OVERCOMING EMAIL SECURITY ISSUES IN CLOUD USING SECAAS

E.J.Thomson Fredrik¹ & Vijyendra Karpatne²

Abstract: Top problems are specified on major email based cloud development application in order to provide email services to the organization. There are lot of email security services like Email Threat Prevention (ETP) Cloud service, Advance Threat Intelligence (ATI) and Data Loss prevention cloud services are available for cloud network but all these services create countless complications in cloud like email message security issues, compliance issues, breaching issues, broken link issues and issues with location of data etc. All the organizations must need a solid answer to these questions before they can completely embrace the cloud based email. In order to overcome the several issues with the email security in cloud, we propose SecaaS to enrich email security and confirm strong encryption, logging, theft detection, malware filter and early malware detection on email messages.

Keywords: Cloud-based email; Organizations; Security, ETP, ATI

1. INTRODUCTION
Email plays a dynamic role in business communication among parties. Customers, organization staff and service providers can interact with each other effectively via email. The data can be transferred very easily between senders and receivers over the Internet. The email message can be stored, received, replied to or forwarded as per the user’s choice. The capabilities we find in email message are so worthy and making this to be opted for official communication for many organizations. The email is being used as a personal message communication too as the email facility can be used at different types of software clients and almost on all web browser. Safeguarding email in cloud is very equal to safeguarding email in the organizations or enterprise. Cloud based email security as a service (SecaaS) has unique capabilities which can really secure the emails which are travelling every corner in cloud environment. Cloud based service providers must ensure the security and authenticity of the email message.

The email security services provide the possible assistance to customers in order to communicate without worrying about security of the message and data they send over internet using their email. It’s the duty of cloud based service provider to monitor all spams, malware or any kind of threats using email as a channel. The cloud service provider must provide the email user interface or possible help to an end user.

The high amount of email threats are not new things we are experiencing, but the way it attacks has changed significantly. In the recent past, the number of embattled attacks in the cloud network has increased considerably and most of them were hosted through email system. It is found very difficult to detect the targeted attracts and traditional anti-malware tools are not capable of handling them. Cloud based email safety solutions which are being offered by cloud service providers are not completely correct to keep the organization harmless. Most of the cloud-based email safety solutions offer only basic anti-malware capabilities, which can’t detect newly invented attacks. The reason is that these cloud-based email safety solutions do not include advanced threat protection capabilities. Thus the need of SecaaS becomes mandatory in-order-to fight against the newly discovered classy attacks on the email within cloud.

2. LITERATURE REVIEW
In [1], Y. Chan et al, 2010 revealed that it is a general thought that the cloud providers maintain the security within the cloud but on the other hand SecaaS allows user to rely on the security measures provided by the cloud. He also revealed that the SecaaS treats the security as a service and the organizations or user can enroll to that service as per their demand or requirement.

In [2], S. Creese et al, 2009 discussed how the maturity model for the security and protection for the email message or data in the cloud. The security risks were discussed and it was revealed that the cloud providers use the different models to provide the security for the email messages which can allow minimizing the security risk on the email messages.

In [3], Guilbault 2009, the intrusion detection system was implemented using amazon cloud service. This played a very important role in order to convince organizations and users that the email security within the cloud can be made secure as before. With the help of anti-malware system, the detections on the malware attacks were proven and filtered using the intrusion detection system.

¹ Assistant Professor, Dept. of Computer Sc, Karpagam Academy of Higher Education, Coimbatore, India
² Research Scholar, Dept. of Computer Sc, Karpagam Academy of Higher Education, Coimbatore, India
In [4], Recordon and D. Reed et al, 2006 revealed the open id concept and for identity management in cloud. For the email security, the identity protection is so important hence it was implemented as an underlying protocol to have complete identity check on the email message to ensure that the emails are not delivered to the wrong recipient or the malwares were not added to the broken links before the email message is delivered.

In [5], L. Yan, C et al, 2009 discussed the federal identity management to strengthen the email security in cloud by using the public cryptography. There were situations where one cloud used to contain multiple cloud where the identity was a big challenge.

In [6], J. Vijaya Chandra et al, 2014 discussed the attacks and threat on the on the data which can be transmitted with spoofed and the fake IP address. Their idea leads to have the identity security on the email message in the cloud system.

In [7], S. Ruj, et al, 2014 revealed access control with anonymous authentication of data stored in clouds. The malware attacks are made as an authorized client and try to get the required data from the server. In the reverse action, the attack is made as and actual service provider and then steals the private information before delivery.

In [8], J. Vijaya Chandra, et al 2015 exposed the protection from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform. In the cloud network, the successful relationship is provided between devices. With the help of spoofing, and assailant can outbreak the approved devices of the same network which has positive relationship recognized without getting agreement from legal users.

In [9], Vance A et al, 2014 discussed Advanced Persistent Threats detecting targeted attacks in cloud computing. The learning about the sequence number was discussed. This is the another phase for TCP inoculation after addressee linking details with port are known. In cloud, the invaders try to attack with unlike off-path technique to steal the information and get the sequence number. The attacker cannot see the sequence number directly so different types of efforts are made to get that. The sequence number provides the permission to attackers to inject the data into connection by acting as a server.

### 3. CHALLENGES IN CLOUD FOR EMAIL SECURITY

When we discuss the email security in cloud, lot of issues and challenges come across. Sometimes it really difficult to imagine if those problems can ever be overcome as daily a new malware attack on email is being invented. As the email is the only medium where the malware attack can be made very easily and that too in cloud where millions and millions of email flows on daily basis. It’s very easy to add a malicious email links to the original email and deliver to the recipients.

#### 3.1 Data Security

Broad ranges of security threats are introduced in cloud. Security threats includes the possibility for the cloud provider being hacked, the malicious action by an employee of the cloud provider and exchanging the data in cloud environment. Enormous number of threats is getting introduced in cloud because of email exchange in widely manner.

#### 3.2 Compliance

All the enterprises are bound to address the compliance process and must follow the rules and regulations of any country. All the regulatory requirements must be within the mandatory list to address both domestic and international applications. The industry specific regulations like HIPAA, GLBA. These commitments ensure that the organization will follow all the rules and regulations which are kept in place by the government.

#### 3.3 Data Placement

The data placement says where the data will reside. As the regulations are very strict, the businesses which has world-wide presence are challenged with the fulfilling the data residency guidelines. Organizations must talk to their cloud service provider about the data residency before any contract is signed between organization and the service provider. In most of the cases, the cloud service providers’ charges lots of money from the organization to install costly infrastructure in each location. The email messages are significantly analyzed at higher cost before they are placed in specific jurisdiction.

#### 3.4 Unauthorized Leak

All the cloud service provider should be bound with the legal process which gives access to private emails. The main challenge is that the legal process also does not cover all the aspects where organizations do not have loop holes to share the data via or to the unauthorized means.

### 4. PROPOSED SOLUTION

The implementation of SecaaS will give the confidence to the cloud service providers so that the cloud service provider can tell organizations that they are good to get the end to end protection through every step of the email transition in the cloud. The proposed solution contains considering the SecaaS as a straight forward and compulsory service for cloud-based email and its security.

As a proposed solution, we have added a feature on the AES encryption algorithm, since this is considered as one of the most secure algorithm for email security. We have applied the algorithm to encrypt data in fixed size block at a time. The key bit encrypts or decrypt block in 128 bits. At every round plain texts are converted into cipher texts. The proposed solution
enables the security using SecaaS because it allows 192-bit encryption and decryption. Total of 12 rounds get completed for converting the plain text into cipher text. Only 10 rounds of conversion were possible in the existing algorithm. In the proposed solution, the key size is too large hence it automatically more secure. Moreover, it is never slower than other encryption algorithm. This solution provides more flexibility to choose key process and encryption process. This can be used without many restrictions.

The encryption algorithm involves the below steps
Step 1 – Originate the set of round keys on cipher key.
Step 2 – Get block data and initialize the array. The block data is the plaintext here.
Step 3 – Add the initial round key in the starting of array.
Step 4 – Perform 10 rounds of manipulation and perform Sub byte, shift row, mix column and round key stages.
Step 5 – Perform 11th round of manipulation separately.
Step 6 – Perform 12th round of manipulation to handle 192-bit. This round has slight different manipulation than other rounds. This will be considered as the FINAL round.
Step 7 – Get the Cipher text as a final array state.

The decryption process to get the plaintext from the cipher text involves the reverse process which we followed in encryption process above.

The encryption algorithm involves the below steps
Step 1 – Perform initial decryption stages Inverse_round, Inverse_shift, and Inverse_subbyte
Step 2 – Perform ten full decryption stages Inverse_round, Inverse_MixCols, Inverse_shift, and Inverse_subbyte
Step 3 – Perform 11th round separately.
Step 4 – Perform Final 12th decryption round
Step 5 – Obtain plain text.

The proposed approach incorporates using all available methods of email security, protection, email message encryption, logging, handling malicious links, early malware attacks.

![Fig.1 Email security with SecaaS in Cloud Computing](image)

The above picture demonstrates that the security control policies are applied on the email message in cloud. Answerability is provided since it offers email security measures, logging and auditing. As we implement SecaaS using data-centric approach, which will emphasis the security on the email message rather than the security of networks. Hence the email messages would be scanned right from the beginning. This data centric approach will also help to detect the new and real time attacks on the email message as it exchanges the information from MTA, the mail transfer agent. This approach of SecaaS enables the system to have information exchange from the remote email system for deliveries.

The challenge in the proposed approach aims at analyzing the real-time link which ensures that the malicious links are not delivered to the recipient’s mail box. In the absence of SecaaS security measures, shorts links are redirected multiple times within cloud before it reaches to the final destination. Just before delivering the email messages to the recipients, multiple
email links are consolidated and delivered. Implementation of SecaaS gives strength to the system to trace back the broken or redirected link and protect email so that the malicious links are not delivered to the mailbox. SecaaS enhances the ability of the system to prevent sensitive email. This service can be used to define which email should be encrypted based on the message content. The SecaaS triggers an automatic encryption process if it requires to be applied to an email. If the SecaaS is absent, then the services will not have any contingency plan if the email is attacked.

The below picture shows the email system in Cloud without the application of SecaaS.

![Email security without SecaaS in Cloud Computing](image)

The strong benefit with email SecaaS is that either it can be provided as a complete outsourced email service or as a specific service as per the organization’s need. The email service and the security solutions are provided by the vendor in complete outsourced email service implementation. Whereas as a specific service, the organization demands the upgrade in the in-house email with security services from cloud-based security features. This character of SecaaS increased its flexibility and reaction within the cloud network.

Using SecaaS, the system gets intellect from various streams of email messages and able to deploy the algorithm changes to many organizations at a time. These kind of quick responses in order to fight against the malware attacks on email message are benefitting all the organizations and users who are using email messaging in cloud-based system. SecaaS allows the integration into the organization’s identity management system along with two factor authentication. This provides organization a strong infrastructure and let them access email using only encrypted protocols to ensure the high level of security on email messages.

SecaaS provides the ability to overwrite the email message and just not freeing up the space. Because of this ability, this solution will be the safeguard for the email message in the cloud-based network. SecaaS provides the operation and configuration management so that the events can be logged properly in cloud network and it can be analyzed thoroughly in case of unusual event. The strong recommendation for SecaaS is made because it can use cloud scale and on-demand resources to analyze incoming email message in cloud. When the incoming email messages in cloud network are gathered and analyzed, the malware attacks are minimized and the email messages become more secure.

5. RESULTS AND DISCUSSION

SecaaS have numerous advantages as soon as it is applied to the email message. The SecaaS increases the poise that the email messages are completely secured. We achieved the outcome from the SecaaS implementation on the email messages using the application of data-centric approach. SecaaS guarantees that there is no damage to the email messages travelling within the cloud network. SecaaS provides the additional number of rounds of converting the plain text into chipper texts, so the theft detection ability becomes more. The below graph will demonstrate that the implementation of SecaaS has quite a lot of benefits over other email security techniques.
In the above graph, it is clearly shown that the SecaaS gets advantages over other services which will help to choose the best cloud service for email security. SecaaS performs 12 rounds of encryption and decryption when it works with 192 bit fixed size block. This makes the encryption power better. SecaaS provides the ability to handle key setup and encryption process which gives the opportunity to perform better identity security and good traffic illustrations. SecaaS uses a set of protocol to filter the spam. These features include not only the content and header filters but also the permission and some user defined rules. SecaaS provides to handle the access control features so that the login security can be strengthened. When email is secured in cloud with SecaaS, the stealing rate of email is decreased drastically. The email theft has been the biggest fear without the security services of SecaaS. Logging security is stronger with SecaaS services because it provides multi-layer approach for authentication and fraud detection. No other services except SecaaS provide the strong encryption power algorithm on the email in cloud before it is delivered.

6. CONCLUSION
There are many recent applications where cloud computing plays a very important role. The applications which are used for Email system, weather forecasting, astronomical solutions etc. are the leading recent application which gains lots of popularity in cloud network. The proposed SecaaS explanation combines integration and security in a solitary dais. SecaaS delivers the model for integration of security services into cloud computing infrastructure. SecaaS provides all the detection and prevention of spams. SecaaS deals with the alerts and threats which is a common concern for an email user. SecaaS offers to have WAF (web apps firewall) and SIEM (security info and event management) so that the different tasks can be handled by the different modules with complete ownership. SecaaS provides more control over the security of data and contents which are embedded in the email body along with the attachments. SecaaS overcomes the several issues with the email security in cloud by providing security features such as strong encryption, logging, theft detection, malware filter and early malware detection on email messages.

7. REFERENCE