Advantages of Components in Security & Privacy Architecture as a Service for Small and Medium Enterprises

Nilaykumar Kiran Sangani, Tejas Vithani, and Muthaiyan Madiajagan

***Abstract*— This paper presents the advantages of the six components published in the proceedings of the International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM-12) titled, "Security & Privacy Architecture as a Service for Small and Medium Enterprises," targeting their hosted web applications or services on small clouds to run their organization's business activities. Small and Medium Enterprises (SMEs) should have knowledge of the security protocols while publishing applications on clouds and giving out services to the end-user. Security & Privacy Architecture as a Service (SPAaaS) framework, which has been identified in ICCCTAM-12, will help the SMEs to gain better insight on the security model for such web based applications. The aim of this paper is to highlight the benefits of the six components that need to be addressed and implemented by SMEs in hosting their services in clouds.**

***Index Terms* — Cloud Computing, Cloud Cyber Security, IT Security, Small and Medium Enterprises**

I. Introduction

THE prime objective for a SME is to attain profits by offering solutions to customers. Cloud computing has been erupting as one of the latest technologies having SMEs to acclimate, showcase and offer their business solutions. SMEs either host web applications or hire a vendor to implement their products and services to end users via the Internet. SMEs are cognizant of the infrastructure and hosting mechanism, though they are unaware of the knowledge in order to protect web application data due to lack of either technical security architects or lack of funding[2][3]. The SME will be able to elect on the risks they can have in their bandwidth only after they are able to assess them. There are large amounts of capital invested by SMEs in hiring IT professionals with respect to hardware and software for their internal departments or external end users. By adapting cloud computing, SMEs are able to concentrate more on business goals relatively than IT issues, being that there is no internal IT department. This will also assist management in cutting costs [4].

Over the last couple of years, security and privacy has been a major concern when it comes to adapting cloud computing. It is one of the prime technologies used by SME to broadcast solutions over the web for users; as this helps to reduce IT costs and increase their ROI[3]. SMEs have limited knowledge regarding the security of web applications. They either host on cloud or hire a third party vendor providing Software as a Service.

Manuscript received March 30, 2013; revised April 09, 2013.

N.K.K.Sangani is working with Abu Dhabi Company for Onshore Oil Operations (ADCO), Abu Dhabi, U.A.E as an IT Security Analyst. He is also a student with the Computer Science Department, M.E (Software System), Birla Institute of Technology and Science Pilani-Dubai Campus, Dubai, UAE (email: sanganinilay@hotmail.com).

T.Vithani is a student with Computer Science Department M.E (Software System), Birla Institute of Technology and Science Pilani-Dubai Campus, Dubai, U.A.E (email: tejas.vithani@gmail.com).

M.Madiajagan is Assistant Professor with the Computer Science Department, Birla Institute of Technology and Science Pilani-Dubai campus, U.A.E (email: jagan@bits-dubai.ac.ae).

II. Literature Survey

Hackers and attackers are always eyeing to find vulnerabilities in web applications to launch their attacks. As SMEs are concerned about business profits, they scarcely have knowledge regarding the security and privacy of their web application hosted on cloud. The decision makers of the SMEs though aware that security is a principal concern within the verticals of any strategic decision yet they pay little attention to it. They should be conscious that their services and end users information is widely available over the Internet via a web application on cloud, which can be hacked by the cyber criminals [3][5]. During the budget meetings SMEs have no provisions to accommodate an IT Security expert in their organization, as it is completely not aligned to their business motive to earn profits [5]. Senior managers and the management of the SMEs do not have a clear understanding about protection mechanisms when it comes to hosting web applications on cloud, or hiring a SaaS provider and examining security requirements [6]. They seek to invest both money and time into only those business decisions which provides their organizations huge profits, in turn evolving the future of the company [5]. As they put end users data on cloud, SMEs should be clear that the data is being exposed to everyone, including the hackers and attackers. They should be aware of the security controls that need to be incorporated in order to protect data [5].

Most SMEs employ very few Information Technology mavens to handle their entire IT infrastructure. Information Security has never been their leading objective, as the management of a SME always assumes that it does not assist them in generating profits [3][6]. They hire vendors giving SaaS solutions, or deploy their application on cloud to

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

showcase their products and services without bearing in mind the ill-effects of the lack of security infrastructure in order to protect their data because they do not have gen or the expertise. It is very important for a SME to be knowledgeable about the security components while hosting their web applications on cloud. This information will help them to identify the different types of application, network and data breaches conducted by the attackers, and the precautions to be taken to prevent such attacks [5].

III. RESEARCH GAP

SMEs should accept the fact that hosting applications on cloud will open their information to everyone over the Internet—including hackers. Various attacks, such as data leakage, session and cookie hijacking, web protocol breaches are arising in the cloud computing scene [7]. SMEs should always keep in mind that their services are hosted outside their organization's premises on different servers which can reside anywhere in the world due to which makes the hosted systems highly prone to exploitation by the attackers and hackers [6]. Moving to cloud is an enhancement for their current IT Services. SMEs should clearly understand protection mechanisms for hosted applications in aspect to confidentiality, integrity and availability [5][8]. There is an interruption between SMEs and cloud security due to lack of awareness and expertise on SMEs have in the information security field.

In today's economy, data increases rapidly, enhancing the SMEs to familiarize cloud computing and put up their application on cloud. At the same time, they should not ignore the security implementation of the same. The company's assets need to be protected [9].

Aim of this paper is to bring out the advantages of six components for SPAaaS identified in the paper titled, "Security & Privacy Architecture as a Service for Small and Medium Enterprises," a component based architecture to be implemented by various security solution vendors aiding SMEs in evaluating security requirements and functionality to host their web applications on cloud.

IV. ADVANTAGES OF THE SIX PROPOSED COMPONENTS - SPAAAS

The research conducted to emphasize the advantages in the six components identified in this paper, which will assist the SMEs in their implementation in web applications while hosting them on cloud. Figure 1 depicts the identified six components, which need to be addressed, highlighting their advantages [1].

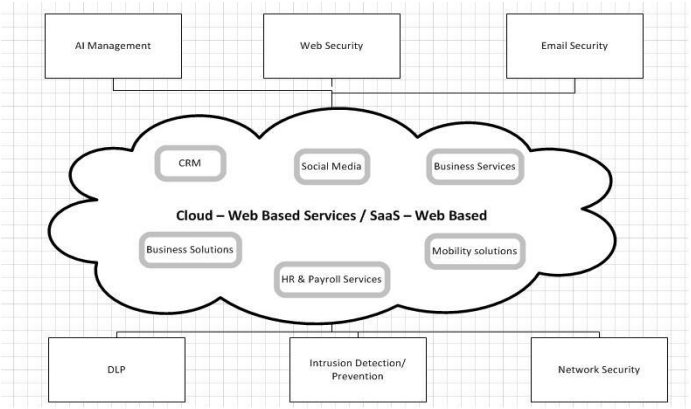

Fig 1: Design – Security & Privacy Architecture as a Service for SMEs for Web Applications (SPAaaS – Web) [1]

A. *Access & Identity Management*

IT Organizations face huge challenges in managing identity and access controls for applications. One of the major obstacles is to identify authorized users on cloud, which can be addressed by implementing Access & Identity Management. The operation of AI Management will provide the following features [9]:

- Management of personal identity information so that access to information system resources such as data, computers, and servers are controlled properly.
- Customers and end users benefit from secure processes while accessing their applications and data on cloud.
- Improves user productivity as sign-on process is executed.
- Reduction in IT costs in managing manual identities for each user.
- Password management and synchronization.

B. *Web Security*

In the past few years, business demand solutions are available freely without any constraints of location, or technology, or devices. Web solutions are becoming mobile and can be accessed from anywhere at any time. Yet, at the same time, web attacks are increasingly targeting end users or the company's liquidity. Administering a web security component will prevent hackers from attacking web applications that are hosted on cloud. A few of the advantages it provides are [10]:

- Implementation of web filtering and malware scanning controls prevents unauthorized sites from being accessed and restricts downloading of materials.
- Analysis and protection against phishing sites, threats and planned web attacks.
- Protection against cross-site scripting and SQL injection attack.
- Combinations of highly advanced web security controls in one component.
- Implementation of SSL.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

C. Email Security

E-mail is one of the most important means of communication in organizations between internal employees, external customers, end users, partners, etc. The messages and data are transmitted over the internal/external network. As it is widely used, it has gained popularity among hackers to attack. An E-mail Security component will have the following advantages [11]:

- Safeguards for incoming and outgoing e-mails by assuring secure mechanisms.
- Encrypt outgoing important e-mails on case-by-case basis.
- Identify phishing mails and mails received from untrusted users.
- Implementing digital signatures, identity and encryption.
- Blockage of spam e-mails from third party vendors.
- Archiving of e-mails, auditing and logging.
- Assurance of complete e-mail availability.

D. Data Loss Prevention (DLP)

For every organization it is extremely important to make sure their customers, end users, internal, and external data is not exposed for attacks. Mechanisms and controls need to be put in place to protect such data from leakage. DLP should be implemented once data is kept on cloud, thus, protecting the data in motion, transit and at rest. The DLP component will have the following advantages [12]:

- Detecting policy violation of the organization during data transmission.
- Monitoring, protecting and verifying the authenticity of the data in motion and at rest.
- Real time inspection and detection of web content.
- Safeguards against the loss of important data.
- Identify sensitive data via algorithms.
- Pattern recognition of violated data.

E. Intrusion Detection & Prevention (IDP)

It is very difficult to monitor all incoming and outgoing points with respect to data, systems, controls, etc. While hosting data and services on cloud, SMEs need to know that their services are exposed over the Internet. Focus should be given to the basics of service and architecture while implementing IDP. The IDP component will have the following advantages [13]:

- Implementing the IDP framework.
- Identifying raw packets and scanning them for any discrepancies.
- Monitoring attacks such as DDOS.
- Implementing HIPS/HIDS to monitor and analyze traffic/packets for any suspicious behavior in applications or protocols.
- Monitoring policy violations during incoming/outgoing of packets.

F. Network Security

Network security consists of the security of the underlying physical environment and the logical security controls that are inherent in the service, or available to be consumed as a service. In a cloud environment, a major part of network security is likely to be provided by virtual security devices and services. Tight integration with the underlying cloud software layer to ensure full visibility of all traffic on the virtual network is important. The network security component will have the following advantages [14]:

- Ensuring basic attack vectors are mitigated by traditional physical controls.
- Implementing perimeter firewall security will help in detecting real time protocol vector attacks.
- Regarding virtual machines, implementation of sub-tier firewall controls provides the second layer of virtualization, real-time protocol inspection and detection.
- Access control lists (ACLs) will help against the threats such as scanning, flooding the network, disrupting the connections etc.
- Logging and auditing in the incoming / outgoing protocol connections.

V. CONCLUSION & FUTURE WORK

This paper accentuates the advantages of the six components used in the security and privacy architecture for the SME's (i.e. access & identity management, web security, e-mail security, data loss prevention, intrusion detection and prevention and network security). In the future, we plan to extend our work by applying a component based architecture design for the implementation of the above-discussed components.

ACKNOWLEDGEMENT

We would like to extend our sincere gratitude to Ms. Charlis Cunningham and Ms. Arundhuti for their copy editing assistance.

REFERENCES

[1] N.Sangani, T.Vithani, M.Madiajagan and P.Velmurugan, Security & Privacy Architecture as a Service for Small & Medium Enterprises, *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on, vol,no.,pp.16,21,8-10 Dec.2012*doi10.1109/ICCCTAM.2012.6488064 Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6488064&isnumber=6488050

[2] F.T.Neves, F.C.Marta, A.M.R Correia and Miguel de Castro Neto, The Adoption of Cloud Computing by SMEs: Identifying and Coping with Extenal Factors, *11a Conferencia da Associacao Portuguesa de Sistemas de Informacao (CAPSI 2011), 19-21th Oct 2011*

[3] L.R.Rewatkar and U.A.Lanjewar, Implementation of Cloud Computing on Web Application, *International Journal of Computer Applications* (0975-8887), Volume 2 -No.8, June2012, pp 28-32

[4] M.Sharma, A.Mehra, H.Jola, A.Kumar, M.Misra and V.Tiwari (2010), Scope of cloud computing for SMEs in India, *Journal of Computing*, Volume 2, Issue 5, May 2010, ISSN 2151-9617

[5] “Moving to the cloud? Take your application security with you”, Cloud Security Alliance, Jan 27, 2011, Available at: https://blog.cloudsecurityalliance.org/2011/01/27/movingto-the-cloud-take-your-application-security-with-you/
[6] N.Sangani and B.Vijaykumar, Cyber Security Scenarios and Control for Small and Medium Enterprises, *Informatica Economica*,vol 16 no.2/2012,pp 58-71
[7] A. Khalid, Cloud Computing: Applying Issues in Small Business Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, vol., no., pp.278-281, 9-10 Feb. 2010 dois: 10.1109/ICSAP.2010.78Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5432738&isnumber=5432354
[8] “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, CSA, Dec 2009, Available at: https://cloudsecurityalliance.org/csaguide.pdf
[9] "Guidance for Identity & Access Management V2.1", Cloud Security Alliance, April 2012, Available at: https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf
[10] "SecaaS Implementation guide, Category 3: Web Security", Cloud Security Alliance, September 2012, Available at: https://cloudsecurityalliance.org/research/secaas/#_downloads
[11] "SecaaS Implementation guide, Category 4: Email Security", Cloud Security Alliance, September 2012, Available at: https://cloudsecurityalliance.org/research/secaas/#_downloads
[12] "SecaaS Implementation guide, Category 2: Data Loss Prevention", Cloud Security Alliance, September 2012, Available at: https://cloudsecurityalliance.org/research/secaas/#_downloads
[13] "SecaaS Implementation guide, Category 6: Intrusion Management", Cloud Security Alliance, September 2012, Available at: https://cloudsecurityalliance.org/research/secaas/#_downloads
[14] "SecaaS Implementation guide, Category 10: Network Security", Cloud Security Alliance, September 2012,Available at: https://cloudsecurityalliance.org/research/secaas/#_downloads

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)