International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

A Computational System in Sequence of Information Ruptures

Md Nazimuddin Ahmed[1] and Md Ateeq Ur Rahman[2]
[1]M.Tech Scholar, Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India
[2]Professor, Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT

This paper contains the achievement of information lineage in malevolent situations. Data breach of individuals is a serious issue considering the information confidentiality and reliability of the data provider. The data provider should properly scrutinize the situation of data infringement and analyze possible solutions for blocking such trespassers. Here we intend to present a system that specifically eliminates all such fissures during allocation of data. The designed methods primarily concentrate upon narrowing down the breach of data instead of only providing alternate data or faked data. Data sent over any network is prone and exposed to different network data breaches. So, diligent security must be implemented with the information sent over the transferred network. With rapid increase in communication means, our smart phones and social networks have a lot of private and confidential information, and all these may be leaked without security. To counter this, data descent mechanism is used or in general the concept of data descent in malevolent conditions is deployed. This generally initiates with improper information fed to suspected requester. The system is developed in a critical environment prone to attack wherein we can transfer our data with different information coupled with different cryptographic techniques. Furthermore, experimental analysis of our design and proper implementation is done in vivid situations of within and outside transfer of organizational data. So, we define the aspects of data breach in various possible situations in general and well-defined implementation of our system in particular to analyze and provide a secure means of data descent.

Keywords: Information Breach, Data Descent, Responsibility, System Design and Analysis, Fingerprinting, Oblivious Transfer, Watermarking, Encipherment.

I. INTRODUCTION

Data infringement is a serious concern in today's world wherein we are directly or indirectly dependent on different types of data and time and again we are exposed to different social media outage and the threat to confidential information. Various threats to data exposed online puts at risk the confidentiality of data and reliability of the information provider. Be it interception, interruption, modification or fabrication, countering them becomes priority for an organization considering the security of individuals in or outside the premises and mitigating risks that hamper the image of the organization.

With the increase in communication mechanisms, the need to provide security to data and eliminate all such possible modes of exposure have become the foremost vital side of data maintenance. Various algorithms, security mechanism and well-defined architectures are therefore the need of the hour which are deployed to form a well-structured secure platform for data exchange. In this small research paper, we have tried to define a basic framework of secured data transfer in various malevolent environments.

Breach specifies exposure of data through security gaps or threats that ultimately puts at risk the sensitiveness, integrity and accessibility of information. Lineage or descent of data primarily pinpoints the flow of data between different individuals and in the case of within same organization and outside of it. Authenticity and non-repudiation of data descent between the provider

and consumer is the primary point of concentration of our system design.

In multinational companies, sensitive information is often fed out to different third parties during various business activities. This may include survey of company data which can include customer data and as such the customer's valuable data is exposed. Some third party may unintentionally or intentionally leak the data or use it for miscreant means. We try to devise a mechanism wherein any such leakage is properly detected and if possible identification of the culprit responsible for the leakage.

II. EXISTING AND PROPOSED SYSTEMS

2.1 Existing system

In today's digital world, data infringement unintentionally or intentionally by disgruntled employees with intent to harm the organization pose a big threat to the organizational security. Security is required with the enormous use of data within and outside for business. Both physical and administrative security is provided considering the value of the resources.

Threat is an indication of potential or imminent danger or in general something that is regarded as a danger. That is, a threat is a possible danger which exploits the possible aspects of vulnerability. Many times, data leakage is not exposed as there are no primary tools of detection and often go unnoticed as lot of data can be copied and passed on without any trace of loss. As such, detection becomes more difficult in such a situation. Data breach problem has thus reached a new dimension these days.

2.1.1 Disadvantages

Applying access control can provide security until the malevolent user has gained access to the data. Access controls such as encryption protects the data until the data is not decrypted. Once done, it is exposed to unauthorized usage and even can be passed on over the network without any trace. Data leakage thus becomes more impossible to counter and further difficulty is encountered while estimating possible means of countering while acting proactively.

2.2 Proposed System

Different aspects of system design are adopted with the mindset of achieving success in countering data breach. The older system uses the technique of comparing the pairs to validate received data for their equality while our designed system uses oblivious transfer with cryptographically locking both versions in encrypted form for more secured validation.

Both the systems have complexities in implementation and flaws as well. While creating two different versions out of the same watermark, the option to view recipient watermark still remains in the event of fail of equality test. In the case of any failure, the possibility of any discrepancy is eliminated by the oblivious transfer with watermarking and cryptographic encipherment of the recipient message. Asymmetric fingerprinting that is based on oblivious transfer suffer from identical weakness that's deployed. We basically try to eliminate this aspect in our designed framework by including a signed message in addition to the watermark's content. This helps in validating the recipient's request. The message can also be read by the receiver to validate sender's message which is not possible in the case of watermarking.

2.2.1 Advantages

- ✓ The recipient has both concealed data and encipher key.
- ✓ The pixel density is increased.
- ✓ Data is comparatively more secured.

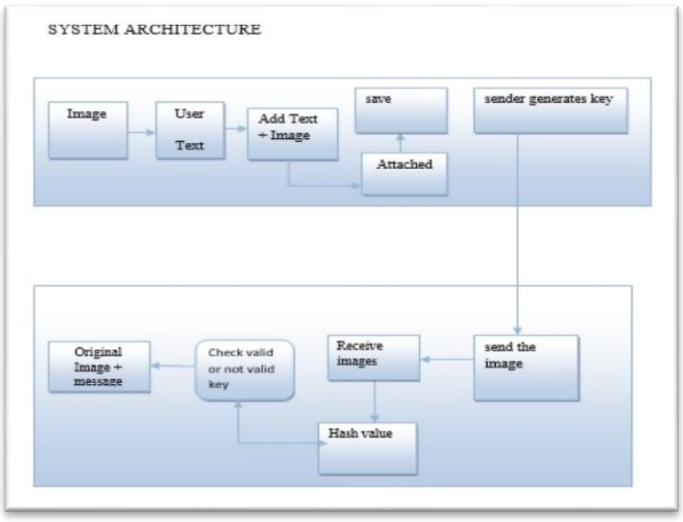

Figure 1: System Architecture

The figure 1 shows the architecture of the proposed system.

The proposed approach works in the following mode of operation.

1. Micro standardization
2. Possible information deformation
3. Information transmission
4. Secured watermarking

1. Micro Standardization

Protocol is enforced diligently and performance is analyzed specifically. Within the oblivious transfer sub protocol, it is deployed using PBC library which includes in itself the GMP library protocol. BLS scheme is applied for signature validation that is present in PBC library. AES performs symmetric encipherment which is present in the Crypto++ library. Cox algorithm rule for sturdy image is employed in the case of watermarking. For correct implementation, we set the -factor to 0.1, that determines the strength of the watermark.

Different parameters are used as input to research the performance of the system. Execution of sender and recipient part takes part in the same program and stress is put on computational performance, not on analyzing network sending. The sample executing machine used is a generic laptop with 8 GB RAM and 4 × 2.6GHz cores, but all executions are performed sequentially. Implementation times for different phases of the protocol: watermarking, signature generation, encipherment, oblivious transfer and identification are properly evaluated.

2. Possible Information Deformation

A simple splitting algorithm is employed wherein the image is divided into n equally sized squares. However, on deploying a strong watermark, variations between adjacent components become visible. Multiple iterations produce stronger image quality. Distortions of such sort often affect the quality of the document. Stress has always been continuously on providing best results while deploying our mechanism. The Cox algorithm is used with 0.1 parameter and no distortion is primarily visible. Use of elaborate splitting algorithms can facilitate in reducing this facet of the matter.

3. Information Transmission

Distribution of data is done through a multicast system so that the recipients can have distinctive watermarked version. Data/File/Information is divided into blocks and each lock has two different versions by watermarking with different watermarks and properly encrypting with different keys. A bunch of keys is assigned to every recipient, so that one can decrypt exactly one version of each part. The consequent integration of components will unambiguously determine the recipient.

It also shows another approach for a broadcasting system that allows identification of recipients by their received files. Using the technique of finger casting during the decryption process, recipients automatically embed a watermark in files. Chameleon cipher on which this is based, gives the option to decrypt encrypted information with different set of decryption keys, that uses noise as means of detection of any anomaly. For conspiring attackers, finger casting technique along with a random fingerprinting code is used to provide better security against any threats. The aspect of an un-trusted sender/source is not specified in this broadcasting approach.

4. Secured Watermarking

Data groups like relational databases that include text files and Android applications have Watermarking techniques. Data or information descent in malevolent conditions is employed generally to user databases or medical records for verification of information. Watermarking relational databases can be done in many ways. One of the most common technique is to embed information along with noise-tolerant characteristic of the inputs or to create pseudo data base inputs. Text watermarking basically has two basic approaches. This technique clubs important information by changing the text view (appearance of words and lines) that cannot be grasped by humans. The other approach also known as language watermarking primarily gives important on the semantic level of text rather than how the text is being presented.

A proposed way to watermark Android applications have also additionally been devised. In this mechanism, a permutation graph is watermarked and therefore the graph is hidden within the application as a linked list. The list representation in the case of any attack, provide a solid secure way of dealing any trespass as the execution state is watermarked and not the syntax and claims to be one of the robust means of protection in the approach for proposing watermarked secured mechanisms. During this approach, the proposed framework is designed to rather take away existing information rather than adding new information or modifying existing information.

III. IMPLEMENTATION AND RESULTS

Users already registered or fresh users can register to access the server with their credentials. Steganography technique is deployed to merge text and image into the steganography image. Hash value is generated after that by SHA or MD5 algorithm. The encrypted image is then forwarded to the receivers. On the receivers' end, the decryption of image is done and cross-verification of the sender is done through audit. This is a brief explanation of the implementation of our experiment.
A lot of protocols are steered to enforce corporation and by using specific techniques we are able to establish escape in malevolent atmosphere with the price being effective. Beyond the fascinating price and additionally many times systems don't generate the appropriate results. We've got to unravel the escape of data problem that occur in several situations by postulating to search out the demonstrably associating the reason to the leakages and work on the lineage methodologies. For that we tend to also understand various situations which shows the flow of information through varied locations.

Watermarking is done for data descent in our framework. Different watermarking techniques are employed for different data types. The designed system has data owner, data consumer and data auditor. Data owner is associate degree entity that manages documents and takes care of accuracy, integrity and timeliness. Also, access control is also defined by owner. Data consumer will receive the data and use it for appropriate purposes. Data audit involves the processing of data and plays vital role during data leakage. For a trusted sender, basic cryptographic protocol is applied and no further security is required. No framing property is applied in the case of an untrusted sender. The data is split into parts and each part is uniquely watermarked. For each part, a signed message of the watermarked content and timestamp is present.

Below are some of the screenshots of the process.

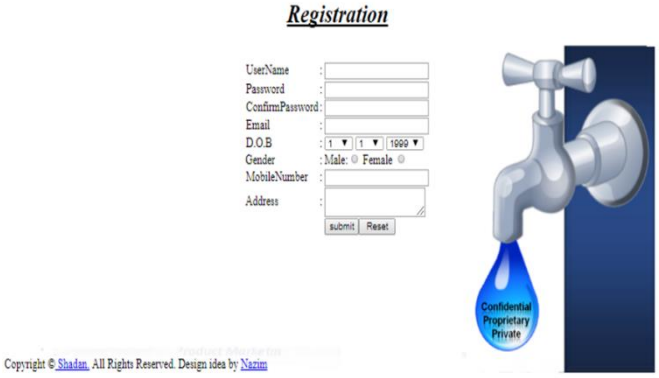

Figure 1: New user registration.

The Snapshot 1 shows the options for a new user to sign up for our portal.

Figure 2: Sender login

The snapshot 2 shows the authentication module in which the credentials of the login users are authenticated and if they are found to be genuine, access is given to the system otherwise the user is denied access. After getting the access, the user can upload the image to be sent to the receiver as shown in snapshot 3.

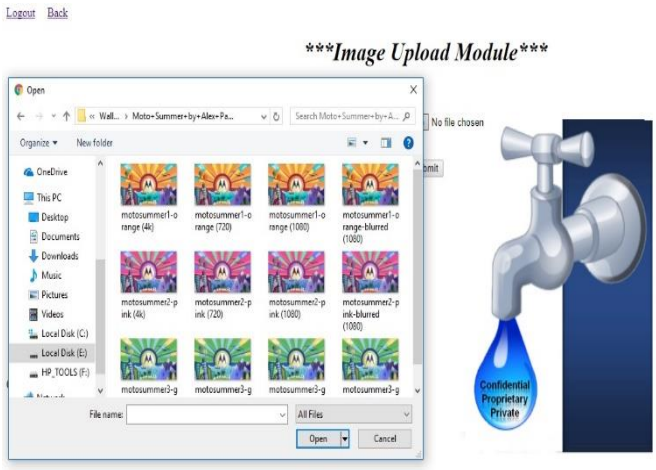

Figure 3: Image upload by sender

The intended image to be sent is embedded with the secret message to be transferred to the receiver as shown in snapshot 4. For the message embedded in the image a secret key is generated with the steganography technique for enhanced security as displayed in snapshot 5.

Figure 4: Embed image with secret message

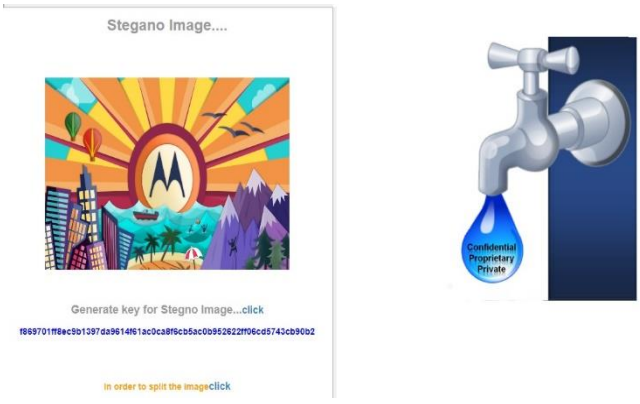

Figure 5: Secret key generation with steganography

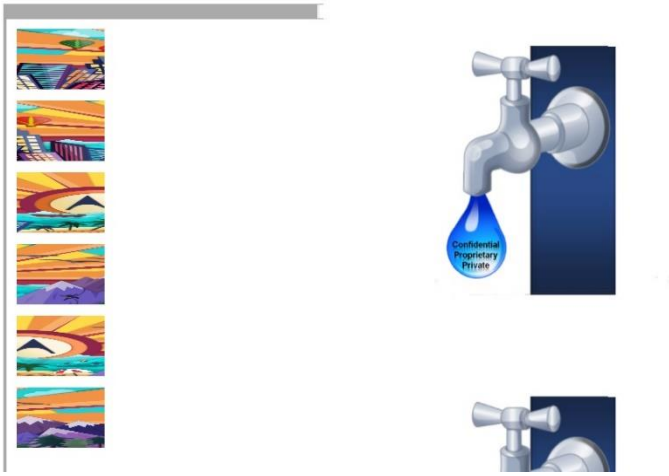

Figure 6: Image split

Figure 7: Sending to receiver

As per the proposed approach, the uploaded image is further divided in multiple small images as shown in snapshot 6 and then sent over the network as shown in snapshot 7.

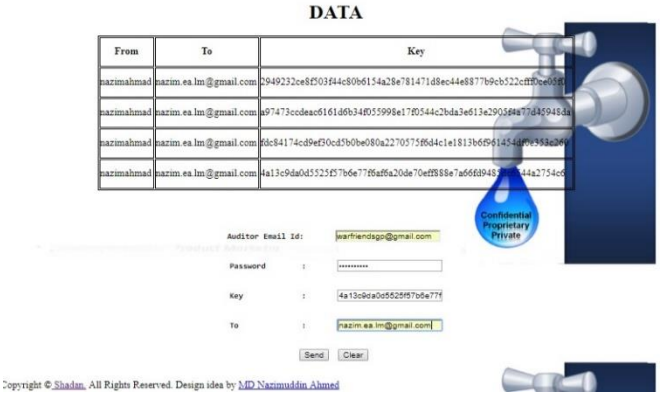

Figure 8: Auditing

Figure 9: Message received by receiver

All the information of split images and the encrypted message sent is subjected to auditing as described in snapshot 8 and after crucial auditing, the information after successful transmission will reach the receiver's inbox as shown in snapshot 9.

Figure 10: Decrypting message

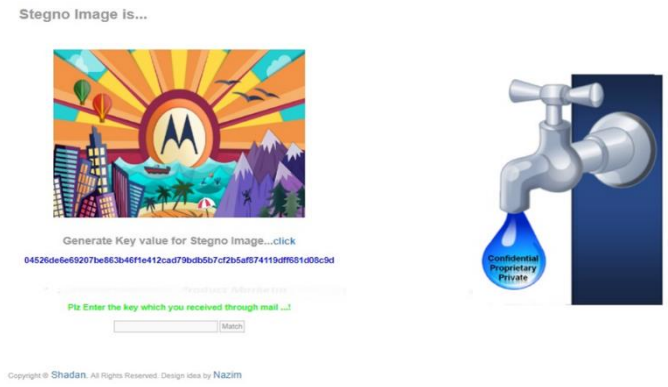

Figure 11: Image received with secret code

The received encrypted information is decrypted at the receiver's side and also the image sent by the sender is received at the receiver's end with the code as shown in snapshot 10 and 11.

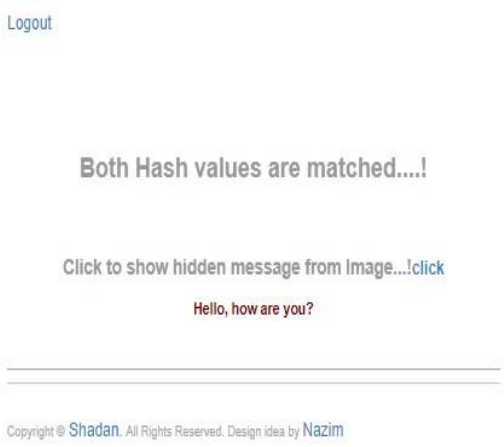

Figure 12: Secret message revealed after hash value matched

From the reconstructed image, the original secret message is revealed sent by the sender once the hash values are matched as shown in snapshot 12.

IV. CONCLUSION

Thus, in this paper we have briefly presented our model which is liable for data forwarding among various myriad units. We have set up common techniques of data transfer which includes oblivious transfer protocol, robust watermarking technique and digital signatures to cross verify data descent. Micro standardization results have given the veracity and equity of the implementation of the deployed mechanisms.

Deterring malevolent parties from leaking information and data and providing protection for sensitive data to encourage the people who trust in an organization is the primary goal of this design. This technique is versatile as correct differentiation is completed between sure senders (usually owners) and untrusted senders (usually consumers). For sure sender, a really simple protocol with very little overhead is feasible. An uncertain sender is at risk to a lot more sophisticated protocol. Furthermore, the results are tallied with trust assumptions and intrinsically trust issue of the concerned entity is a lot more. Future work conjointly motivates more analysis on knowledge outpouring detection techniques for varied document varieties and eventualities. For instance, it'll be a stimulating future analysis direction to style a verifiable lineage protocol for derived information.

VI REFERENCES

[1]. M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253-266, Feb. 2005.

[2]. J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," in Proc. Inf. Technol. Coding Comput., Las Vegas, NV, USA, Apr. 2001, pp. 223-227.

[3]. H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 456-465, Sep. 2008.

[4]. D. Coltuc, "Improved embedding for prediction based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873-882, Sep. 2011.

[5]. X. Li, B. Ying, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524-3533, Dec. 2011.

[6]. Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500-1511, Dec. 2008.

[7]. B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise predictionerror expansion for efficient reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010-5021, Dec. 2013.

[8]. W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906-910, Jun. 2009.

[9]. C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognit., vol. 41, no. 12, pp. 3582-3591, Dec. 2008.

[10]. P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, no. 6, pp. 1129-1143, Jun. 2009.