A Novel Approach for the Security Remedial in a Cloud-based E-learning Network

Md Anwar Hossain Masud*, Xiaodi Huang, and Md Rafiqul Islam
School of Computing and Mathematics, Charles Sturt University, Albury, Australia
*Corresponding author, Email: manwarhossain@csu.edu.au {xhuang, mislam}@csu.edu.au

***Abstract*—Cloud computing is an evolving paradigm with tremendous momentum, but its unique attributes exacerbate security and privacy challenges. Moving computing into the "Cloud" makes computer processing much more convenient for users, but also presents them with new security problems about safety and reliability. To solve these problems, it is necessary to establish security architectures for cloud based networks. This paper describes the trends in security requirements for cloud based networks, along with security architectures such as access protocol, authentication and identity (ID) management, and security visualization. This article discusses the barriers and solutions to providing a trustworthy cloud computing environment. These will help to overcome the security threats in cloud based e-learning network. Solving the key problems will also encourage the widespread adoption of cloud computing in educational institutes.**

I. INTRODUCTION

Cloud computing is an emerging technology that utilizes the cloud power to many technical solutions. The e-learning solution is one of those technologies where it implements the cloud power in existing systems to enhance the functionality providing to e-learners. Cloud technology has numerous advantages over the existing traditional e-learning systems. However, security is a major concern in cloud based e-learning networks. Therefore security measures are unavoidable to prevent the loss of users' valuable data from the security vulnerabilities. In past three decades, the computing world is based on the Internet, featured by the rapid development and applications of computer technology. The cloud computing model is one of the very important shapes of a new era. This technology is based on the distributed computing, parallel computing, grid computing, virtualization technologies, and property-based remote attestation technologies. Cloud computing is one of the best solutions as it delivers the computing resources (hardware and software) as a service over the Internet [1]. It provides resources and capabilities of information technology via services offered by CSP (cloud service provider). By extending Information Technology's (IT) existing capabilities, it is a novel way of increasing the capacity or adding capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software.

Cloud computing has generated significant interest in both academia and industry, but it is still an evolving paradigm. Essentially, it aims to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources. Confusion exists in IT communities about how a cloud differs from existing models and how these differences affect its adoption. Some see a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy, and culture. Nevertheless, cloud computing is an important paradigm, with the potential to significantly reduce costs through optimization and increased operating and economic efficiencies. Furthermore, cloud computing could significantly enhance collaborations, agilities, and scales, thus enabling a truly global computing model over the Internet.

Cloud computing amplifies computer security issues that have proliferated with the growth of the Internet. A broad range of security research is being applied to cloud computing. When cloud computing is applied in the field of education, a lot of problems have been studied, such as the technology for future distance education cloud, teaching information systems [2] [3] [4], the integration of teaching resources [5], and teaching systems development [6]. For the integration of e-learning and networks, an emphasis is placed on building of software and hardware platform in e-learning systems, functional structure, network security management and training, information technology integration to teaching [7], campus network environment [8], online education [9] and semantic web technologies-based multi-agent systems [10] [12].

Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy, and data protection continues to plague the market. Several surveys of potential cloud adopters indicate that security and privacy are the primary concern hindering its adoption. This paper examines security issues associated with e-learning. It focuses on the basic way of cloud computing development in relation to e-learning, growths and common security issues arising from the usage of cloud services. It also illustrates the unique issues of cloud computing that exacerbate security and privacy challenges in cloud based networks. We discuss various approaches to addressing these challenges

doi:10.4304/jnw.9.11.2934-2942

and exploring the future work needed to provide a trustworthy cloud computing environment.

The rest of this paper is organized as follows. Section II describes privacy and security in e-learning while section III explains the security concerns in cloud computing. Section IV describes security in cloud based e-learning, section V describes security and data privacy guidance based on the survey done among the higher educational institutes of Bangladesh. Section VI describes the proposed identity authentication in cloud based e-learning and section VII is the conclusion.

II. Privacy and Security in E-Learning

Security and privacy problems appear in e-learning because of the operation mechanism and policy mechanism. The failure of security technology makes personal privacy be spread, diffused, aggrieved and scouted without permission. The primary concern in e-learning is the security that can be summarized as follows [18]:

A. User Authorization and Authentication

The elementary feature of an e-learning system is the reliable identification – recognition of a user as a genuine member of a user community because it is the basis for Access control to the e-learning system.

Authentication – verification of the user's identity.

Authorization – permission to access specific resources. The Authorization is usually granted only to registered students and even their access are generally restricted to the appropriate part of e-learning materials based on the billing. If e-learning is offered on the billing basis and on the level of learning of the registered student, this will allow him/her to either to move to the next level or have a revision of the previous session.

B. Entry Points

There are many "entry points" in an e-learning system. A system can be attacked only through its "entry points". Designers can limit the security risks by reducing the number of entry points. But e-Learning systems cannot be implemented using this since there are a large number of multiple users from different geographic locations.

C. Dynamic Nature

The other challenge is the dynamic nature of e-learning systems where any process may join or leave the group sessions at any time. Security is also concerned with each particular member process. A strict session has to be maintained and the credentials are to be verified to control both at the session level and at the participant site.

D. Protection against Manipulation

One of the issues of e-learning is the manipulation from the side of the students. The system must be secured against manipulation. There are many possible solutions in which any manipulations can be protected by using the techniques of encryption, digital signatures, and firewalls.

E. Confidentiality

Confidentiality refers to the assurance that information and data are kept secret and private and are not disclosed to unauthorized persons, processes or devices. From an e-learning perspective, students need the assurance that their assignments they submit online are kept private and only disclosed to the intended examiner.

F. Integrity

Integrity is that only authorized users are allowed to modify the contents which include creating, changing, appending and deleting data and metadata. The attacks on integrity are generally the attempts made to actively modify or destroy information in the e-learning site without proper authorization.

G. Availablity

The e-learning material, e-content, and data (or metadata) are to be made available to the learners at the specified sessions when the users log on to the system for their session at the period of time, if the required material is not available the learners will lose their interests and not get the most use of the e-learning system. Mainly there are two types of attacks, (i) blocking attack and (ii) flooding attack, e.g. Denial of Service, Node attacks, Line attacks, and Network infrastructure attacks [16].

H. Non-Repudiation

Non-repudiation is another important step in information security where the learners have to be provided with E-Learning services without any possible fraud. For example, when computer systems are broken in to or infected with Trojan horses or viruses, to deny the works or changes done by them in the system elimination of a refuted activity performed by a user.

III. Security Concerns in Cloud Computing

Security is one of the people's peak concerns on all grounds. People are more concerned about the security especially for the use of the technologies that involve the Internet. Because the Internet has many loopholes that can crash the application or hack it to gain access to the users or company details by hackers worldwide. E-learning technology is now incorporated with many latest technologies to provide more provision and reduce the complexity from traditional e-learning methodology to their users. So a question is raised on how the cloud provides security in e-learning technology and to the e-learners. Our research shows light on identifying the security issues with cloud based e-learning and the countermeasures need to be taken for solving those problems.

The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. Due to the extensive complexity of the cloud, we contend that it will be difficult to provide a holistic solution to securing the cloud, at present. Cloud systems will: (i) support efficient storage of encrypted sensitive data. (ii) Store, manage and query massive amounts of data. (iii) Support fine-grained access control and (iv) support strong authentication. Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects

the systems in a cloud has to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

IV. Security in Cloud Based E-Learning

Cloud Computing predicts so many benefits but still there are also numerous issues and challenges for organizations covering the Cloud technology. Privacy of sensitive data is of paramount importance, and having dedicated servers is essential if the Cloud environment is to be accepted. When shifting e-learning in the cloud, main security concerns are about confidentiality, integrity and availability, as depicted in "Fig. 1".

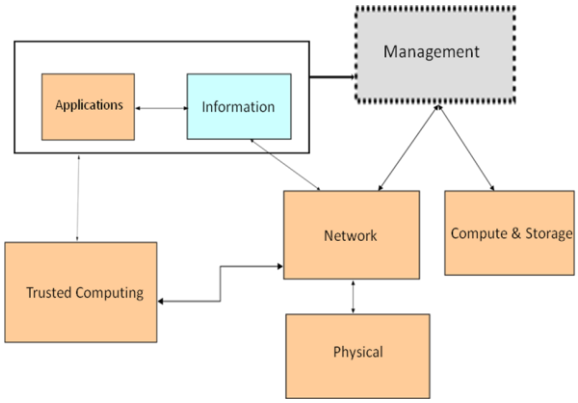

Figure 1. Areas of concerns in a cloud based e-learning system

As security remains as an integral component of the top issues in cloud based e-learning netwotks, there are several significant threats that should be considered before adopting the paradigm of cloud computing in e-learning. These threats are described as follows:

A. Misuse of Cloud

Cloud services providers are often targeted for weak systems with limited fraud detection capabilities. Misuse includes creating spam, decoding and cracking of passwords, executing malicious codes to access rich information such as question papers, learning materials, and assessments.

B. Software Access

Various software interfaces and APIs are used by the cloud users in e-learning to access and manage the cloud services. These APIs play an integral part during provisioning, management, orchestration and monitoring of the processes running in a cloud environment. Hence these APIs needs to be secured and should include features of authentication, access control, encryption, and activity monitoring.

C. Malicious Insider

Malicious employees who are working in the providers or user site can be able to perform insider attacks. This insider can steal the confidential data of cloud users in e-learning. Malicious insider can easily get the cloud users in e-learning confidential data such as passwords, cryptographic keys and files.

D. Data Loss

Operational failures, unreliable data storage and inconsistent use of encryption keys will lead to a data loss. Operational failure includes deletion, incomplete deletion or alteration without any backup of the source e-learning content. Unreliable data storage means storing a data on an unreliable media which cannot be recoverable if the data is lost. Inconsistent use of encryption keys will lead to unauthorized access and data loss such as destruction of sensitive and confidential information.

E. Incorporated Risk

It is essential for the every e-learning user to know the software versions, security practices, software code updates and intrusion attempts. Cloud service providers usually advertise these futures and functionality with the necessary details such as the internal security procedure, configuration hardening, patching, auditing and logging. E-learning users must be aware and clarify how their data and related files are stored.

V. Security and Data Privacy Guidance Based on Survey

There are various steps given by the cloud service providers to ensure the security concern in the cloud computing which could be applied to cloud based e-learning netwoks. Few guidelines have been given by the organizations such as Cloud Standards Customer Council, Intel, and Microsoft.

In recent days, awareness about cloud computing problems is heavily weighted towards security and reliability problems. This research conducted a survey to assess problems related to Cloud adoption for higher educational institutes of Bangladesh from the customer viewpoint. Table 1 reveals that security, stable operation, and a support system; that is, safety and reliability, ranked highest among user concerns. Given that in Cloud computing the information technology (IT) system is invisible to the user, it is understandable that educational institutes strongly want their information to be fully protected and services to be provided stably.

A. Brief Description of the Survey

The research takes a positivist stance and is deductive in nature and it used an empirical survey to collect quantitative data to determine the cloud readiness and its adoption and the barriers behind the adoption process. The target population of the research was those IT managers and head of departments who have influences or decision-making capabilities related to ICTs within their organizations. SPSS has a procedure that conducts exploratory factor analysis. 70 Universities were chosen from a population of 110 Universities in Bangladesh. The list of universities was obtained from the University Grant Commission. The universities chosen included State, and private universities. The questionnaires were distributed to management (academic and administrative) and information technology staff of the universities. These categories of staff are likely to be responsible for taking decisions on the adoption of major technology

facilities. The data gathering instrument used in the research is the questionnaire.

TABLE I. PERCENTAGE OF DIFFERENT FACTORS AS BARRIERS FOR CLOUD ADOPTION

What would you consider as barriers to cloud computing adoption?				
	Freq.	%	Valid Percent	Cum Percent
Security concerns				
Integration issues with existing systems and applications	40	19.0	19.0	69.5
Loss of control over data and applications	42	20.0	20.0	89.5
Availability and performance concerns	14	6.7	6.7	96.2
Regulatory, Compliance and IT governance issues	8	3.8	3.8	100.0
Total	210	100.0	100.0	

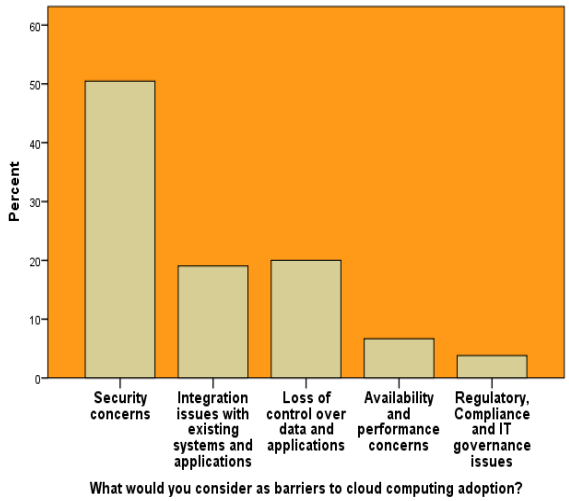

Figure 2. Barriers for cloud computing adoption

B. Survey Instrument

The survey instrument consists of questions that were designed to collect information. The targeted participants in this survey were IT executives, and departmental heads. A total of 210 participants had responded to the survey questionnaire within the timeframe allotted for statistical analysis. The data was then imported into SPSS student version 20.0 software for the required statistical analysis. Multiple regression analysis were performed as confirmation to the chi-square results obtained as well as to provide comparative analysis to the results obtained through prior research and for analysis of barriers for cloud adoption.

C. Summary of Findings

In Table 1 and Fig. 2, it is evident that the dominant barriers are security concerns, integration issues with existing systems and applications, loss of control over data and applications, availability and performance concerns, regulatory, and compliance and IT governance issues. The dominant contributors and enablers of Cloud computing are: good awareness, sufficient resources, affordable and good Internet infrastructure, good or guaranteed security and privacy, functionality and efficiency. The poor telecommunications infrastructure and lack of skills are highlighted in developing countries. The telecommunication findings are consistent with those of earlier academic research and white papers. This supports the requirement to do technology readiness and e-readiness research. Also, the lack of skills in developing countries is a matter of concern. In the bi-variate correlations test as given in Table 4, the tests also reveal that the relationship between - what would you consider as barriers to cloud computing adoption?—and which of the following issues are most likely concerns of Cloud adopters privacy? is positive at $r = .263$ ($p < .001$, $r2 = .069$).

In Table 2 and corresponding Fig. 3, subsequently in Table 3 and Fig. 4, security is the main obstacle that is encountered when implementing cloud computing, followed by issues regarding compliance, privacy and legal matters. Organizations are worried about security and privacy concerning the use of cloud computing services as the market provides marginal assurance. Matching internal security requirements with the cloud computing vendor's measures and controls proves to be difficult in practice due to discrepancies, lack of insight and insufficient expertise.

D. Guidelines for Security Enforecement in a Cloud-Based E-Learning

A cloud service provider should ensure that the customers will use Cloud computing without worry. The necessary security considerations for performing critical tasks on a Cloud-computing platform are furnished below. This can serve as a reference for both the vendors and users of Cloud computing based solutions.

- Authentication and Identity Management: Identity and access management are very important for the strategic use of dynamic cloud computing resources. Providers' authentication systems should either meet or exceed enterprise standards. Enterprises should be encouraged to adopt single-sign on for applications to simplify identity and access management. By using cloud services, users can easily access their personal information and make it available to various services across the Internet.
- Access Control and Accounting: It is important that the access control system employed in clouds is easily managed and its privilege distribution is administered efficiently. It should be ensured that cloud delivery models provide generic access control interfaces for proper interoperability, which demands a policy-neutral access control specification and enforcement framework that can be used to address cross-domain access issues. The access control models should also be able to capture relevant aspects of SLAs. The utility model of clouds demands proper accounting of user and service activities that generates privacy issues because customers might not want to let a provider maintain such detailed accounting records other than for billing purposes. This can be shown in Fig. 5.

TABLE II. ISSUES OF CONCERN FOR CLOUD ADOPTER'S PRIVACY

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Availability of services and/or data Availability of services and/or data	53	25.2	25.2	25.2
	Integrity of services and/or data	31	14.8	14.8	40.0
	Confidentiality of corporate data	61	29.0	29.0	69.0
	Denial Of Service	12	5.7	5.7	74.8
	Loss of control of services and/or data	12	5.7	5.7	80.5
	Lack of liability of providers in case of security incidents	15	7.1	7.1	87.6
	Inconsistency between trans national laws and regulations	10	4.8	4.8	92.4
	Unclear scheme in the pay per use approach	6	2.9	2.9	95.2
	Uncontrolled variable cost	5	2.4	2.4	97.6
	Cost and difficulty of migration to the cloud (legacy software etc...)	3	1.4	1.4	99.0
	Intra-clouds (vendor lock-in) migration	2	1.0	1.0	100.0
	Total	210	100.0	100.0	

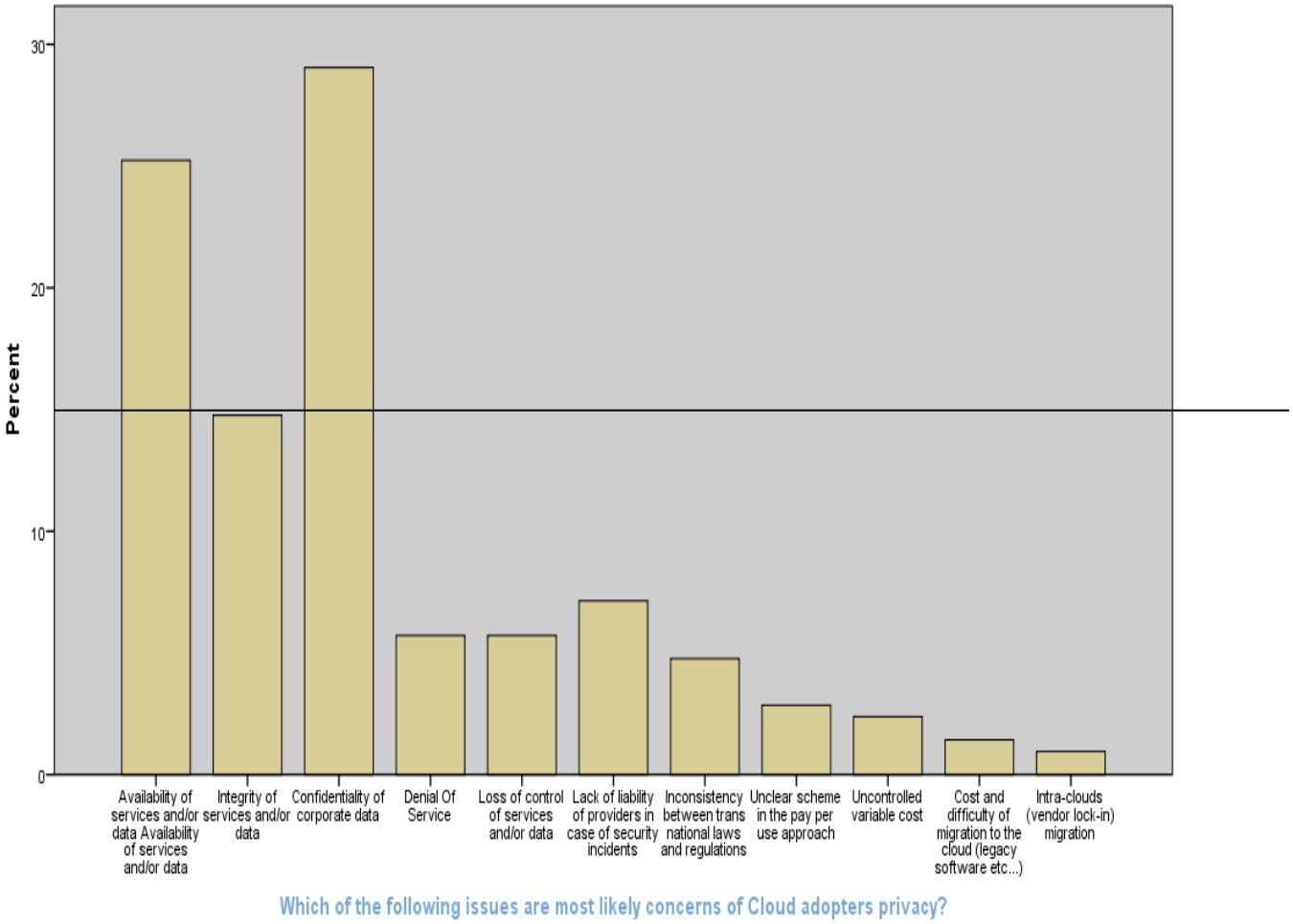

Figure 3. Issues of concerns for cloud adopter's privacy

TABLE III. BIVARIATE CORRELATIONS

		What would you consider as barriers to cloud computing adoption?	Which of the following issues are most likely concerns of Cloud adopters privacy?
What would you consider as barriers to cloud computing adoption?	Pearson Correlation	1	.263**
	Sig. (1-tailed)		.000
	N	210	210
Which of the following issues are most likely concerns of Cloud adopters privacy?	Pearson Correlation	.263**	1
	Sig. (1-tailed)	.000	
	N	210	210
**. Correlation is significant at the 0.01 level (1-tailed).			

TABLE IV. COVENANTS REQUIRED IN A CONTRACT

	Freq.	Percent	Valid Percent	Cum Percent
Network security requirement	49	23.3	23.3	23.3
Physical security requirement	73	34.8	34.8	58.1
Education activities for users	46	21.9	21.9	80.0
Support SLA	36	17.1	17.1	97.1
Peak load capacity guarantees	6	2.9	2.9	100.0
Total	210	100.0	100.0	

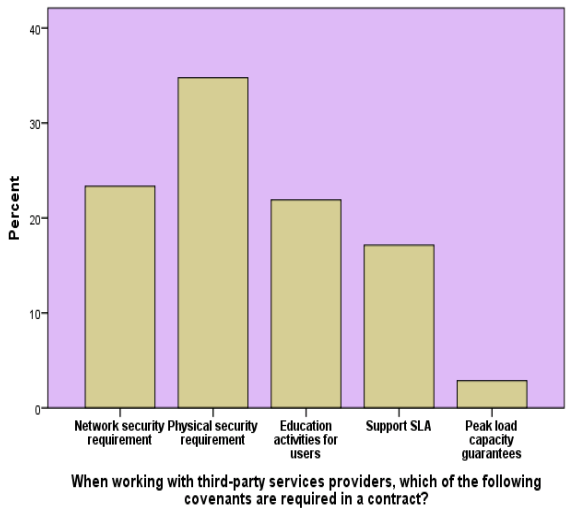

Figure 4. Covenants required in a contract

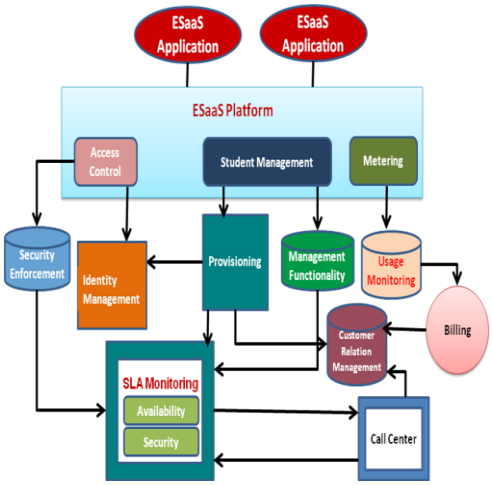

Figure 5. Visualized a Cloud Model to ensure the proposed guideline

- Data-Centric Security and Privacy: Data in the cloud typically resides in a shared environment, but the data owner should have full control over who has the right to use the data and what they are allowed to do with it once they gain access. To provide this data control in the cloud, a standard-based heterogeneous data-centric security approach is an essential element that shifts data protection from systems and applications. Cryptographic approaches and usage policy rules must be considered. In this approach, documents must be self-describing and defending regardless of their environments.
- Institutional Security Management: Existing security management models significantly change when enterprises adopt cloud computing based solutions. Customers consequently need to consider newer risks such as data leakage within multi-tenant clouds and resiliency issues. The possibility of an insider threat is significantly extended when outsourcing data and processes to clouds. Within multi-tenant environments, one tenant could be a highly targeted attack victim, which could significantly affect the other tenants which is depicted in "Fig. 6"

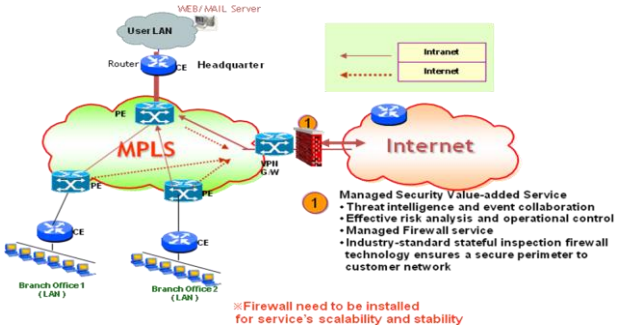

Figure 6. Institutional security enforcement in Network

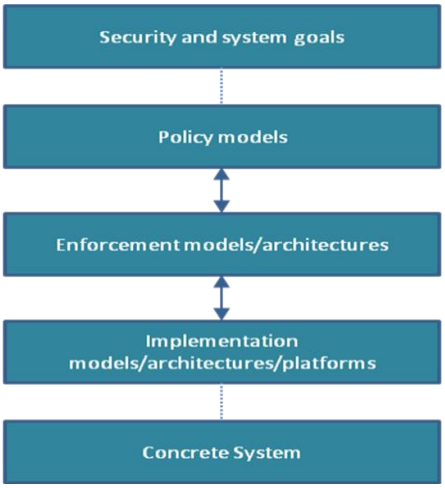

Figure 7. Layered stacks for security enforcement

- Data backup and disaster recovery: Data backup and disaster recovery are among the most desired security and control. Vendors need to ensure the redundancy and backup of all hosted data through replication and storage across multiple zones. It is important to know who created a piece of data, who modified it and how, and so on. Provenance information could be used for various purposes such as trace back, auditing, and history-based access control.
- Trust Management and Policy Integration: Although multiple service providers coexist in clouds and collaborate to provide various services, they might have different security approaches and privacy mechanisms, so we must address heterogeneity among their policies. Cloud service providers might need to compose multiple

services to enable bigger application services. Therefore, mechanisms are necessary to ensure that such a dynamic collaboration is handled securely and that security breaches are effectively monitored during the interoperation process. Thus, a trust framework should be developed to allow for efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements.

According to the guideline, the following layered stacks are proposed for enforcement of security in a cloud based system, especially for the education arena, as shown in "Fig. 7".

VI. Proposed Identity Authentication in Cloud Based E-Learning

On the basis of the survey and studies, activities for organizing Cloud computing requirements have started. Among these requirements, access control, authentication and ID management are prominent and need to be given attention. Traditionally, identity authentication is applied when an individual requests access to a system. For this situation, the three elements or items used for identity authentication are what you have, what you know, and what you are. Cloud computing introduces a whole new challenge for identity authentication. For the example of an identity authentication, consider that when a program running within the cloud needs to access some data stored in the cloud, i.e., what you have and what you are. However, the context of the access request is relevant and can be used [18]. Only some access key and the careful monitoring protects against unauthorized access. In cloud computing (as well as other systems), there are many possible layers of access control. For example, access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM. Depending on the deployment model used, some of these will be controlled by the provider and others by the consumers.

Google Apps, a representative SaaS Cloud controls authentication and access to its applications, but users themselves can control access to their documents through the provided interface to the access control mechanism. In IaaS type approaches, the user can create accounts on its virtual machines and create access control lists for these users for services located on the VM. Regardless of the deployment model, the provider needs to manage the user authentication and access control procedures (to the cloud). While some providers allow federated authentication – enabling the consumer-side to manage its users, the access control management burden still lies with the provider. This requires the user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies. This can be burdensome when numerous users from different organizations with different access control policies, are involved. This proposal focuses on access control to the cloud. However, the concepts here could be applied to access control at any level, if deemed necessary. We propose a way for the consumer to manage the access control decision-making process to retain some control, requiring less trust of the provider as illustrated in "Fig. 8".

This approach requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer. It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions [20]. Furthermore, we need to show that this approach is at least as secure as the traditional access control model. This approach requires the data owner to be involved in all requests. Therefore, frequent access scenarios should not use this method if traffic is a concern. However, many secure data outsourcing schemes require the user to grant keys/certificates to the query side, so that every time the user queries a database, the owner needs to be involved.

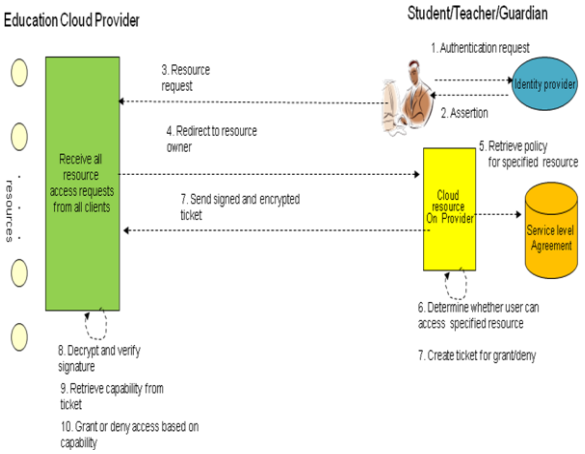

Figure 8. Proposed Identity Authentication in cloud based e-learning

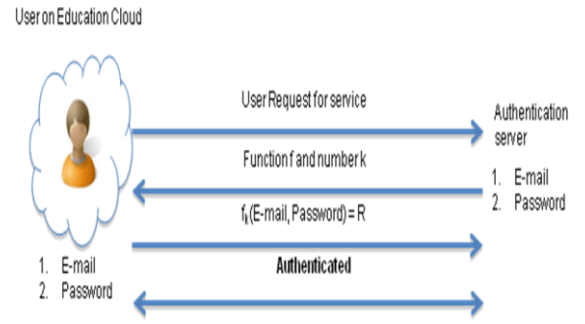

Figure 9. Proposed Identity Authentication for proofing in details

The proposed method has the ability to use identity data on untrusted hosts, i.e., Self Integrity Check. It should be independent of a third party. It establishes the trust of users through putting the user in control. Identity is being used in the process of authentication, negotiation, and data exchange as shown in "Fig. 9".

VII. Conclusion

Security is one of the major issues that reduces the growth of cloud based networks and complications with data privacy. Data protection continues to plague the

growth. Security and privacy services in the cloud can be fine-tuned and managed by experienced groups that potentially provide efficient security management and threat assessment services. The issues we have discussed in this paper show that existing security and privacy solutions must be critically reevaluated with regard to their appropriateness for clouds. Many enhancements in existing solutions as well as more mature and newer solutions are urgently needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. This paper has described in brief the cloud security issues and solutions. Some security challenges that are specific to cloud based networks have been described. Security solutions must make a trade-off between the amount of security and the level of performance costs.

The key conclusion of this paper is that security solutions applied to cloud computing must span multiple levels and across functions. Our goal is to spur further discussions on the evolving usage models for clouds and the increasing security cover these will need to address both the real and perceived issues, thus spurring new research in this area. Economic benefit of such research and resulting solutions will be increased trust in, and accelerated adoption of cloud computing. In the background of cloud computing, both of the data privacy and the data dissemination are important. Authentication and authorization are done to ensure data security in cloud based networks, so security deficiencies and benefits need to be carefully weighed before making a decision to implement it. However, the future looks less cloudy as far as more people being attracted by the topic and pursuing research to improve on its drawbacks.

REFERENCES

[1] A. Hossain Masud, X. Huang, "ESaaS: A New Education Software Model in E-learning Systems", *Information and Management Engineering, Communications in Computer and Information Science*, 2011, Volume 235, Book Chapter pp 468-475.

[2] Ahmed, S., Buragga, K. & Ramani, A. K. Year. Security issues concern for E-Learning by Saudi universities. *In, 2011. IEEE*, 1579-1582.

[3] A. Hossain Masud, X. Huang, "Enhanced M-Learning with Cloud Computing: The Bangladesh Case", *Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design, IEEE CSCWD 2011, Switzerland*, pp 735-741.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, et al., "A View of Cloud Computing," *ACM Communications*, vol. 53, pp. 50-8, 2010.

[5] D. Kasi Viswanath, S. Kusuma and Saroj Kumar Gupta, "Cloud Computing Issues and Benefits Modern Education", *Global Journal of Computer Science and Technology Cloud & Distributed.*, Vol. 12 Issue 10 Version 1. 0 pp. 15-19, July 2012.

[6] S. Al-Rwais, and J. Al-Muhtadi, "A Context-aware Access Control Model for Pervasive Environments," I*ETE Technical Review, vol. 27, pp. 371-9, 2010.*

[7] Sehgal NK, Sohoni S, Xiong Y, Fritz D, Mulia W, Acken JM. A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing. *IETE Tech Rev* 2011; 28:279-91.

[8] Md. Anwar Hossain Masud, Xiaodi Huang, "An E-learning System Architecture based on Cloud Computing", *World Academy of Science, Engineering and Technology 62 2012 available at http://www. waset. org/journals/waset/v62/v62-15. pdf*

[9] Z. Zhong-ping, L. Hui-cheng "The Development and Exploring of E- Learning System on Campus Network", *Journal of Shanxi Teacher's University (Natural Science Edition)*, Vol. 18, No. 1, Mar. 2004, pp. 36-40.

[10] T. Jian, F. Lijian, G. Tao, "Cloud computing-based Design of Network Teaching System", *Journal of TaiYuan Urban Vocational college*, Mar. 2010, pp. 159-160.

[11] H. Xin-ping, Z. Zhi-mei, D. Jian, "Medical Informatization Based on Cloud Computing Concepts and Techniques", *Journal of Medical Informatics, V*ol. 31, No. 3, pp. 6-9, 2010

[12] J. A. Méndez and E. J. González, "Implementing Motivational Features in Reactive Blended Learning: Application to an Introductory Control Engineering Course", *IEEE Transactions on Education*, Volume: PP, Issue: 99, 2011.

[13] R. Buyya, C. S. Yeo & S. Venugopal, "Market-oriented Cloud computing: Vision, hype, and reality of delivering IT services as computing utilities," *10th Ieee Int. Conf. High Performance Comput. Comm.*, p. 5–13, 2009.

[14] M. Lijun, W. K. Chan & T. H. Tse, "A tale of Clouds: Paradigm comparisons and some thoughts on research issues," *Ieee Asia-pasific Services Comput. Conf., Apscca08*, pp. 464–469, 2008.

[15] K. Praveena& T. Betsy, "Application of Cloud Computing in Academia," *Iup J. Syst. Management*, vol. 7, no. 3, pp. 50–54, 2009.

[16] K. A. Delic & J. A. Riley, "Enterprise Knowledge Clouds, Next Generation Km Syst". *Int. Conf. Inform., Process, Knowledge Management, Cancun, Mexico*, pp. 49–53, 2009.

[17] D. Chandran and S. Kempegowda, "Hybrid E-learning Platform based on Cloud Architecture Model: A Proposal", *Proc. International Conference on Signal and Image Processing (ICSIP)*, pages 534-537, 2010.

[18] S. Ouf, M. Nasr, and Y. Helmy, "An Enhanced E-Learning Ecosystem Based on an Integration between Cloud Computing and Web2. 0", *Proc. IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pages 48-55, 2011.

[19] A. Hossain Masud, X. Huang, ―"A Novel Approach for Adopting Cloud-based E-learning System", *IEEE/ACIS 11th International Conference on Computer and Information Science, China*, pp 37-42, 2012.

[20] Xuefei Chen, Jing Liu, Jun Han, Hongyun Xu, "Primary Exploration of Mobile Learning Mode under a Cloud Computing Environment", *E-Health Networking, Digital Ecosystems and Technologies (EDT), International Conference*, Vol. 2, PP. 484 – 487, IEEE 2010.

[21] N. Sclater, "elearning in the cloud", *International Journal of Virtual and Personal Learning Environments*, Vol. 1, No. 1. pp. 10-19. January 2010.

[22] Carsten Ullrich, Ruimin Shen, Ren Tong, and Xiaohong Tan, "A Mobile Live Video Learning System for Large-Scale Learning—System Design and Evaluation", *Transactions on Learning Technologies*, vol. 3, IEEE 2010.

[23] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, and D. Riboni. "A survey of context modeling and reasoning techniques", *Pervasive and Mobile Computing*, Vol. 6, Issue 2, 2010.

[24] A. Hossain Masud, X. Huang, J. Yong, "Cloud Computing for Higher Education: A Roadmap", *Proceedings of IEEE*

16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2012.

[25] N. M. Rao, C. Sasidhar, and V. S. Kumar, "Cloud Computing Through Mobile Learning," *(IJACSA) Internationa Journal of Advanced Computer Science and Applications*, Vol. 1, No. 6, pp. 42 – 46, December 2010.

Md. Anwar Hossain Masud is currently a Ph.D student at Charles Sturt University, Australia. He obtained his M.Sc degree in ICT from Ritsumeikan University, Japan in 2007. He is a Life fellow of Engineer's Institute of Bangladesh. He has served in Govt sector of Bangladesh in the field of Telecommunications for the last 16 years. His research interests are IP based network, Cloud computing and NGN.

Xiaodi Huang obtained his PhD degree in Computer Science from School of Information Technology at Swinburne University of Technology in 2004. As a senior lecturer, he joined the School of Business and Information Technology at Charles Sturt University in July 2007. Prior to that, he was a lecturer in School of Mathematics, Statistics and Computer Science at the University of New England, Armidale, and University of Southern Queensland, Toowoomba, respectively. His research interests are Visualization, Data Mining, Wireless Networks and Web Services.

Rafiqul Islam is a Lecturer in the School of Computing and Mathematics, Charles Sturt University. He earned BSc (Honours) and MSc (Research) from the department of Computer Science and Engineering, University of Dhaka, and PhD degree with the specialisation in Network Security from Deakin University, Australia. Before joining CSU, Rafiqul has worked in the School of Information Technology, Deakin University, Australia. He was also a Lecturer & Assistant Professor in the Department of Computer Science and Engineering, University of Dhaka. Dr. Islam is a member of the Institute of Electrical and Electronics Engineers (IEEE) and Fellow member of Association of Accounting Technician (AAT).