International Journal on Applications in Engineering and Technology
Volume 8 : Issue 2 : May 2022, pp 82 – 86 www.aetsjournal.com ISSN (Online) : 2455 - 0523

ADOPTION OF ANTI-EMAIL SPOOFING USING GEO-FENCE FRAME WORK

PRAVEEN KUMAR S[1], SANTHOSH S[2], TAMIL THENDRAL S[3], FARITHA BEGUM M [4]

[1, 2, 3] Undergraduate student, Department of Computer Science and Engineering, Pavai College of Technology
[4] Assistant Professor, Department of Computer Science and Engineering, Pavai College of Technology

Abstract: *- – This project proposes the establishment of a blockchain-based system for managing medical records called Med Chain. Med Chain is intended to improve current systems by providing patients with interoperable, secure, and effective access to medical information. For managing transactions and limiting access to electronic medical records, Med Chain uses timed-based smart contracts. It uses modern encryption techniques for further protection, as well as an unique incentive scheme that rewards health practitioners for their efforts in keeping medical records up to date and producing new blocks.*

Key words: Med chain, interoperable, secure, electronic medical records.

I. INTRODUCTION

End users' everyday lives are growing more and more dependent on data exchange and protection in order to access various systems, services, and apps. In actual email services, data exposure regularly takes place. In safe data transfer medium, authentication and copyright protection of multimedia materials have long been issues. With the increased use of the Internet and digital technology, the issue has gotten worse. Making copyright protection is more challenging and complex, though. As a remedy to the copyright protection issue, digital watermarking was proposed. Both watermarking and encryption techniques are used in the suggested method employing Geo-fence technology for effective material sharing.

In digital material like photographs, watermarking is used to conceal information like secret information. Data security is achieved using encryption methods. In order to prevent unwanted access, information is encoded using encryption, making it impossible for those who are not allowed to view it. Finally, using the inbuilt data verification mechanism, an authorised user can extract the decryption key. When user information does not match embedded information, unlawful or unauthorised access can be recognised. This suggested application aids in the detection of unauthorised access and the prevention of content redistribution in email environments. Additionally, you may offer group data sharing based on a rules-based strategy employing a machine learning algorithm, as well as a mail delivery and acknowledgment system.

Network protection is an extensive time period that covers a mess of technologies, gadgets and processes. In its only time period, it's far a hard and fast of policies and configurations designed to shield the Integrity, confidentiality and accessibility of laptop networks and records the usage of each software And hardware technologies. Every organization, irrespective of size, enterprise or infrastructure, requires a diploma of community protection answers in location to shield it from the ever-developing Landscape of cyber threats within side the wild today. Today's community structure is complicated and is Faced with a danger surroundings this is continually converting and attackers which are continually looking to Find and make the most vulnerabilities.. These vulnerabilities can exist in an extensive range of areas, Including devices, data, packages, customers and locations. For this reason, there are numerous Network safety control equipment and packages in use these days that cope with character threats and exploits and additionally regulatory non-compliance. When only some minus of downtime can Cause enormous disruption and large harm to an organization's backside line and Reputation, it's far critical that those safety measures are in place.

1.1 OBJECTIVE

Email Services had been began out to turn out to be an end result of the opposite improvements Within the Internet programs technologies, in addition to the unconventional infrastructures and systems which are dominating today's WWW. Cloud electronic mail offerings had been these days

delivered to the public on account that much less than a decade. This evolution began out while the primary cloud primarily based totally utility Send mail" turned into delivered. To make electronic mail common unique steady and private, electronic mail servers Protocols offer an inexpensive safety however numerous limitations have. This assignment discusses Limitations of electronic mail safety protocols, analyses and evaluates their effectiveness in electronic mail Server. It additionally proposes strategies to enhance performance of electronic mail servers in detecting spoofed e-mails from domain names that don't observe any fashionable anti-spoofing protocol. Further, it offers consequences of research achieved to appraise electronic mail person practice; information of safety protocols and their self belief in electronic mail system.

1.2 PPROJECT DESCRIPTION

A mail server (also known as a mail transfer agent or MTA, a mail transport agent, a mail router or an Internet mailer) is an application that receives incoming e-mail from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. In this module we can create the framework like as mail server. This framework contains server and multiple users. Server can maintain all user details. Users easily upload the files in inbox and also share the data anywhere and anytime. Because it is difficult for an intruder to manage multiple account and send these kinds of message. This is done for avoiding early detection of spammers. A large frequently. This work focuses on PRE for secure media sharing in the encrypted cloud media or variety devices such as mobiles, laptops, tablet computers desktop computers comes into popular there by use of social networking is also increased. Spamming can be spread to new technologies rapidly. Micro-blogging services like twitter became a prominent platform for many activities like campaigning. Spam promoting campaigns are need to be detected.

II. SYSTEM ANALYSIS

A. 2.1 Existing System

An e mail server, or sincerely mail server, is a software or laptop in a community whose sole motive is to behave as a digital put up office. The server shops incoming mail for distribution to neighborhood customers and sends out outgoing messages. To aid get right of entry to manage for secure facts sharing within side the encrypted cloud media centre, essentially there are extensively famous Approaches within side the literature. The first type of technique is primarily based totally on attribute-primarily based totally encryption (ABE) wherein a content material issuer can specify an related get right of entry to shape over attributes, and Thus the cipher textual content saved within side the cloud can most effective be decrypted with the aid of using customers whose attributes fulfil That get right of entry to shape. The latter type is primarily based totally on proxy re-encryption (PRE) wherein the cloud Acts as a proxy to assist delegate the decryption rights to legal customers in a controllable Manner. Compared with ABE, PRE may be extra effective within side the experience that, in ABE the Content issuer wishes to download, decrypt, and re-encrypt facts whilst get right of entry to guidelines alternate frequently. This painting makes a speciality of PRE for steady media sharing within side the encrypted cloud media Centre. Digital watermarking is a type of approach that offers possible answers to the hassle of tracing unlawful content material redistribution. Typically, it really works with the aid of using first imperceptibly embedding a Unique watermark in every replica of the obvious media content material, and later detecting the life of The specific watermark from a suspicious replica for traitor tracing. Earlier watermarking schemes had an issue though: a malicious content material issuer should body a person with the aid of using unfairly accusing Him of leaking a media object. To resolve this hassle, a person must be capable of argue towards that in the course of a dispute. While making sure traceability, honest watermarking similarly affords fairness .To save you the content material issuer from framing customers. However, for steady cloud-primarily based totally media Sharing, a way to well follow honest watermarking to allow honest traitor tracing isn't always but clean and stays explored.

2.2 PROPOSED SYSTEM

Security in Information and Communication Technology is described as good enough safety of records towards unauthorized disclosure, unauthorized amendment and unauthorized withholding. It has a near courting with privateers as insecure records cannot make certain customers privateers. In E-mail messaging, safety may be described because the cap potential of the device to offer I) privateers, ii) sender authentication, iii) message integrity, iv) non-repudiation, and v) consistency. E-mail device includes some of hardware and software program additives that comply with a few described requirements. These requirements additionally consist of requirements for message addressing and formatting and some of associated protocols. Simple Mail Transport Protocol is the number one and the maximum

extensively followed protocol for email delivery. It lacks safety capabilities for privateers and authentication of sending party. E-mail in simple textual content passes from sender to recipient thru many intermediaries like routers, and mail servers. It is thus, inherently prone to each bodily and digital eavesdropping as malicious attackers who benefit get admission to to those intermediaries can examine e-mails. Further, E-mail Service Providers (ESPs) have skills to keep copies of email messages even if those are deleted via way of means of the customers from their mailboxes. It has no mechanism to authenticate the sender or different depended on fields in any way. It does now no longer confirm or validate the senders email cope with or different header fields. As such senders can lie approximately their real identities, date and time of introduction of message, go back cope with and different info which bring about safety demanding situations of various types. In this project, we will put into effect the framework to authenticate the customers and additionally offer the safety primarily based totally on geo-fence framework. This framework consists of the watermarking, encryption and gadget studying techniques. Sender can ship the report and watermarked via way of means of discrete wavelet remodel set of rules and additionally encrypted the usage of AES set of rules. Then ship the report to suitable makes use of from the particular groups. And additionally ship notification approximately unauthorized get admission to.

III. MODULE

MODULE 1: EMAIL SERVER FRAMEWORK

A mail server (additionally referred to as a mail switch agent or MTA, a mail delivery agent, a mail router or an Internet mailer) is a utility that gets incoming email from nearby users. A laptop devoted to jogging such programs is likewise referred to as a mail server. In this module we will create the framework like as mail server. This framework incorporates server and a couple of users. Server can keep all person details. Users without difficulty add the documents in inbox and additionally percentage the records everywhere and anytime.

MODULE 2: DATA SHARING

Data may be allotted electronically in limitless ways. The maximum not unusual place of those is email and diverse records sharing offerings. By email, an attachment may be quick introduced to a recipient. E-mail messages characteristic high-quality while the variety of messages and those within side the communication is small. Data sharing offerings characteristic higher than email in conditions wherein there are numerous humans within side the communication or massive variety of messages sent. Messages do now no longer block email and document control is simpler and centralized. Conversations and documents may be saved so long as required. In this module, we will add the records in diverse form.

MODULE 3: SECURE THE DATA

The proliferation of virtual media over the net has been raised in previous couple of years. The improving utilization of digitization has given high-quality cause copyright issues. To address with copyright issues, virtual watermarking comes out as appropriate solution. Digital watermarking is procedure of putting watermark facts into host data. In this module, we will put in force discrete wavelet rework set of rules to watermark the content. Discrete Wavelet Transform is rework this is utilized in numerical in addition to purposeful analysis. In this rework, the wavelets are sampled with Fourier Transform is that it captures each frequency and region facts. In Discrete values. The primary gain of this rework over. Wavelet Transform, sign electricity concentrates to unique wavelet coefficients. After watermark the content, put in force AES set of rules encrypt the data. AES encryption or superior encryption standard is a sort of cipher that protects the switch of data.

IV. SYSTEM TESTING

4.1 Unit Testing

Unit checking out contains the set of checks done through an man or woman programmer previous to integration of the unit into a bigger system. The module interface is examined to make certain that statistics nicely flows into and out of this system unit. The neighbourhood facts shape is tested to make certain that facts saved quickly keeps its integrity for the duration of all steps in an algorithm's execution. Boundary situations are examined to make certain that the module operates nicely at barriers installed to restrict or limitation processing. All impartial paths thru the manipulate shape are examined. All error-dealing with paths are examined.

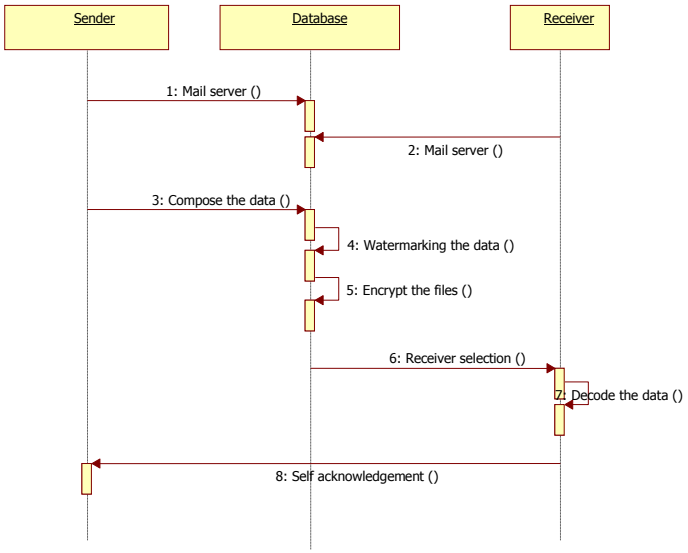
4.2 Block Box Testing

Black-field trying out is a way of software program trying out that examines the capability of a utility without peering into its inner systems or workings. This approach of take a look at may be implemented simply to each degree of software program trying out: unit, integration, machine and

acceptance. It is on occasion known as specification-primarily based totally trying out.

V. SEQUENCE DIAGRAM

A collection diagram in a Unified Modelling Language (UML) is a form of interplay diagram that suggests how procedures function with each other and in what order. It is a assemble of a Message Sequence Chart. A collection diagram suggests item interactions organized in time collection. It depicts the items and training concerned within side the state of affairs and the collection of messages exchanged among the items had to perform the capability of the state of affairs. Sequence diagrams commonly are related to use case realizations within side the Logical View of the gadget beneathneath development. Sequence diagrams are every so often known as occasion diagrams, occasion scenarios, and timing diagrams.



VII. CONCLUSION

Propose a mixed cryptography and watermarking strategies for stable transmission of data via E- Mail server. Discrete Wavelet approach is used for watermarking and AES cryptography is used for encryption purposes. The proposed approach isn't handiest designed to offer copyright protection; however, its miles proposed to offer integrity and authentication offerings for the media records primarily based totally on Geo-fence framework. It consists of the Machine mastering set of rules to select institution records sharing primarily based totally on region of institution. Therefore, its goal isn't to be strong towards amendment attacks; however its goal is to hit upon any unlawful sports at the watermarked data. The capacity of this approach is recognized to test if the integrity and authentication of the shared data are corrupted on the receiver end. At the receiver aspect the proposed approach detected this alteration and despatched a message to the content material issuer concerning unlawful distribution. And additionally offer mail shipping gadget to realize approximately popularity of mail at recipient aspect.

VIII. FUTURE ENHANCEMENT

In future, we will make bigger the framework to enforce in numerous cryptography algorithms and carried out in numerous applications. We aren't capable of discover any contacts to responsible CSIRT. Using the equal above-mentioned notifications approach, we despatched emails, of the attachment files, we needed to ship separate emails, one associated with SPF. Finally, a few CSIRT's modified their e-mail addresses in order that we acquired bounced emails. In overall, our revel in from the 2 notification campaigns suggests that reporting vulnerabilities via CSIRT's may be powerful however relies upon on its feasible effect and importance of affected resources.

REFERENCES

[1]. Abdelsatir, Eltigani B., and Mohammad H. Alrashdan. "On the Implementation of a Secure Email System with ID-**primarily based totally** Encryption." 2019 International Conference on Advances **within side the** Emerging Computing Technologies (AECT). IEEE, 2020.

[2]. Nemavarkar, Apeksha, and Rajesh Kumar Chakrawarti. "A uniform **method** for multilevel **e-mail safety the use of photo** authentication, compression, OTP & cryptography." 2015 International Conference on Computer, Communication and Control (IC4). IEEE, 2015.

[3]. Liyanage, Geethapriya, and Shantha Fernando. "A **complete steady e-mail switch** model." 2017 IEEE International Conference on Industrial and Information Systems (ICIIS). IEEE, 2017.

[4]. Singh, Priyanka, et al. "S3Email: A **approach** for securing emails from **carrier** providers." 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2017.

[5]. Huo, Bo, Yihong Long, and Jinglin Wu. "A Secure Web Email System Based on IBC." 2017 **thirteenth** International

Conference on Computational Intelligence and Security (CIS). IEEE, 2017.

[6]. Xuan, Jiaxing, et al. "Design of **steady** and **impartial** controllable **e-mail device primarily based totally** on Identity-Based Cryptography." 2016 **2d** IEEE International Conference on Computer and Communications (ICCC). IEEE, 2016.