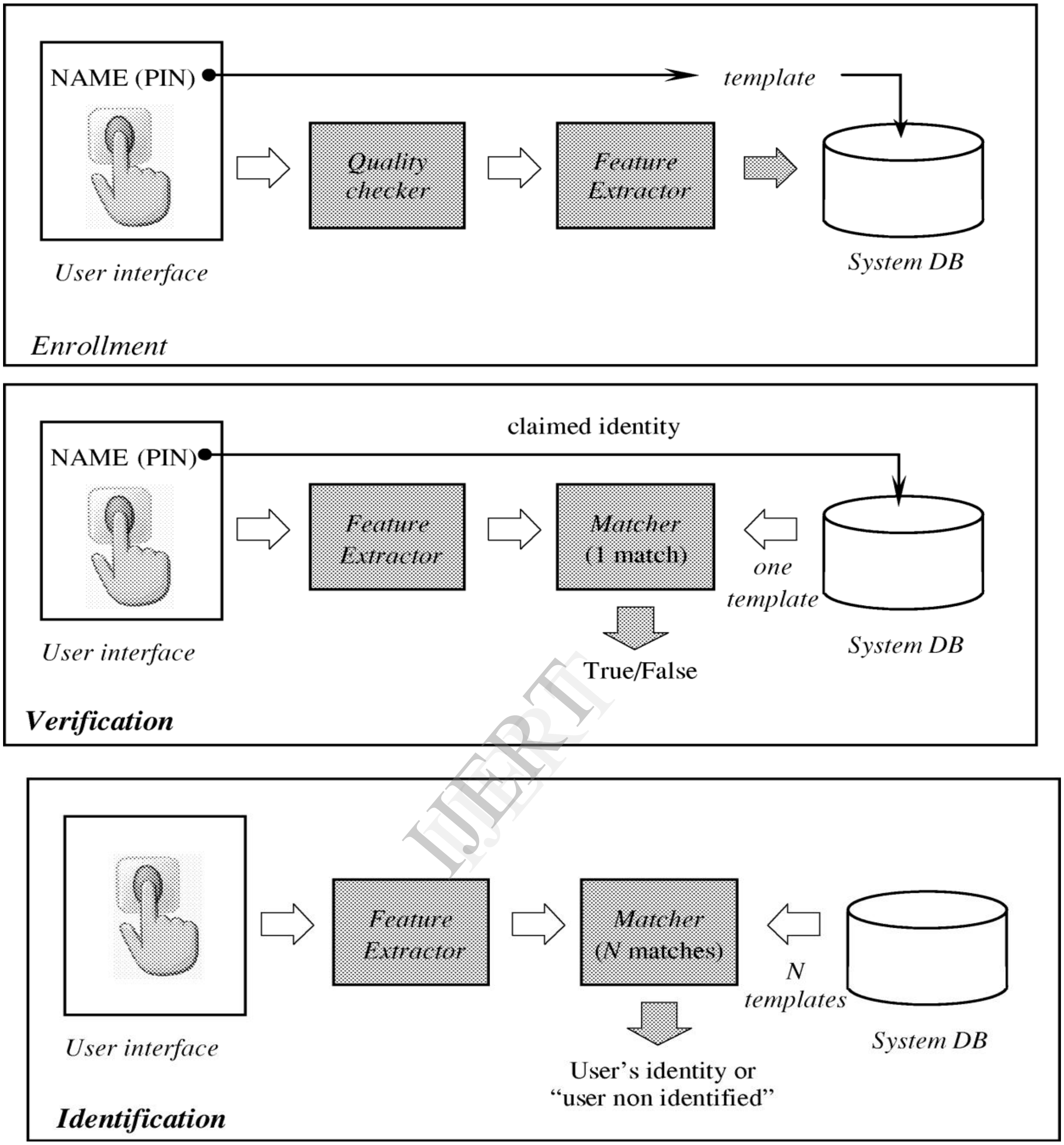


Fig. 1. Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database. [1]

[1] "An Introduction to Biometric Recognition". Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Salil Prabhakar, *Member, IEEE*

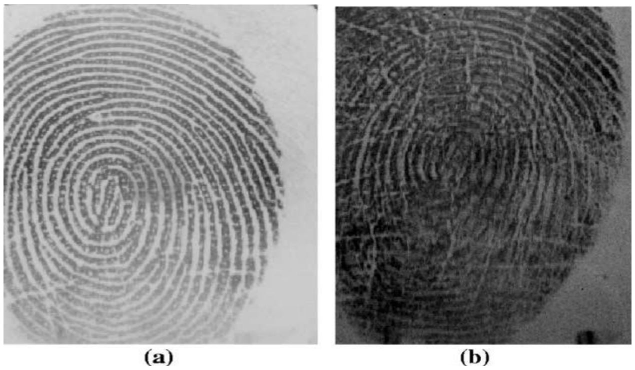


Fig 2. Effect of noisy images on a biometric system. (a) Fingerprint obtained from a user during enrollment. (b) Fingerprint obtained from the same user during verification after three months. The development of scars or cuts can result in erroneous fingerprint matching results.[2]

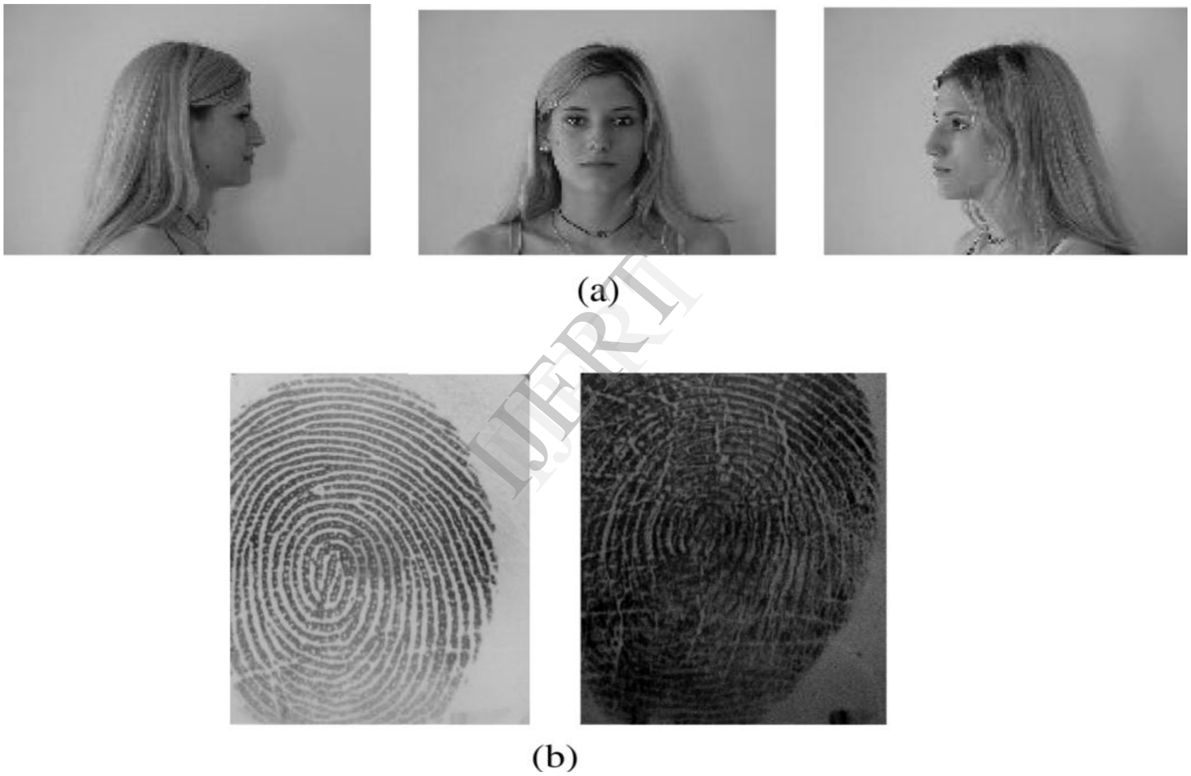


Fig 3. Variations in a biometric signal: (a) inconsistent presentation: change in facial pose with respect to the camera [6]; (b) irreproducible presentation: temporary change in fingerprint due to the wear and tear of ridges.[3]

The MIST

[2] "An Introduction to Biometric Recognition". Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Salil Prabhakar, *Member, IEEE*

[3] "Biometrics: A Tool for Information Security". Anil K. Jain, *Fellow, IEEE*, Arun Ross, *Member, IEEE*, and Sharath Pankanti, *Senior Member, IEEE*

Force the user when they setup the Cloud account to setup their own security question and not just provided by the system as most systems do. We have seen this implemented but it results in account suspension since the user honestly forgetting the answer to their question. So what we propose is the user must enter their question and then the system will display 50 random words that contain the answer and the user will have 16 seconds to pick a word. Failure of selecting the words can lead to account suspension. If the unauthorized user tries to enter the wrong question and/or if they guessed or somehow found out the question they will have tough time finding out what the word is in 16 seconds out of 50 words.

Pros and Cons of Suggested Methodologies

Pros:

1. The Mist is highly effective if implemented right.
2. The Mist can be easily installed
3. Very simple but yet effective technique
4. Can be changed and modified as needed

Cons:

1. The time of 16 seconds may raise a lot of issues with people who cannot remember what the word or phrase was before they forgot it
2. Needs to be tested on large Cloud systems.
3. It is very new and needs brush up job

Conclusion

We have provided a very new yet good methodology of accessing a Cloud account via the proven and traditional techniques utilizing Biometrics. These are effective techniques and work very well if funds are available. Otherwise, we recommend the ***Mist***. The Mist is easy to install and apply yet very solid and creative.

Future Research

We are implementing a cloud server at Southeastern Louisiana University Computer Science Department and implementing the Mist will be our prime objective. So we will test it and add to our newest invention of Cloud account security. No one methodology exists without the interface of other methodologies.

APPENDIX A

TABLE 1

Device	Verify	ID	Accuracy	Reliability	Errors	Error Rate	False Positive	False Negative	User Acceptance	Intrusive	Ease of Use	Low Cost
Speaker Recognition	Y	N	● ●	*	Noise Weather Illness	1 in 50	Medium	Easy	● ● ●	Non	● ● ●	Y
Dynamic Signature Verification	Y	N	● ●	*	Changing Signatures	1 in 50	Medium	Easy	● ●	Non	● ● ●	Y
Iris Scanning	Y	Y	● ● ● ●	* * *	Bad Lighting	1 in 131,000	Very Difficult	Very Difficult	● ●	Non	● ●	N
Fingerprinting	Y	Y	● ● ● ●	* * *	Dryness Dirt Age Injuries	1 in 500+	Extremely Difficult	Extremely Difficult	● ●	Somewhat	● ● ●	Y
Hand Geometry	Y	N	● ● ●	* *	Injuries Age	1 in 500	Very Difficult	Medium	● ●	Non	● ● ●	N
Facial Recognition	Y	N	● ● ●	* *	No Data	No Data	Difficult	Easy	● ●	Non	● ●	Y

All data displayed in this chart was obtained from the National Center for States Courts (NCSC) Web site.

REFERENCES

[1] Erl, Thomas, Zaigham Mahmood, and Ricardo Puttini, "Cloud Computing Concepts, Technology, and Architecture", Prentice Hall, 2013

[2] Bowers, Eric, and Adams, Randee, " Reliability and availability of Cloud Computing", Wiley, 2012.

[3] Miller, Michael."Cloud Computing Pros and Cons for End Users". InformIT, Feb 13,2009.< http://www.informit.com/articles/article.aspx?p=1324280>.

[4] "The Advantages of Cloud Computing". WebHostingReport. Retrieved on May 5, 2012 from < http://www.webhostingreport.com/learn/advantages-of-cloud-computing.html>.

[6] “Cloud Computing Architecture”.Theindiagate. Retrieved on May5,2012 from < http://www.theindiagate.info/2011/03/cloud-computing-architecture/>

[7] Walker,Grace. “Cloud Computing Fundamentals: A different way to deliver computer resources”.IBM, December 17, 2010. < http://www.ibm.com/developerworks/cloud/library/cl-cloudintro/>

[8] “Platform as a Service”. Zoho. Retrieved on May 5,2012 from < http://www.zoho.com/creator/paas.html>

[9] LIoyd,Mike. “Cloud Watching #1-Cloud 101”. Edutechassociates, February 23, 2011. < http://edutechassociates.net/2011/02/23/cloud-watching-1-cloud-101/>

[10] Brodkin, Jon. “10 Cloud Computing Companies to Watch”.Network World, May 19, 2009.< http://www.networkworld.com/supp/2009/ndc3/051809-cloud-companies-to-watch.html>

[11] Babcock,Charles. “Cloud Computing Can Drive Business Innovation”. InformatioWeek, February 13, 2012.< http://www.informationweek.com/news/hardware/utility_ondemand/232600687>

[12] Columbus,Louis. “Roundup Cloud Computing Forecasting and Market Estimates, 2012”. Softwarestrategiesblog, January 14, 2012. < http://softwarestrategiesblog.com/2012/01/17/roundup-of-cloud-computing-forecasts-and-market-estimates-2012/>

[1]3 http://www.carbonite.com/en/v2/about/our-story

[14] http://www.npr.org/blogs/alltechconsidered/2012/04/17/150808257/greenpeace-how-clean-and-green-is-your-cloud

[15] http://www.npr.org/blogs/alltechconsidered/2012/08/07/158365355/how-his-life-was-hacked-in-the-cloud

[16] http://www.npr.org/2011/11/29/142521910/the-digital-breadcrumbs-that-lead-to-big-data

[17]http://www.npr.org/blogs/alltechconsidered/2012/10/01/162080613/cloud-computing-saves-health-care-industry-time-and-money

[18] http://blog.lastpass.com/2011/05/lastpass-security-notification.html

[19] http://computer.howstuffworks.com/cloud-computing/5-ways-to-keep-your-information-secure-in-the-cloud.htm#page=0

[20] http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm

http://dictionary.reference.com/browse/cloud

[21] http://www.google.com/intl/en/chrome/devices/acer-c7-chromebook.html

[22]http://www.greenpeace.org/usa/Global/international/publications/climate/2012/iCoal/HowCleanisYourCloud.pdf

[23]Edge, I. E. (2010). Employ five fundamental principles to produce a SOLID, secure

network. *Information Security Journal: A Global Perspective*, 19, 153-159. doi: 10.1080/19393551003649008

Ihssan Alkadi is on the faculty at South eastern Louisiana University (*SLU*) He works in the Computer Science and IT Department. He received his BS Degree in Computer Science at SLU, May 1985. In May 1992 he earned his MS. In Systems Science from Louisiana State University (LSU). He earned his Doctoral degree in Computer Science at LSU May 1999. His areas of expertise include software engineering in general, testing in particular, Internet, HTML, and operating systems. His research interests include testing in object Oriented systems, systems validation, and system Verification. *Corresponding author.

Ghassan Alkadi is on the faculty at Southeastern Louisiana University (*SLU*) He works in the Computer Science and IT Department. He received his BS Degree in Computer Science at SLU, May 1985. In May 1992 he earned his MS. In Systems Science from Louisiana State University (LSU). He earned his Doctoral degree in Computer Science at LSU May 1999. Teaching Expertise: Introduction to Programming, Applications of Science and Technology, Software Engineering, and Information Systems

Kuo-pao Yang is on the faculty at Southeastern Louisiana University. He works in the Computer Science and Industrial Technology department. He received his B.S. degree in Computer Science at Tamkang University, Taipei, Taiwan, R.O.C., June 1991. In December 1994, he earned his M.S. degree in Computer Science from Illinois Institute of Technology. He earned his Ph.D. degree in Computer Science at Illinois Institute of Technology, June 2003. His research interests include Computer Architecture, Programming Languages ,and Expert Systems.