ABSTRACT

In present days, several state and central governments have taken initiative to successfully implement E-Governance in various areas of services. The main criterion is to provide services in transparent & accurate manner among the citizens by the use of different ICT tools and techniques. E-Tendering is one of the sensitive functions of good governance, which helps to simplify complex manual activities for purchasing of goods and services using the Internet in a transparent manner but which lacks transparency, accountability and security. One of the major factors that are limiting the success of E-Tendering approach is that the security measure is not properly implemented. In this paper, we propose a UML implementation of Secret-Key Watermarking algorithm for integrity verification of transmitted tender document via Internet from public sector organization to the supplier and vice versa in E-Tendering system, so that the watermark is capable enough to detect any changes made to the online tender document by malicious users.

Keywords


1. INTRODUCTION

There are various drawbacks in the traditional tender processing system [1] such as delay in tender processing, human interference at every stage, inadequate transparency, and most importantly lack of security. The vendor communities, who are part of the process, took advantage of the dependencies involved, manipulated the prices and dictated terms. The main challenge for an organization is to provide security measures, reduce processing time, and make the competition fair and transparent. In order to achieve all these organizations has implemented a web-based Government to business (G2B) solution for E-Tendering process.

Today, internet is the only medium that is used to provide end to end communication between different communicating parties. Malicious users in internet can not only destroy the confidential information [8] but also hampers the integrity of the system. The organization need to provide high level of security of online tender documents that are exchanged between different stakeholders.

The successful implementation of E-Tendering system must satisfy following criteria’s like –

1. Cost savings for supplier and organizations.
2. Speed up the process by shortening the tender cycle.
3. Anytime, anywhere access to information.

4. Transparency and accountability in the process.
5. Increased efficiency and productivity.

In this paper, section-II identifies basics of Secret-key Watermarking technique along with methods of incorporating watermark and its extraction. Section-III identifies the algorithm for authentication in E-Tendering system and Section-IV identifies the UML implementation of the algorithm in detail, which may be used to support security strength of the system.

2. SECRET-KEY WATERMARKING TECHNIQUE

Digital watermarking [3] is a technique of ownership verification and/or authentication. It inserts information that will be hidden into the message [11] and the information is referred as watermark. After inserting the watermark [5], the original media will be slightly modified and is referred as watermarked media. The changes between the original media and the watermarked one are very little and the difference is not visible in human eyes. The watermarked media are sent over the transmission channel to the receiver. In the receiving end they are checked for authenticity of the owner. Watermark extraction [5] is performed in the receiving end for verification of the ownership.

In Secret-key watermarking [6, 10], we have an embedding function that takes a message and outputs a watermarked work. Similarly, we have a detection function, which takes a watermarked work and outputs a message. Watermark key controls the mapping between the watermarked works and the messages. Secret-key watermarking does not allow a public recovery of the watermark. In Secret-key watermarking, the watermark embedder and the watermark detector use the same watermark key.

Here, in watermark embedding process [10, 12], the input to the scheme is the watermark (unique supplier id), the cover-media (tender document) and a Secret-key (generated using our algorithm). The Secret-key is used to enforce security, which is the prevention of unauthorized parties from recovering and manipulating the watermark. The output of the watermarking scheme is the watermarked tender document. In Watermark detection process [7, 9], inputs to the scheme are the watermarked tender document and same Secret-key, that are used in the watermark insertion. The output of the scheme gives us some kind of confidence measure regarding privacy and confidentiality of the online tender document by checking integrity and authenticity of the test data.

3. E-TENDERING AUTHENTICATION ALGORITHM

The primary concern in E-tendering application is Security. We used a Secret-key in our algorithm for embedding and extraction...
process of watermark. We have chosen a large key-space [15, 17] for our proposed algorithm to make exhaustive search attacks impossible. The message is encrypted before it is embedded and decrypted after it is detected to provide an extra level of security [13]. Such a system requires two types of keys – the watermark key, which controls watermarking process and the encryption key, which controls encryption and decryption process.

Key Generation Algorithm: In this algorithm, server side machine (organization site) generates two types of keys, the watermark key and the encryption key. The encryption key along with tender paper is supplied to the vendors via internet and the vendors can use the supplied tender paper to create their tender proposal at client side (vendor site) with the help of shared secret key. Server side machine use a cryptographically strong pseudorandom number generator [2, 14, 15] to produce the watermark key and the encryption key. The generator uses three 3DES [2, 4] standard algorithm with two keys and is shown in next page. The first pseudorandom number uses a 112 bit seed as the initial vector (IV), the rest of the pseudorandom numbers use the seed that are generated by the previous phase.

Watermark Embedding Algorithm: To insert generated watermark [19, 20, 21] in the original message (tender document) to provide security and authenticity, this algorithm is used. This process is also executed in the server side (organization site) of the application.

1. Initially, server side application program pad some information (if needed) within the message so that they can evenly break the message into blocks of 128 bits.
2. The server side machine then chooses the generated encryption key to encrypt the block using encryption function E (.). The encryption function uses AES technique with 12 rounds and key size of 192 bits.
3. After encrypting the block, the server side machine applies another encryption function E1 (. ) using watermark key to incorporate the watermark information on the message block.

In 3DES, we used only two keys. The first and the third stages in each block use one key and the second stage uses another key. The keys that are used here are generated by cryptographically strong pseudorandom number generator. The left hand side column denotes the encryption of message and includes encryption-decryption-encryption blocks. On the other hand, right hand side column denotes the decryption of message and includes decryption-encryption-decryption blocks.

Watermark Detection Algorithm: To identify authenticity of the message and to extract generated watermark [13, 18] from the watermarked message, the following algorithm is used. The decryption functions are complementary of the encryption functions that are used in the embedding algorithm. This process is also executed in the server side (organization site) of the application.

1. The server side machine split the watermarked message into several blocks.
2. Then, the server side machine applies a decryption function D1 (. ) on individual blocks using the same watermark key to produce the corresponding block of watermarked message. The decryption function here uses AES technique with 14 rounds and key size of 256 bits.
3. Finally, the server side machine applies another decryption function D (.), using the same encryption key, which is used to decrypt the block to identify actual information. The decryption function uses AES technique with 12 rounds and key size of 192 bits.

4. UML IMPLEMENTATION

The Unified Modeling Language (UML) [22] is a collection of three major notations [22] and a number of modeling techniques. It actually helps us to specify, visualize, and document models in a manner that supports security and robust execution. UML provide facilities to create modular designs and helps us to establish consistency across the systems. In UML, Structural diagrams identify the static features of any model. It shows the parts of the model and identifies how they are organized, but it never shows how the finished product will behave and look like. The class diagram in UML models the resources that are needed to build and operate the system. Class diagrams models the structure, relationships, and behaviors of each and every resource that are used in the system. The object diagram in UML support facts and examples and are generally useful in the early phases of the project development. In this paper, we used UML to implement server side (organization site) and client side (vendor site) applications. In server side two keys along with the tender paper is generated and in client side with the help of those generated keys tender documents are populated. Finally populated tender document is checked for validation at the server end.

Combined Deployment Diagram: It models the hardware implementation of the system and each and every node in the diagram generally represents one type of hardware.
In the above diagram, database server is a dedicated server machine which actually generates two keys as well as the blank tender document. It is also the central repository of all populated tender documents that are sending by different clients. Apart from that it acts as an executor to process the tender documents also. The client machine is only responsible for the population of blank tender documents. The notation 1..* at server side indicates that 1 or more client can access a single tender document and the notation 1..* at client side indicates that a client can access more than one tender document.

Use Case Diagram: It models the interaction of the user’s with the system. The people in these models are referred as actors and features of the system are called use cases.

In the above diagram, the external user is referred as client and she can communicate with the system to perform the above mentioned activities.

Activity Diagram: The activity diagram implements logic of the system from workflow to use cases to methods. The arrows in the diagram indicate the flow from start to end through different decisions and loops.

In the above diagram, the logic is represented to implement the behavior of the system and it also represents the logic at any level of the execution.

5. CONCLUSION

We have applied an open algorithm called AES block cipher algorithm for encryption and decryption of messages as well as for watermarking which can be implemented in software, hardware, and firmware at ease. Practically the space in digital contents where watermarking can be applied is very limited and our algorithm is so simple that they can be easily implemented using cheap processors and a minimum amount of memory. The algorithm is designed in such a way that we can easily implement the algorithm into any Government-to-Business (G2B) model. The UML implementation actually helps us to simplify the design steps as well as implementation process. It is suited not only for this sort of problems but also for other types as well.

Distribution of key is a point of concern for E-tendering approach and if not controlled in secure way, then the hacker can hamper the security of the system in large. If we can apply compression prior to encryption of the message, the computational demand of the subsequent encryption stage will be decreased.

As we know, the main requirements on watermarking schemes is security and robustness against intentional or un-intentional attacks attempting to remove or destroy the water-marks, this Secret-key authentication watermark can detect any changes made to the document & thus satisfies our purpose.

6. REFERENCES


