# Email Encryption

Geeta Chopade[1],Asmita Sawant[2],Bharati Makar[3], Nilam Munde[4], Mrs.Sayali Kshirsagar[5].

[1] *Student, Computer Engineering, Marathwada Mitra Mandal's Polytechnic , Thergaon ,Pune411027,Maharashtra, India*

[2]*Student, Computer Engineering, Marathwada Mitra Mandal's Polytechnic, Thergaon ,Pune411027,Maharashtra, India*

[3]*Student, Computer Engineering, Marathwada Mitra Mandal's Polytechnic, Thergaon ,Pune411027,Maharashtra, India*

[4]*Student, Computer Engineering, Marathwada Mitra Mandal's Polytechnic, Thergaon ,Pune411027,Maharashtra, India*

[5] *Professor, Computer Engineering, Marathwada Mitra Mandal's Polytechnic, Thergaon ,Pune411027,Maharashtra, India*

**ABSTRACT**

*We describe any story solution in unifies strengths of previous approach and also provide additional information or features for users having much flexibility for e-mail communications. Our new technique called XML e-mail is a new XML e-mail format which provides the e-mail security. It provides security to our e-mails. It is combination of XML Security and Web Services Security, which provides a better protection to our messages as well as interoperability and high protection compared to the other systems. This is client server architecture where there would be a client application which will talk to web service running on the server for communication based on cryptographically signed XML messages. An email client is an email program which will have a GUI like Outlook Express, for sending, receiving and organizing your email messages. Every client needs to be authenticated to the server. A login screen will be provided where will be provided where user will put username and password to get into the system.*

**Keyword :** -*Sender, Receiver ,Encryption ,Decryption.* ,email security

## 1. INTRODUCTION

Email is stand on Electronic Mail, it is technique for sending digital messages for human use. Email system is based on a store-and-forward technique. That technique computer server system accept the message then forward, deliver and store the message in user side. It is rarely cases to delivered message sending by sender to receiver device. Text is a way to communication medium to communicate with each other and we can also attach the multi-media files which were standardized in with RFC 2045 through RFC 2049 called Multipurpose Internet Mail Extension (MIME ) Email has two parts one is Header part and another is body of the message The Header part contains the control information about sender as well as one or more Receiver addresses .We can add additional information like subject header field. Email messages are sending by sender is not secure do over the internet. Often Information sending by us it is important and valuable such that the effective Protection is enviable in order to prevent messages for secures thee-mail from Unauthorized users These days the large

numbers of e-mails security mechanism are developed for unauthorized users .They build a solid source for secure –mail communication.

## 2.GOALS AND OBJECTIVES

Our main aim is to secure email message in the form of XML, format by encryption and signature in its header part and also body part by using a session key for encryption purpose and then sending this to the receiver. After encryption session receives encrypts this using the receiver's public key. Signature present on its header and body part by using a session key for encryption and then sending it to the receiver. When the sender sends the encrypted message this time receiver encrypts the same using receiver public keys.

## 3. PROPOSED SYSTEM

This is client-server architecture for communication based on cryptographically signed xml messages.
It achieves higher security and interoperability when combined with well known standards of XML Security along with digital signature, compared to the previous solutions.
Therefore our main focus is to develop an email system which will encrypt a mail along with all the headers of that particular mail.

## 4. STEPS

1. It convert the text message into XML format before encryption.
2. It encrypts the whole content of message along with headers which acheives Confidentiality.
3. After encryption, it gets digital signature which achieve Authencation and Integrity.

## 5.PROCESS OF SENDING EMAIL

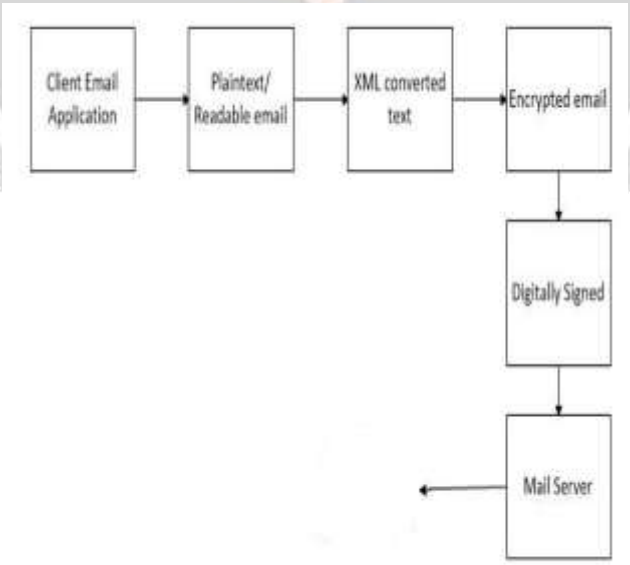


**Fig.1- sending email**

## 6. PROCESS OF RECEIVING EMAIL

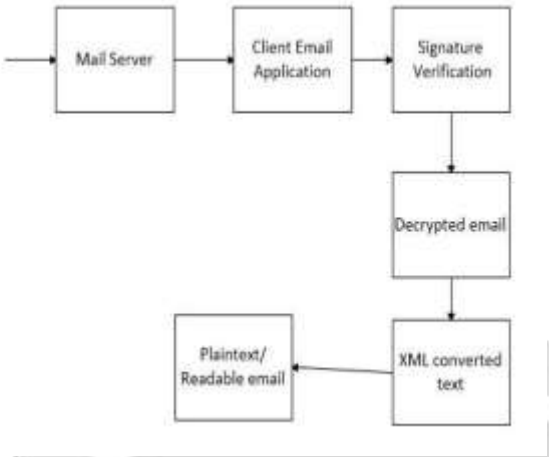


**Fig.2-receiving email**

## 7. ADVANTAGES OF EMAIL ENCRYPTION

1. Your device and your personal data are sefe
2. No one can hack your personal information
3. Simple to implement
4. AES algorithm are required for the data is encrypted and decrypted
5. Less resources needed to maintain it
6. Authenticity and Protection of the Message
7. Easy to replay
8. International Availability
9. Easy Sending of enclosures
10. Convenient Sending to multiple recipients

## 8. DISADVANTAGES OF EMAIL ENCRYPTION

1. In case, if your forget Passcode or PIN or Password then you have to format it.
2. Encryption/decryption can be resource intensive on constrained device.
3. A secure provisioning of the key to the MQTP client must be implemented.
4. Do sent prevent from man-in –the-middle attacks and replay attacks.
5. Encryption works well is situation where your cant securely shear a key, like over the internet.
6. It relates to key is that the security of the becomes the security of the encryption key. Loss that key and you effectively lose your data.

## 9. SYSTEM REQUIREMENTS

Hardware Requirements:

1. Processor :Intel i3
2. RAM: 4GB
3. Hard disk:100 GB

Software Requirement:

1. Operating system:32bit or 64 bit window 7 and on words
2. Coding language: Java J2EE
3. IDE: Eclipse Kepler
4. Database: MYSQL

## 10. FEATURE OF EMAIL ENCRYOTION

1. In today electronic world, email is critical for business that want to stay competitive, productive and efficient. While this reliance on technology is a great convenience to employees, coustomers and venders ,it can also be a great source of risk if not adequately prodected.
2. Encryption using than strong email security important than ever.
3. Hosted email services often provide basic security such as virus and spam protections but depending on your industry.

## 11. MOTIVATION OF THE PROJECT

1. Once logged in successfully he will see the email application this application will have following functionality:
2. Compose e-mail
3. Inbox
4. Received e-mail display
5. Option to view encrypted XML conversion of email message
6. The scope of the windows is vast. We are going to target only above mentioned features. The e-mail sever is a web service hosted on the IIS on a different machine called as web server

## 12. FUTURE SCOPE

In today's world the protection of sensitive data is one of the most critical concerns for organizations and their customers. This, coupled with growing regulatory pressures, is forcing businesses to protect the integrity, privacy and security of critical information.. No one would dispute that cryptography and encryption are new technologies. It was true in particular ago and it is still true today encryption is the most reliable way to secure data. National security agencies and major financial institutions have long protected their sensitive data using cryptography and encryption.

## 13.CONCLUSION

In this project, we developed a XML-based e-mail format to provide more security properties. Using XML structure the message is efficient for processing, archiving and searching. Using XML conversion and XML encryption, the client implementation simplifies and makes the signature and encryption readable for a natural person. Additionally XML e-mail can be transported via the existed systems. As our future work, we will extend the current model to provide better counter measures against the spam e-mails, add more security properties to satisfy the legal requirements for advanced digital signatures (e.g. using X Ad ES) and extend the existing transport systems for more efficient transport of XML e-mail.

## 14.REFERENCE

1. Lijun Liao, Jorg Schwenk, Secure Emails in XML Format Using Web Services, Fifth European Conference on Web Services, Dec 2007. [Online]. Available: http://ieeexplore.ieee.org/document/4399742/
[2] RA. K. Saravanaguru, Securing Web Services Using XML Signature and XML Encryption, IJETTCS 2011. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.0910.pdf
[3] Ms Sushma phalke , Prof. Mahesh Dube, Securing Web Services Using XML Signature and XML Encryption, IJETAE, April2013.[Online].Available: http://www.ijetae.com/files/Volume3Issue4/IJETAE_0413_81.pdf
[4] B. Ramsdell (Editor), Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, IETF RFC 3851, July 2004. [Online]. Available: https://www.ietf.org/rfc/rfc2633.txt
[5] Abd El-Aziz Ahmed, Kannan Arputharaj, A Comprehensive Presentation to XML Signature and Encryption , ICRTIT 2013-IEEE Xplore. [Online].
Available:https://www.researchgate.net/publication/252067529_A_Comprehensive_Presentation_to_XML_Signature_and_Encryption
[6]R.Housley,CryptographicMessageSyntax,IETFRFC3852,July2004.

[7]M.Bartel,J.Boyer,B.Fox,B.LaMacchia,andE.Simon,XML-SignatureSyntax andProcessing,W3CRecommendation,Feb.2002.[Online].Available: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
[8]T.Imamura,B.Dillaway,andE.Simon,XMLEncryptionSyntaxandProcessing, W3CRecommendation,Dec.2002.[Online].Available: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/