Cloud Based Emails Boundaries and Vulnerabilities

Taiwo Ayodele
Information Intelligence
Infonetmedia Portsmouth, United Kingdom

Dennis Adeegbe
IFREC IFREC, Osaka
Osaka, Japan

***Abstract*—since there is significant increase in adoption of cloud computing, securing users emails is also a growing concern. This paper reviews the boundaries, privacy, vulnerabilities, varying legislations of cloud based emails, and how to mitigate such to provide reliable and secure cloud based email services for users and organizations. We propose a new framework to improve security of cloud based email messages: Intelligent Cloud Based Email Encryption and Decryption System (ICLEEDS). The goal is to encrypt content of email mail messages from users' mail box before being sent. The intelligent machine learning encryption system helps to protect users against email interception, re-construction, phishing attacks, relaying of previous messages, spoofing, eavesdropping and provide high level of privacy.**

Keywords—component; Email messages, Cloud based email, email services, email Vulnerabilities, email privacy, eavedropping, secured cloud based email messages, Intelligent cloud based email encryption and decryption, email security and privacy, cloud computing

I. INTRODUCTION

Emails can be stored and be accessed anywhere in the world as it has become the major means of communications among users and is used virtually in all aspects of our daily lives. Everyone now has email account and if you sign on with Hotmail, Gmail or Yahoo, you possibly have a cloud based email account that could be viewed and shared all over the world. One issue with cloud based email is that one does not have knowledge of where in the world your emails and sensitive data are stored.

Every day, more users transfer their data, files, archived mails, attach photos and documents from the desktop to their mailbox, and rely on web applications to store and access them. But this new technology involves serious risks that are not obvious to most people. Every message that we send from our mailbox to the outside world are now stored in the cloud, bringing up the issues of boundaries, privacy, content licensing, and a host of vulnerabilities.

Cloud computing according to Mel et al [1] is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Chan and colleagues at IBM [2] also elaborated that Cloud is a computing model providing web-based software, middleware and computing resources on demand by deploying technology as a service, which give users access only to the resources they need for a particular task. This prevents one from paying for idle computing resources. Cloud computing can also go beyond cost savings by allowing users to access the latest software and infrastructure offerings to foster business innovation. Such offerings include but not limited to:

- **Reduction of Data Storage:** Storing MP3′s, video, photos and documents online instead of at home provides the freedom to access them wherever one can find web connectivity
- **Collaboration:** Downloading files onto flash memory, emailing documents to friends, family, and colleagues or sending submissions by mail is gradually becoming old fashioned. Few years ago, Google launched a service that allowed groups of people to work on the same document, idea, or proposal in real time or whenever convenient to each participant. Using Google Apps, one can create a document and then invite others to comment, amend, offer opinion, or otherwise join in with the creation of the final draft
- **Cloud based Infrastructure:** Rather than purchasing servers, software, and network equipment, etc, users would buy into a fully outsourced set of online services instead. Most cloud environments on offer can customize the kind of service provided to exactly suit the needs of the user. If one needs more processing power from time to time, a cloud-based infrastructure, being scalable, negates the need for up-front investment in client-owned resources

Considering the aforementioned facts about cloud computing in relation to email services being provided, it becomes evident that cloud computing consists of hardware and software resources made available on the Internet as third party-managed services. In addition, it also offers the benefit of being able to access web-based services that host all programmes and applications that is needed through a remote machine owned by another organisation.

This means an organization's data may reside on the same hard drives as another's bringing into question the physical and logical separation of information on these shared infrastructures. In addition, there is concern regarding backups, lost or stolen drives, just to mention a few. Without clear boundaries, it becomes difficult to provide security for such information.

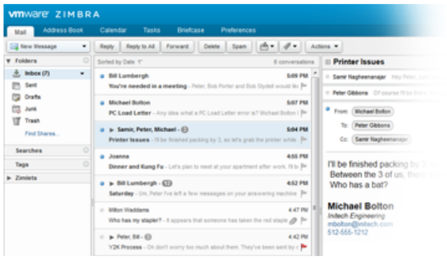
II. EXISTING WORK

In the field of cloud computing, email servers and services are paramount and seems to be cost effective to service providers, users, and businesses. Having on-demand access to email services and other computing resources as well as global communication clearly has its advantages.

However, it can have disadvantages too, because emails on the cloud is stored in various countries and locations and different countries have different laws on matters such as data protection, tax, the prevention of terrorism, and more. How much of this national legislation affects businesses and email users will depend on numerous factors and awareness of such rules and regulations should be presented to users as they sign on for such email service.

Several applications have been developed using the cloud as the storage place to provide email services for users and businesses. Some existing cloud based services and apps are:

- Google Apps [3]: (comprising Gmail, Google Calendar, Google Docs, and other web applications) provide familiar, easy to use products and services for business settings. These services, characterized by redundant computing environments and dynamic resource allocation, enable customers to access their data virtually anytime and anywhere from Internet-capable devices. This computing environment — often called the "cloud" — allows CPU, memory and storage resources to be shared and utilized by many customers while also offering security benefits.
- IBM LotusLive iNotes [2]: This service is IBM's first real foray into a mass-market cloud-based service, including e-mail, calendaring, and contact management all designed to work with existing on-premise e-mail or operate as a standalone solution. Per user pricing will start at just $3 per month.
- VMware vSphere 5 [4]: This is the industry-leading virtualization platform for building cloud infrastructures. VMware vSphere accelerates the shift to cloud computing for existing data centers. It also underpins compatible public cloud offerings, paving the way for the industry's only hybrid cloud model. With the introduction of VMware vSphere 5. figure 1 illustrates the VMware mail services.



Bill Lumbergh 5:09 PM
You're needed in a meeting - Peter, Bob Porter and Bob Slydell would lik

Michael Bolton 5:07 PM
PC Load Letter - Any idea what a PC Load Letter error is? Michael Bolton

Samir, Peter, Michael - 5:04 PM
Printer Issues - I'll be finished packing by 3, so let's grab the printer while

Joanna 4:55 PM
Dinner and Kung Fu - Let's plan to meet at your apartment after work. I'll b

Bill Lumbergh - 4:52 PM
Saturday - Um, Peter I've left a few messages on your answering machine

Milton Waddams 4:47 PM
Who has my stapler? - It appears that someone has taken the red staple

Peter, Bill - 4:42 PM
Y2K Process - Oh don't worry too much about them. They've been sent by

Printer Issues
Samir Nagheenanajar
Peter Gibbons
From: Michael Bolton
To: Peter Gibbons
Cc: Samir Nagheenanajar

I'll be finished packing by 3,
Between the 3 of us,
Who has a bat?

Michael Bolton
Initech Engineering
mbolton@initech.com
512-555-1212

Fig. 1. VMware Zimba

VMware is evolving the product's licensing model to give customers the opportunity to move to a more cloud-like, "pay for consumption" approach to IT. The changes lay the foundation for a more modern IT cost model that is based on consumption and value rather than components and capacity

There has been significant rise in the adoption of cloud computing and Software-as-a-Service (SaaS). Figure 2 shows the level of awareness and cloud email usages. This highlights the significance of cloud service as the future for most users.

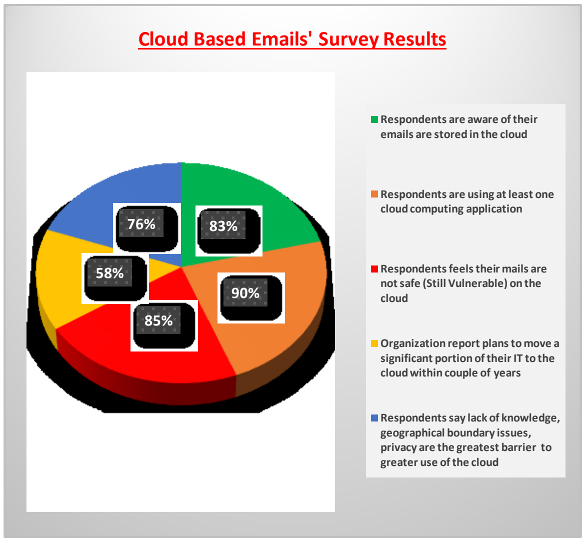


Fig. 2. Cloud Based Email Awarenes

This statistics as shown in figure 2 demonstrates the cloud awareness and this determines the level of usage to some extent, showing that 76% of respondents are aware of cloud based emails, 90% are aware of Cloud Application, 85% are skeptical of vulnerabilities of mails in the cloud, 76% are unaware of lack of knowledge of Cloud Barriers while 58% of organizations plan to move their IT Infrastructures to the Cloud

However, the present concern over security has greatly impacted its growth within email services. Four of the most common security concerns include privacy, data exclusion, data protection issues (differences in countries' legislations) and user access privileges. These are explored further in section 3.

III. Boundaries, Privacy and Data Exclusion Issues with Cloud Emails

A. *Varying Laws*

Different countries have different laws on matters such as data protection, tax, among others. How much of this national legislation affects email users as well as businesses will depend on numerous factors. These range from country to country and the ethics that cloud service providers must abide by must be made open to email users. Awareness of such will enlighten users to either be careful before signing on an account or be careful on the use of such account. In some countries, email users can create various accounts for several family members. Since the user is the only one managing such accounts for all members of the family, other people's data could be compromised. Some countries on the other hand have stricter rules that protect individuals.

B. *Access Privileges*

For email users, personal access privilege is ultimately what users expect but with cloud based email services, the threat of malicious, accidental user breaches, email phishing, spoofing, eavesdropping, and access right violations remain a concern. In further analysis of security concern of cloud based email, James et al, [5] stated that in a model where security is only as good as your weakest link, many overlook the user threat that may exist within an outsourced organization that now controls your sensitive communication. Cloud providers should therefore take serious steps to mitigate this sort of problem.

C. *Data Protection and Privacy*

When it comes to accessing and managing your email messages by cloud providers or third party establishments that manage infrastructures or web services, data protection act (DPA) must be in place–to protect users and organizations' misuse and abuse of data [6].

Companies and organizations that would like to process, access or manage your mail services need to comply to data protection act principles and practices such as:

- Notifying the Office of the Information Commissioner (a government body) that they are doing so. This is important as it makes it possible to know who is legitimately processing data and who is not.
- Adhering to eight principles embodied in the law. For instance, data must be obtained "fairly" - that is, at the point of collection it must be made clear what the data will be used for. It must be accurate and up to date and it must be held securely.
- Obtaining User's permission which is needed before the messages or data access is permitted by the user.
- Making the user aware about access that is needed and the reason for such access into their personal messages or data. These include seeing what is held about the user, compensation, (when things go wrong) and, in some cases, the right to prevent access.

The major concern is that not all countries abide by this DPA, so users data could be shared without their permission or knowledge.

IV. Intelligent Cloud Based Machine Encryption And Decryption System (ICBMEDS)

Intelligent cloud based email machine encryption and decryption system is a novel machine learning data encryption and decryption algorithm that provides cryptographic privacy especially for email communication.

Intelligent cloud based machine encryption and decryption system (ICBMEDS) encryption uses machine compressed data, combined machine generated keys that use algorithms that are aligned with user email address and login details. ICBMEDS combines machine-generated keys encryption with public key encryption. So, each message is encrypted using machine encryption algorithm that requires combined machine generated keys. Figure 3 illustrates the ICBMEDS system.

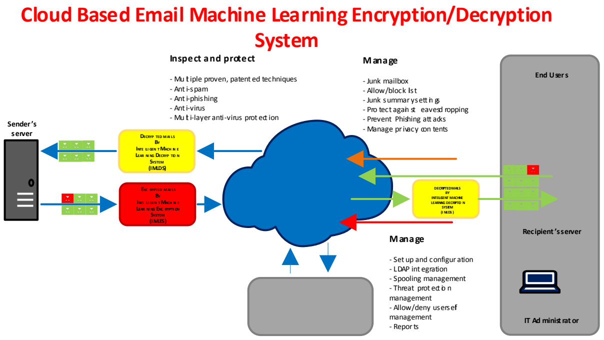

Cloud Based Email Machine Learning Encryption/Decryption System
Inspect and protect
- Mu tiple proven, patent ed techniques
- Ant i-s pam
- Ant i-phis hing
- Ant i-virus
- Mu t i-layer anti-virus prot ect ion
Manage
- Junk mailbox
- Allow/block lst
- Junk summar y sett in gs
- Pro tect again st eavesd ropping
- Prevent Phishing att acks
- Manage pr ivacy con tents
End Users
Sender's server
Decryp ted mails By Inte ligen t Mach ne Lear ning Decryp tio n System (IMLDS)
Enc rypted mails By Inte ligen t Mach ne Lear ning Enc ryption System (IMLES)
DECRYPTED MAILS BY INTELIGENT MACHINE LEARNING DECRYPTIO N SYSTEM (IMLDS)
Recipient's server
Manage
- Set up and configur ation
- LDAP int egration
- Spooling management
- Threat prot ect io n management
- Allow/deny users ef management
- Repor ts
IT Ad minist rat or

Fig. 3. Cloud Based Email Machine Learning Encryption and Decryption System

The ICBMEDS framework provides high level of privacy, prevents email interceptions or re-constructions, prevents eavesdropping, phishing attacks and many more.

V. Conclusion and Future Work

Increasing numbers of businesses, organizations, Universities, Colleges and host of enterprises are now migrating to the cloud necessitating a need to address security concerns. In this paper, we build a novel intelligent cloud based machine learning encryption and decryption system (ICBMEDS) that provides email users with better security and privacy irrespective of geographical boundaries, and varying legislative laws. This novel model addresses security concerns, including lasting recommendations or solutions to boundaries issues, provision of reliable and sustainable security against email vulnerabilities, and this should result in more and more organizations beginning to weigh cloud services for their IT needs, including modernization of their email infrastructure. Our future plan includes improving the ICBMEDS with more sophisticated self-learning, self-adaptive encryption and decryption algorithm. In order to verify the generality of our findings, we are working on evaluating our methods with varying data in an attempt to ultimately create a gold standard for cloud based email messages.

References

[1] Mell, P., Grance, T., The NIST Definition of Cloud Computing, in Recommendations of the National Institute of Standards and Technology, N.I.o.S.a.T. (NIST), Editor 2012, NIST Special Publication NIST Special Publication 800-145. p. 1-7.

[2] Chan, R., LotusLive iNotes: Accessing Critical Information, Anywhere, Anytime, 2006: IBM Corporation.

[3] Google, Security Whitepaper: Google Apps Messaging and Collaboration Products, 2011: Google Inc.

[4] VMware, VMware vSphere 5: Licensing, Pricing and Packaging, 2011, VMware, Inc. p. 1-13.

[5] James, B., Getting Productive With Google Apps. 2009, San Francisco, CA.[6] ICO, Data Protection Act Factsheet, I.C.s. Office, Editor 2012, Information Commissioner's Office p. 1-3.