RESEARCH ARTICLE OPEN ACCESS

E-Mail Systems In Cloud Computing Environment Privacy,Trust And Security Challenges

Maha Attia[1], Mona Nasr[2], Ahmed Kassem[3]
[1]*Engineering Institute, CIC Deputed of Faculty of Computers & Information, Helwan Univ.*
[2]*Faculty of Computers & Information, Helwan Univ.*
[3]*Faculty of computers & Information, Helwan Univ.*

ABSTRACT
In this paper, SMCSaaS is proposed to secure email system based on Web Service and Cloud Computing Model. The model offers end-to-end security, privacy, and non-repudiation of PKI without the associated infrastructure complexity. The Proposed Model control risks in Cloud Computing like Insecure Application Programming Interfaces, Malicious Insiders, Data Loss Shared Technology Vulnerabilities, or Leakage, Account, Service, Traffic Hijacking and Unknown Risk Profile.
Keywords: Cloud Computing, Software as a Service, Cloud Security, Mail Security, Mail System, Cryptography, Authenticating.

I. INTRODUCTION

The cloud computing is a common technology in developing software, it gains a lot of popularity as it has many benefits. Cloud can enhance collaboration, agility, scaling, and provision of cost reduction through optimized and efficient computing.Cloud computing is a model for enabling timely, on-demand network access to a shared pool of configurable computing resources and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing as explains the development of many existing technologies and approaches to computing into something different. Cloud distributes application and information resources from the underlying infrastructure, and the mechanisms used to provide the service over the internet ,the capability provided to the user is to use the provider's applications operating on a cloud infrastructure. The applications are accessible from multiple client devices through a thin client interface such as a web browser.

Costs Reduction is one of the advantages when using cloud computing. Cloud Computing decrees hardware, implementation, operation and software licensing costs, that means lower capital and operating costs. This definite advantage for start-out businesses. Also, charges based on used resources only.

Mobility makes the ability to access data and system any time any anywhere, using PC, PDA, mobile device and internet browser. Scalability of cloud computing provides the advantage of the easy scalability of increasing or decreasing the size of one's service according to the exact requirements. Technology in cloud computing allows getting the value of access to shared IT resources benefit from advanced technologies that would otherwise be unaffordable.

Collaboration is an additional advantage of cloud computing multiple users can collaborate easily. This makes it possible to collaborate with members in different locations and in different time zones. Data Reliability in cloud computing makes data loss prevention method to avoid the issue of destroying your valuable data on a personal computer for hardware or software loss reasons, Also, the ability to have a value of disaster recovery and backup systems.

Cloud Computing enables Business Agility as it rapidly solves problems using IT resources without long-term commitment and pattern of agility at a much lower cost. Performance is increased because of using system updates, latest version availability, and reliable high-performance hardware systems

In cloud computing as a service, a user does not manage or control the underlying cloud infrastructure containing network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Security is one of the key areas and is most often mentioned by corporate decision-makers as they consider cloud computing for the future. Figure 1 displays the top cloud computing security concerns .Specifically, safety of data during transfer when stored as reviling of sensitive data my occurs. The valid security architecture in place will ensure that data is kept completely separate from the encryption keys that enable access. Security rules in cloud computing for the most part, not different than

security rules in any IT environment. Because of the cloud service models applied, the operational models, and the technologies used to enable cloud services, cloud computing present different risks to an organization than traditional IT solutions.

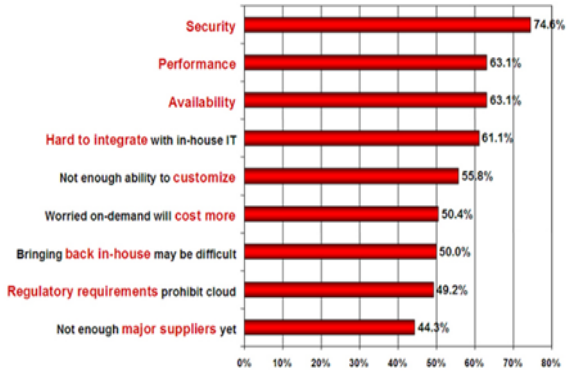

Figure 1: The Top Cloud Computing Concerns [1]

Cloud computing is about appropriately losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties. An organization's security posture described by the maturity, effectiveness and completeness of the risk-adjusted security controls executed. Certain controls executed in one or more layers ranging from the facilities to the network infrastructure, IT systems, and all the way to the information and applications. Additionally, controls implemented at the people and process levels, such as separation of duties and change management, respectively. In this research is a model for e-mail security is proposed. The model is based on web service and cloud computing. This paper is organized as the follows; Section two overviews Cloud Computing Security; Section three reviews the related work; Section four demonstrate the proposed Secure Mail using Cloud Software as a Service (SMCSaaS) model; Section five views operation comparison between model and traditional e- mail systems; Section six discusses the conclusion.

II. CLOUD COMPUTING SECURITY

Cloud Computing Security Challenges

The ENISA 2012 Cloud Risk Assessment considers security benefits offered by the Cloud computing model. These have to be weighed against the risks that this model brings with it. Although they are not strictly necessary for assessing the risks, they have been kept in this document to put the risks into perspective.

Security measures increase cost-benefit analysis when deployed on a larger scale. For the same amount of investment in security gains excellent protection. That includes all types of the defensive standard such as filtering; patch management, hardening of virtual machine instances and hypervisors, etc. Other benefits of scale include different locations, edge networks timeliness of response, to incidents and risk management.

Security is a priority attention for many cloud customers; many of them will make a decision based on the status for confidentiality, integrity, flexibility and the security services offered by the cloud provider. That is a strong driver for cloud providers to improve security practices.

Rapid and custom scaling of resources: the ability of the cloud provider to dynamically allocate resources for filtering, traffic management, authentication, encryption, etc., to defensive measures has obvious advantages for resilience.

Benefits of resource consolidation: Although the consolidation of resources surely has an impact on security it has the advantage of physical parameters and physical access control and the easier and cheaper application of many security-related processes.

III. RELATED WORK

This part explains the traditional key management architectures used in mail security.

3.1 Symmetric Key Cryptography

Cryptography Architecture [2] uses the same key to encrypt data. Symmetric key use same key for encryption and decryption. Key manager generates the unique key for every message the key stored in a database with the list of recipient. When the message received the recipient, authenticate to the Key Manager to retrieve the key from the database, the recipient address matched with authorized recipients list. If everything checks out, after validation the decryption key sent to the recipient to decrypt the message.

3.2 Asymmetric Key Cryptography

Asymmetric cryptography is the cryptographic system that uses pairs of keys; public keys can be distributed to requesters paired with private keys which are known only to the owner.

One of the popular cryptographic systems used to secure email is Public Key Infrastructures (PKI)introduced by Diffie and Hellman in 1976[3].

The asymmetric cryptography, which contains a pair of keys to allow secure communication between parties, the trusted party require to verify public key, PKI authenticating all public key. PKI systems trust user's key instead of trusting users, the traditional PKI system, all entities in the system trust a central party called the Certification Authority (CA). CA guarantees public and private keys belong to the claimed owner.

Traditional email systems using Public Key Infrastructure (PKI) for Encryption and Digital

Signature on message communications flow when sending or receiving emails, the following diagram show digital signature operation

Public Key Infrastructure must share the private key between users before secure communications.

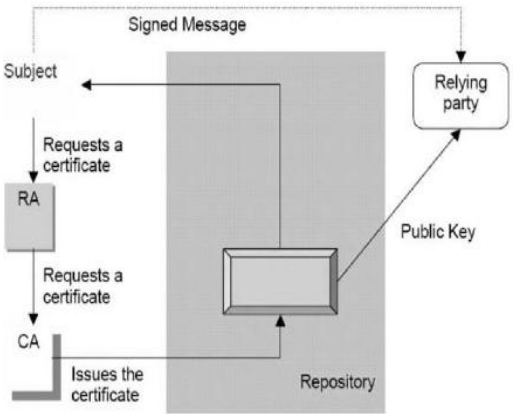

Figure 2: PKI Entity and Operations [4]

registration authority server then receive signed certificates from Certificate Authority Server this process consumes time and requires expensive infrastructure. Online server requirements certificate leaked and complexly in exchanging keys and complex system management described in the following Mail Send and revive Flow Process.

The PKI Mail Send Flow Process New Email Message in Figure 3 that merged encryption mechanism using the following sequence

- Receive Sender Information Identification
- Receive Recipient Information Identification
- Signing Message using Digital Signature and Sender Identified Information
- Email Message Digitally Signed
- Encrypting Email Message using Encryption Mechanism and Recipient Identified Information
- Output Process Digitally Signed and Encrypted Message.
- Send Message

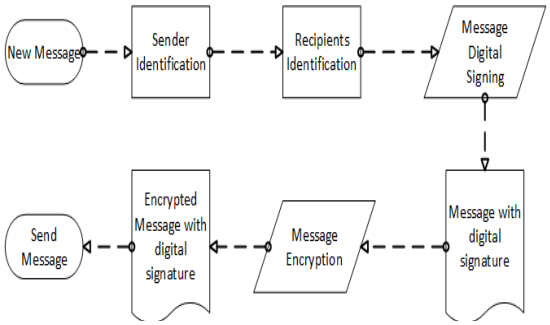

Figure 3: Mail Send Flow

The PKI Mail Receive Flow Process in figure 4 that merged encryption mechanism using the following sequence

- Receive Encrypted Email Message
- Receive Recipient Information Identification
- Decrypting Email Message using Recipient Identified Information
- Email Message Decrypted
- Decrypted Message.
- Digital signature was received Inside Unencrypted Message.
- Receive Sender Information Identification
- Signing Message using Digital Signature and Sender Identified Information
- Identify Email Message Digital Signature and Recipient Information Identification
- Message Validation
- Receive Message to Recipients Mailbox

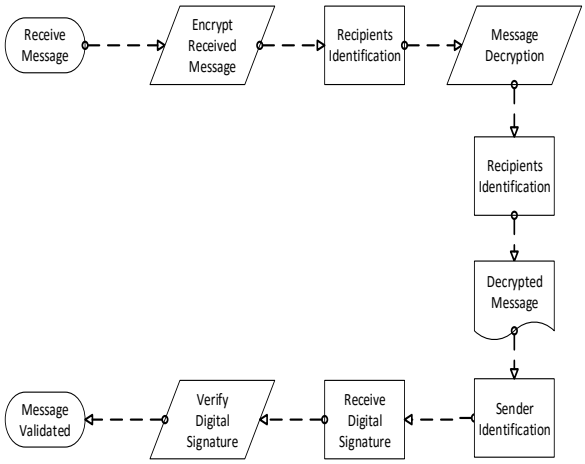

Figure 4: Mail Receive Flow

Pretty Good Privacy PGP

Pretty Good Privacy or PGP [5] it was developed by Philip R. Zimmermann in 1991, has used to encrypt email over the Internet, and authenticate email with digital signatures and encrypted attached files. PGP using public key types Rivest Shamir Adleman (RSA) and Diffie-Hellman, RSA uses the MD5 algorithm to generate a hash key.

Diffie-Hellman uses the SHA-1 algorithm to generate hash code. PGP using the public key known to all users this key used to encrypt email and private key uses to decrypt the message, Encrypted message, and the short key sent to the receiver who have a private key to decrypt the short key and then uses that key to decrypt the message.

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) [6] use the assumption that finding the discrete algorithm of random elliptic curve parts concerning a publicly known base point is unfeasible. The common types of ECC are Curve Diffie-Hellman (ECDH), Edwards

curve Digital Signature Algorithm (EdDSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). The ECC security advantage is that comparable security to a 3072-bit RSA with a 256-bit ECC. That required decreasing required computing power to encrypt and decrypt messages with ECC and that faster than standard RSA message encryption.

Identity-Based Encryption

Identity-based public key (IBE) [7]proposed by Adi Shamir on 1984. The purpose of IBE is to reduce the cost of public key certificate management. Instead of generating and using public and private key pair in a public key encryption system like RSA, the idea of using a username or email address as a public key, with the identical private key is generated by Private Key Generator (PKG). Since users public key is based on some publically available information, which uniquely represents the user. An identity-based encryption system can do away with public key directory maintenance and certificate management.

Traditional authentication Mechanism

One factor authentication almost using username and password as the credential for the user, figure 5 view the authentication process.

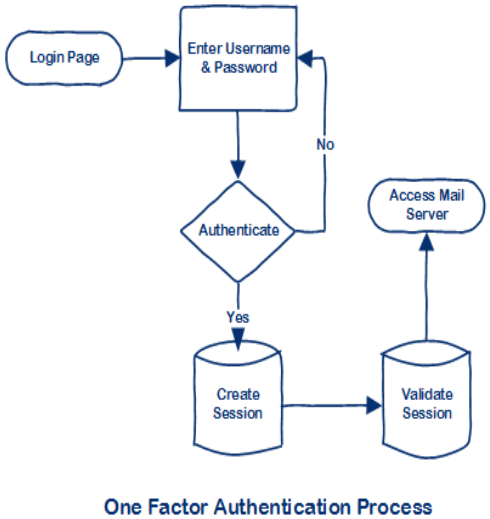

Figure 5: One factor Authentication Process

IV. SECURE MAIL USING CLOUD SOFTWARE AS A SERVICE (SMCSAAS).

This research proposed **S**ecure **M**ail using **C**loud **S**oftware **a**s **a** **S**ervice (SMCSaaS). This model is different from the traditional Email. SMCSaaS similar to SaaS model access using web services, as it requires two essential features encryption and sophisticated authentication. SMCSaaS is based on Identity-Based Encryption (IBE) technology and uses two-factor authentication instead of single-factor authentication. Mechanisms like passwords are vulnerable to many security threats, but two-factor authentication increases the information security as it uses two authentication tokens during the authentication process. Tokens are bound together and required to be authenticate simultaneously.

The first part of SMCSaaS is IBE that contains private key generator(PKG). Challenges and issues on exact Public Key Infrastructure (PKI) scheme are decreasing process cycle and limit required resources. Email security process that handles user identity as a public key with the corresponding private key is generated by Private Key Generator in both send and receive email directions is described in Figure 6.

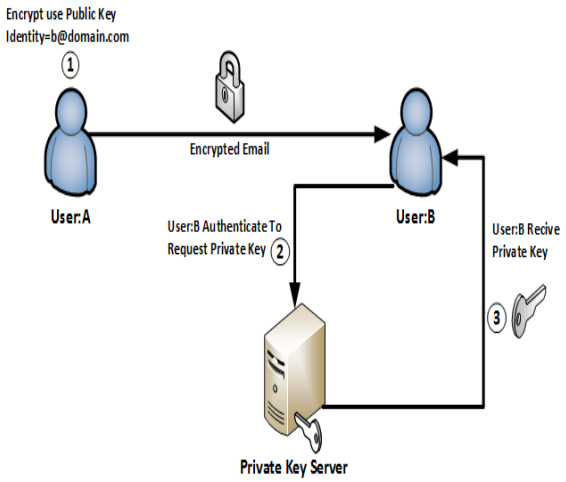

Figure 6: New Model Mail Flow with Private Key Generator

The IBE Mail Flow Process mechanism uses the following sequence

- User A composes a new email to User B.
- The PKG Server generates a secure random key based on symmetric encryption requests IBE public key for the recipient and his identity to encrypt the email.
- The encrypted email is sent to an email server as normal email delivery and stores the message in the encrypted form.
- User B is authenticated by Private Key Generator (PKG) server to receive the private key to decrypt email message.

The decryption cannot be perform without user identity involvement. The second part of SMCSaaS is using two-factor authentication for email accounts. Figures 7 views the two-factor authentication process.

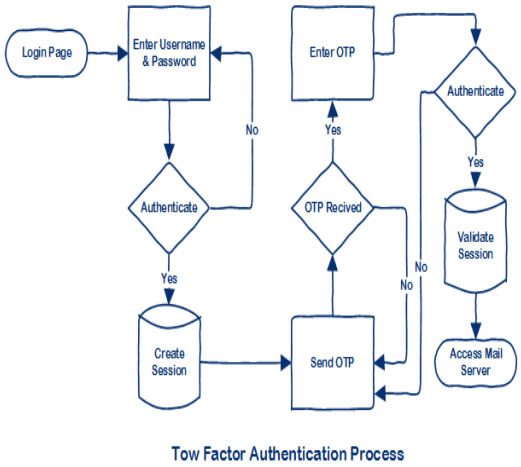

Figure 7: Two-factor authentication with OTP Process

The first authentication is a regular authentication for email system. The second authentication needs preparation, the preparation is registration of a new device refer to as token device. Must be registered once to receive One-Time password (OTP) on token device. The second authentication is one time usage password sent to the token device.

V. DISCUSSIONS

The following table views operation comparison between SMCSaaS and Symmetric Key Management and PKI components of traditional e-mail systems.

Criteria	**Symmetric Key Management**	**PKI**	**SMCSaaS**
User Authentication	Single factor authentication required	Single factor authentication required	Two-factor authentication required
Encryption	Yes, with online connection required	Yes, without previous requirements	Yes, without previous requirements
Decryption	Yes, online connection required	Yes, previous enrollment required	Yes
Integration with infrastructure	Requires decryption lookup	Very Complex	Simple, as it is non domain related certificate.
Scalability	Limited	Limited, complex	Easy, as it requires limited number of servers.
Key Infrastructure	Required Complex infrastructure	Required Complex infrastructure	Simple infrastructure
Key Repository Database	Required	Require large database	Not required, as it doesn't need repository database
Private Key Transport	Required	Not required	Require Secure connection
Computing Resources Requirements	Medium	High	Low, as it uses short key

SMCSaaS security analysis.

This section lists common risks and their countermeasures in SMCSaaS.

Sniffing, Packet sniffing allows attackers to capture data when transmitted over a network. The countermeasure is using cryptography mechanism to prevent an attacker to access the data.

Session Hijacking, is the exploitation of a valid session to have unauthorized access to information or system. The countermeasure is encryption of the data passed between the parties as well as using long random number or chain as the session key prevent session hijacking.

Eavesdropping, sniffing on network layer attack by capturing packets from the network transition and reading data content to access sensitive and confidential information. The countermeasure is cryptography mechanism to prevent an attacker to access the data.

Man in the Middle, attacker, secretly relays and possibly alters a direct communication between two parties. The countermeasure is two-factor authentication provides additional security controls by using OTP to prevent attackers from access information even if user password is known.

Phishing occurs when an attacker fraud the user credential or account information. The countermeasure is two-factor authentication OTP.

Password Theft or Discovery, in a case of password theft. The countermeasure is two-factor authentication mechanism through e-mail password and OTP requirements.

Replay Attacks, occurs when attacker hacks the connection between the server and user and takes the authenticated information or sharing key and then

reconnect to the server with that information. The countermeasure is OTP password that expires after a very short time.

Social Engineering Attack, is to manipulate and fraud users to discover confidential information like user credential. The countermeasure is two-factor authentication mechanism as OTP.

Token Theft or Discovery, is physical token loss so the attacker can access authentication token. The countermeasure is Token deregistration in two-factor authentication that provides blocking the physical token.

Brute force attack, the attacker or malware tries to access system systematically entering is all possible characters' combinations. Of OTP in two factor authentications.

Dictionary attack, in case if Dictionary attack identity's user password the attacker cannot access system because. Of OTP in two factor authentications.

VI. CONCLUSION

The proposed SMCSaaS imposes extra security steps to the traditional e-mail system. The Model overcome the distribution of PKI over Cloud multi-tenants. The integration between Private Key Generator (PKG) and two-factor authentication need uses one-time password to enhance security. Also, low technical support team is required as less of platform resources are needed.

Two-factor authentication dramatically improves the security of email server and personal information store. This is an extra layer of email security server to ensure authentication even if someone hacks the password. Also, Non repudiation benefit obtained by using OTP.

Private Key Generator (PKG) solve confidentiality and integrity security problems by providing policy-based encryption, client mobility. Also, short key decreases the requirements for hardware and computing resources without compromising security. The reason is that generated key with length 256-bit ECC provide same security level of key with length 3072-bit RSA in PKI.

REFERENCES

[1]. Results of International Data Corporation (IDC) survey ranking security challenges2010.

[2]. Rahul Kale, Neha Gore, Kavita, NileshJadhav,SwapnilShinde " Review Paper on Two Factor Authentication Using Mobile Phone" InternationalJournal of Innovative Research and Studies, Vol. 2,Issue 5, pp. 164 - 170, May 2013.

[3]. Stallings., (2003).Cryptography and Network Security Principles and Practices, Prentice-Hall of India PrivateLimited, 3rd Edn.

[4]. John R. Vacca(2004), Public Key Infrastructure: Building Trusted Applications and Web Services: CRC Press.

[5]. J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. OpenPGPMessage Format. RFC 4880 (Proposed Standard), Nov. 2007. Updated byRFC 5581.

[6]. Fabio Alessandro Locati,OpenStack Cloud Security,Packt Publishing, July 2015.

[7]. Anthony T.Velte, Toby J. Velte& Robert Elsenpeter. (2010). Cloud Computing A Practical Approach, Tata McGraw-Hill Edition.

[8]. Krutz Ronald, Dean Vines & Russell. (2010). Cloud Security A Comprehensive Guide to Secure Cloud Computing: Wiley Publishing.

[9]. Rittinghouse John &Ransome James. (2009). Cloud Computing Implementation Management and Security: CRC Press.

[10]. Stanoevska-Slabeva Katarina, Wozniak Thomas &RistolSanti. 2009. Grid and Cloud Computing: A Business Perspective on Technology and Applications: Springer.

[11]. J. Heiser& M. Nicolett. (2008). Accessing the Security Risks of Cloud Computing: Gartner.

[12]. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS), http://iase.disa.mil/stigs/index.html.

[13]. Reese, George, Cloud Application Architectures, Sebastopol, California: O'Reilly Media, 2009.

[14]. Daryl C. Plummer. (2010). Cloud Computing: Defining and Describing an Emerging Phenomenon: Gartner.

[15]. Miller & Michael. (2008). Cloud Computing: Web-Based Applications that Change the Way You Work and Collaborate Online: Que.

[16]. Ahson Syed, Ilyas Mohammad. (2010). Cloud Computing and Software Services Theory and Techniques: CRC Press.

[17]. Ommeren Erik, Duivestein Sander, DeVadoss John, Reijnen Clemens &Gunvaldson Erik. (2009). Collaboration in the Cloud: How Cross-Boundary Collaboration Is Transforming Business: UitgeverijKleineUil.