International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 2 February 2016

Result Evaluation for Multilevel Email Security using Image Authentication, Compression, OTP & Cryptography (IA-COTPC)

Rajesh Kumar Chakrawarti[1], Apeksha Nemavarkar[2]
CSE,RGPV, Reader SVITS Indore, MP 452010/Indore,India[1]
CSE,RGPV, PG Scholar SVITS Indore, MP 452010/Indore,India[2]
rajesh_kr_chakra@yahoo.com[1], apeksha.sept@gmail.com[2]

Abstract: *A Client verification and distinguishing proof have dependably spoken to a test in online email frameworks. The text based verification and client distinguishing proof are not adequate to address the security issues confronting online email frameworks. This kind of security is totally retrograde and out of date for current security dangers that effortlessly undermine verification, ID and non-denial. In this paper, a security increment in email customer is proposed by presenting multiple level verification and distinguishing proof in email customers [1]. The proposed multilevel verification and distinguishing proof comprise of four levels, where level-1 is the content based verification, level- 2 includes a picture based confirmation lastly level-3 what's more, level-4 utilize a particular calculation that adventures the intense properties. The different encryption strategy gives adequate security to electronic exchanges over remote system. In this examination paper, the requirements of different encryption method in Secure Electronic Exchange are proposed to upgrade the security of classified information. This system expands the information security in such a way, to the point that unapproved client cannot get to any piece of data over remote system as web [2].*

Keywords: *Data Security, Multiple Encryptions, user authentication and image-based authentication*

1. INTRODUCTION

Secure Electronic Transaction (SET) is a standard convention for securing MasterCard exchanges over unreliable systems, particularly, the Internet. SET is an arrangement of principles and regulations that empower clients to perform budgetary exchanges through existing instalment framework over unstable remote system (web) in much secure and dependable way [3]. SET is an application to give different security administrations as privacy, information honesty and realness for all electronic exchanges over the web. Secure Electronic Transaction (SET) is vital for the effective electronic exchange over the remote system; secrecy is required to conceal the delicate information from unapproved client, information honesty is required to guarantee that entirety data is exchanged with no alteration through interloper, and validation . Truth be told a few cases from the seasons of old Greece are accessible. As of late, everything is slanting toward digitalization and with the fast advancement of the Internet advances, computerized media can be transmitted advantageously over the system. Subsequently, messages should be transmitted subtly through the computerized media by utilizing the numerous security methods accessible in market, for the most part it depend on either steganography or cryptography.

A one-time secret key (OTSK) is a watchword that is legitimate for one and only login session or exchange. OTSK dodge various weaknesses that are connected with conventional (static) passwords. The most imperative deficiency that is tended to by OTSK is that, as opposed to static passwords, they are not powerless against replay

assaults. This implies a potential interloper who figures out how to record an OTSK that was at that point used to sign into an administration or to direct an exchange won't have the capacity to manhandle it, since it will be no more legitimate. On the drawback, OTSK are troublesome for individuals to retain. Thusly they require extra innovation to work. How to create OTSK and appropriate? OTSK era calculations normally make utilization of pseudo arbitrariness or haphazardness. This is vital in light of the fact that else it is observing so as to anything but difficult to anticipate future OTSK past ones [4]. Concrete OTSK calculations change extraordinarily in their subtle elements. Different methodologies for the era of OTSK are recorded underneath:

- Based on time-synchronization between the verification server and the customer giving the secret key (OTSK are legitimate just for a brief timeframe)

- Using a numerical calculation to produce another secret word in view of the past watchword (OTSK are viably a chain and should be utilized as a part of a predefined request).
- Using a numerical calculation where the new secret word depends on a test (e.g., an irregular number picked by the confirmation server or exchange subtle elements) and/or a counter.

There are additionally distinctive approaches to make the client mindful of the following OTSK to utilize. A few frameworks use exceptional electronic security tokens that the client conveys and that produce OTSK and demonstrat to them utilizing a little show. Different frameworks comprise of programming that keeps running on the client's cell telephone. Yet different frameworks produce OTSK on the server-side and send them to the client utilizing an out-of-band channel, for example, SMS informing. At last, in a few frameworks, OTSK are imprinted on paper that the client is required [5, 6].

2. LITERATURE SURVEY

Amidst the most recent couple of years unmistakable examination articles had scattered which surrenders the inconspicuous parts to a specific level and in the wake of looking at those some best in class procedures had been seen. Go on advances the study, underneath are some related works that associates this paper for further works.

In the paper [7], To secure against the abuse of email accounts through presentation of passwords, this paper recommend that email reports be guaranteed using a customer specific email narrative interference revelation system. Not in any way such as host or framework IDSs that are planned to guarantee one or more PCs, we acknowledge that an email record IDS should be proposed to secure one resource: a customer's email storage facility. Reliably, an email narrative server then would truly be running different IDSs, with one case each customer. This blueprint choice is by and large propelled by the amazingly singular nature of email; it in like manner, on the other hand, has basic impact on our general system auxiliary arranging, showing technique, and the potential adaptability of the structure. More especially, the work on this issue with the going with danger model. In any case, expect that the attacker has permission to a customer's entire gear and programming environment: either the aggressor utilizes the same stage. As a beginning move towards building such a system, developed an essential probabilistic model of customer email direct that associate email senders and a customer's mentality of messages. In tests using data amassed from three months of watched customer direct and built models of aggressor lead, this model demonstrates a low rate of false positives (all around one false ready every couple of weeks) while so far getting by and large attacks. These results recommend that inconsistency acknowledgment is a conceivable strategy for securing email reports, one that does not oblige changes in customer confirmation or access conduct.

In the paper [8], The proposed novel programming security code encryption arrangement in light of the rundown table. This strategy uses a novel and beneficial encryption system called semi group encryption for encryption the recorded table. It gives scarcest similarity of the first data when encoded. Yet, semi bundle encryption is not viable in diffusing the estimations of the plain substance. This impediment can be overcome by using changes. Therefore, this procedure utilizes binded Hadamard changes and Number Theoretic Transforms to present scattering close by the quasigroup change. The proposed technique is differentiated and the other encryption approaches and is seen to give better results.

In the paper [9], it gives a novel picture steganography method to hide messages or information inside other information in such a course as to not be discernible. This makes usage of the route that there is a ton of data being traded reliably, making it hard to yield all the information for disguised messages. Standard cryptographic frameworks

obscure the information, on the other hand it is still especially clear that a message is being sent. Steganography attempts to amend this imperfection so an observer is not ready to know whether a message is being sent or not. This can be used as a piece of development to standard cryptographic techniques, so the security may be redesigned, expecting that the customary frameworks are being used with the same painstaking quality as some time as of late. Steganography in pictures is each pixel is encoded as a movement of numbers which address the red green and blue qualities which make up the shading for that pixel. Following a slight change in this shading arrangement is not discernible by the human eye, it can be used to cover information. This is ordinarily satisfied by changing the smallest huge piece, or LSB, for each pixel to identify with the bits of the hid message

The paper [10] proposed a novel The degree of the Proposal is compelled to the remote acceptance of trademark and legal components using electronic accreditations. For the reasons of this document, we will consider remote acceptance to constitute an affirmation procedure where there is a certain physical division between the encouraging region of the application obliging confirmation and the beginning stage of the character information on which the check method is based Problem Statement

.

3. PROBLEM DEFINITIONS

The most commonly used authentication credentials, reusable passwords, are extremely vulnerable due to common patterns of user behaviour. Many users choose simple passwords that are easy to remember; many such passwords, however, can be compromised by different type of attacks. Users enter passwords on non trusted machines that may be infected with many type of viruses, malicious software, spyware etc.

Such malware can be used to capture passwords. Also, users often share passwords across domains and applications, allowing one weak application (e.g. one that sends passwords in the clear) to result in the compromise other, more secure systems. Additionally, users often reveal passwords to friends, family members, and co-workers. Sometimes it is used in advertently to facilitate the sharing of information or resources. Those very same insiders however, often have motive for compromising a user's privacy.

Also by studying the mentioned literature & other material some of the configured problems or issues are identified which is continuously compromising the security. These issues need to be overcome to provide a better user satisfaction regarding the safe email archives. These are:

- User archives in Emails are not secure.
- Users have no control over security
- Dependency on older text based authentication
- Attack related to channel can easily decode the messages
- Single mechanism is not sufficient for security
- Compression must be lossless to be used with encryption

4. PLANNED OUTCOME

Key Space Analysis:
Attempt to discover the checking so as to unscramble key every conceivable key. The quantity of attempt to discover specifically alludes to key space of the cryptosystem become exponentially with expanding key size. It implies that multiplying the key size for a calculation does not basically twofold the required number of operations, yet rather squares them. An encryption calculation with a 128 piece in key size characterizes a key space of 2128, which takes around 1021 a long time to check all the conceivable keys, with elite PCs of these days. So a cryptosystem with key size of 128 piece computationally looks strong against a savage power assault.

Factual Analysis:
Factual dissecting exhibits the connection between the unique and encoded picture. Accordingly, encoded picture must be totally not quite the same as the first. Because of Shannon hypothesis [17] It is conceivable to unravel numerous sorts of figures by factual examination. For a picture there are a few approaches to figure out if the figured picture releases any data about the first one or not.

Relationship Analysis:
Two neighbouring pixels in a plain picture are firmly associated vertically and on a level plane. This is the property of a picture, the most extreme estimation of relationship coefficient is 1 and the least is 0, a hearty scrambled picture to factual assault should have a relationship coefficient estimation of 0.

Differential Analysis:
The point of this analysis is to decide the affectability of encryption calculation to slight changes. In the event that an adversary can make a little change (e.g. one pixel) in the plain picture to watch the outcomes, this control ought to bring about a noteworthy change in the encoded picture and the rival ought not have the capacity to locate an important

relationship between the first what's more, encoded picture regarding dissemination and disarray, the differential assault loses its proficiency and get to be futile.

Key Sensitivity Analysis:
Also of sufficiently vast key space to oppose a cryptosystem at savage power assault, likewise a protected calculation ought to be totally touchy to mystery key which implies that the scrambled picture can't be decoded by somewhat changes in mystery key.

- Existing work aims in improving code quality by predicting pre-release defects and efficiently allocating testing resources.
- Initially, it has four main phases. In the first phase, it aimed at measuring the static code attributes at functional/ method level from their source code.
- In the second phase, planned to match those methods with prerelease defects. The third and fourth phases are planned to build and calibrate a defect model.

Additionally by examining the specified writing & other material a percentage of the arranged issues or issues are distinguished which is consistently trading off the security. These issues need to be overcome to give a superior client fulfilment in regards to the safe email documents.

5. RESULT ANALYSIS

Various customers pick clear passwords that are definitely not hard to recall; various such passwords, on the other hand, can be bartered by online and disengaged from the net word reference attacks. Customers enter passwords on untrusted machines that might be polluted with contaminations, spyware, or distinctive malicious programming. Such malware can be used to catch passwords. Furthermore, customers routinely bestow passwords across over spaces and applications, allowing one feeble application (e.g. one that sends passwords free) to bring about the exchange off other, more secure structures. Moreover, customers frequently reveal passwords to allies, relatives, and associates. On occasion by the way, yet here and there to energize the granting of information or resources. Those to a great degree same insiders regardless, much of the time have basis in haggling a customer's security to implement them equipment and programming assets are required, henceforth the rundown of fancied assets and their specialized details are given in this section. Moreover of that, this segment incorporates the re-enactment parameters and executed system situations. This segment of the archive gives comprehension of recreation and its determinations in subtle element.

Fig-1: Login Window

In this step user have to insert the basic user name and password which was given at the time of registration process. If user does not have username and password, he may click the new user link to register himself to get the credentials and provide image sequence index for login authentication process. If the user could not provide the username password either the basic credentials of specific image index, system will prompt a message of "Login failed tries again".

First step is included in first level of security From which we can identifies that authorize user access the mail or not. System authenticate only access of authorize user. It is basic step of entering in to the system.

Fig-2: Image Authentication Window

In this level we are providing a unique feature for logging to a system. This is image authentication. In this user will select

an order of image from multiple categories & register this sequence as identification along with its regular user id & password. When user tries to logging again he must have to select the same sequence from the shown category. This sequence is matched from database through pattern recognition. Image authentication techniques have recently gained great attention due to its importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet

Fig-3: Composition Window

In this level for further security we are using the lossless compression technique before encoding the message. The architecture is able to compress both the string & the whole file. For this Gzip & Huffman compression technique is used which gives the better results with low complexity at cheaper cost. In this step user can send an email to other users, one can write the email message and can also attach file with that message. After that as system facilitate user to encrypt and compress the message and file, user needs to click on the "Encrypt and Compress" This action will encrypt the message of the email with provided algorithms and also reduces the size of the file attached with that message to serve several benefits.

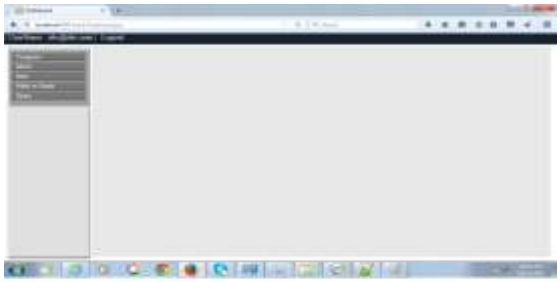

Fig-4: Mailing Board

If above steps are satisfied, in this step user need to press the "send message" button. If the message sent successfully system will prompt a message "Message sent successfully". When intended recipient read the message then message generate automatically "FILE NAME(abc) is read by receiver (xyz@gmail.com) and it will send on sender registered mobile number.

6. APPLICATION

The email security can be done through various ways but the email encryption after compression is better approach in order to protect against the various attack. And this approach can be useful in lots of e commerce application this can be useful mostly in the areas where the e- mailing is done such as:

- Banking system – various mails are sent to customer.
- Defence system – secure transmission i.e. protecting against the enemy.
- Finance system – most useful in this area various transactions are done via mail.

7. APPLICATION

In this paper, we have proposed another thought to upgrading the execution of the OTSK to give Authentication to System. OTSK is encoded and send to client and client can login just utilizing portable based innovation. This methodology gives the abnormal state verification to the framework by confirming the client's Password, OTSK and portable number [11]. In this strategy fairly framework burden is expanded by scrambling and unscrambling of OTSK for various clients. Later on, we plan to concentrate how to lessen the framework stack and expand framework execution while utilizing this methodology. Security of advanced pictures in transmission,

distributed and capacity turn out to be more critical because of straightforward entry to open systems and web. In this paper, we have overviewed existing exploration on picture encryption in another methodology by grouping diverse sorts of work utilizing different systems more than just encryption. [12].

ACKNOWLEDGEMENT

First and foremost, I would like to thank **Prof. Rajesh Kumar Chakrawarti**, Reader Computer Science and Engineering,for his most support and encouragement. The work is evaluated and drafted with the help of him .Without them it would not be possible for me to overcome the problems and issues faced. , I would like to thank Almighty God for blessing us with His grace.

REFERENCES

[1] D. W. M. Dietz, A. Czeskis and D. Balfanz, "Origin-bound certificates: A fresh approach to strong client authentication for the web," in Proceedings of the 21st Usenix Security Symposium, 2014.
[2] M. Hearn, "An update on our war against account hijackers,"online,2013.http://googleonlinesecurity.blogspot.com/2013/02/an-updateon-our-war-against-account.html.
[3] S. B. et al, "Authentication techniques for engendering session passwords with colors and text," Advances in Information Technology and Management, vol. 1, no. 2, 2012.
[4] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), 2007, pp. 467–472.
[5] S. Anand, P. Jain, Nitin, and R. Rastogi, "Security analysis and implementation of 3-level security system using image based authentication," in Computer Modelling and Simulation (UKSim), 2012 UKSim 14th International Conference on, 2012, pp. 547–552.
[6] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," in In Proc: International Conference on Computing, Communication and Applications (ICCCA), 2012, pp. 1–4.
[7] A. Luma and B. Raufi, "New data encryption algorithm and its implementation for online user authentication," in Proc of International Conference on Security and Managment. CSREA Press, USA, 2009, pp. 81–85.
[8] A. L. Bujar Raufi and X. Zenuni, "Asymmetric encryption decryption with pentor and ultra pentor operators," Online Journal.
[9] Soheb Munir, A.S.Zadgaonkar and Manish Shrivastava "Key Generation and Verification for Image Authentication", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-3 Issue-12 September-2013
[10] Suresh Kumar B. and Jagathy Raj V. P. "A Secure Email System Based on IBE, DNS and Proxy Service" Journal of Emerging Trends in Computing and Information Sciences©2009-2012 CIS Journal.
[11] Abhas Tandon,Rahul Sharma, Sankalp Sodhiya and P.M.Durai Raj Vincent "QR Code based secure OTP distribution scheme for Authentication in Net-Banking" in International Journal of Engineering and Technology (IJET). Vol 5 No 3 Jun-Jul 2013
[12] Shabir Ahmad and Bilal Ehsan " The Cloud Computing Security Secure User Authentication Technique (Multi Level Authentication)." International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013 2166 ISSN 2229-5518