A CONCEPTUALIZED MODEL FOR ENHANCING NON-REPUDIATION IN UNIVERSITY E-FORM PROCESSING

GBENGA O. OGUNSANWO & OLUWAFEMI S. OGUNSEYE

ICT Unit, Tai Solarin University of Education, Ijebu-Ode, Ogun State

ABSTRACT

Most organizations use one form of online registration or another. Since these registration forms are structured to be open and available to users, many of them do not afford or seem to require basic security measures like access control measures or even basic passwords. This however implies that the authenticity of the user, and accountability of the user to the information provided is not established, thereby making repudiation a possibility. This work proposes a strategy to reduce deniability on the part of the users of e-registration systems, and strengthen accountability using a digital signature based field locking process. The work used students' registration liberally as the focal point and will encourage users to take more seriously the data they fill into online forms just like they do in paper based ones.

Keywords: *Digital Signature, Information Security, Non-Repudiation, E-Form Processing, Information Systems*

1. INTRODUCTION

Many of the world's transactions are now done electronically with varied levels of security applying to disparate processes. The use of electronic forms and online registration by universities, institutions of higher learning and other similar organizations like examination bodies are now firmly established online processes even in developing countries. The reason for the wide acceptance of this e-registration would include its ease of processing, reduced personnel workload and the fact that the users; students in the case of universities can use it from anywhere at any time amongst other propelling factors. In spite of the many obvious advantages of e-registration systems to universities especially in developing countries, e-registration systems do not provide a balance of accountability which used to be available with its predecessor. E-registration systems as used in schools cannot be overly protected to allow for usability. Folorunso et al. (2006) suggested that mass computer literacy and lack of adequate infrastructure amongst other factors impede the use and acceptance of online transaction methods with specific focus on e-learning in developing countries. Their research was able to point out that majority of the citizens lack personal access to internet and have to make do with public cyber cafés. This system thus allows and necessitates people filling the forms on behalf of others which can sometimes be without their permission therefore providing for repudiation on the part of students when inaccurate data is filled. Another issue is that by design, many e-registration systems or online forms are open because they do not necessitate password security since the transactions are temporary. There is therefore a need to be able to ascertain who an online data is coming from and ensure the user can take responsibility for information they fill even in open systems. It will not be surprising that this research stemmed from our experiences with handling registration based issues in Tai Solarin University of Education. Many times scarce resources of time and money is wasted when students come to claim inaccuracy of data filled online blaming it on so many factors especially when such data puts them at a disadvantage in the university. A popular example is the case of state of origin declaration. We have handled thousands of cases where students would claim inaccuracy in the state of origin they filled online after realizing that some states pay cheaper fees than others or where student deny courses they registered for. Online forms collect sensitive data

that the user should be honest and accountable about. These are the motivations for this research. We present a conceptual model that improves students' accountability on registration systems and make entries into e-forms be auditable and verifiable.

2. DIGITAL SIGNATURES

A digital signature is a computer based form of the traditional paper-based signing (Entrust, 2003); it uses the concept of a coded message attached to electronic documents to ensure that the person who signed is indeed the originator of the document and ascertains that the message has not been modified after sending (algorithmic research, 2010). Digital signatures differ from mere electronic signatures because they are a result of cryptographic operations and cannot be copied, tampered or altered while electronic signatures are electronic images that are physically or logically attached to the signed data. They are easy to forge and alter (Algorithmic Research, 2010). Digital Signature can help users know if there has been any alteration to the data/document they signed (Adobe, 2006). They can also improve the trust level for data or information supplied by users. The model we propose will adapt the digital signature process to a large extent. The subsequent sections consider the signing process in detail.

3. TRADITIONAL ONLINE STUDENTS REGISTRATION

The normal online form usually designed with HTML accepts data into predetermined fields. For most systems there are server side or client side scripts that processes the data entered into the form fields checking them for consistency with the developers wishes and storing them in databases. Non repudiation is toned down to a minimum. Most Current methods use access control techniques but they are not strictly enforced to increase usability. Other more Open systems use security measures that protect the owners of the system as against ensuring accuracy of data supplied by users. An Example is the Joint Admissions and Matriculation Board (JAMB) registration portal used in Nigeria and some parts of West Africa. All its security feature focuses on preventing the users from defrauding it by entering false PINs. Many Admission sites around the world are also structured this way.

The steps taken in the traditional/current transaction can be itemized as follows:

- Student access form from school's website
- Student supplies relevant data
- Forms is processed and stored in relevant database.

This process exempts the user from any accountability hoping that the user would naturally be.

4. PROPOSED ENHANCED NON-REPUDIATION MODEL

We show the proposed steps in our model

- The user fills data into necessary fields

This is same as the traditional process. The user enters data into the required fields.

- The user is asked to sign sensitive fields

For the sake of non repudiation, the user is required to fulfill a challenge next to filling sensitive fields. The challenge will necessitate entering private verifiable data like PINS

- The user enters signing criterion
- Signature criterion is verified and timestamped

The signature criterion should be a unique data that is known to the user alone and is traceable to the user. An example is the PIN for the user's debit card confirmable through web service

provision to the SWIFT of the card brokering agent. Once the criterion is confirmed a signature is created through an encrypting function computation on the signature criterion/PIN and included in the data stored in the database. This ensures that the user cannot deny entering the data. In case the signature criterion is denied, the form filling process is cancelled.

The field is locked

Based on the signature and timestamp, the field is considered consciously locked by the signer. A Trusted Timestamp Authority (TTA) and/or verifier-supplied data that can be used to provide assurance as to the accuracy of the timestamp data (Barker, 2009).The

The e-form is accepted.

This algorithm is depicted in the figure overleaf

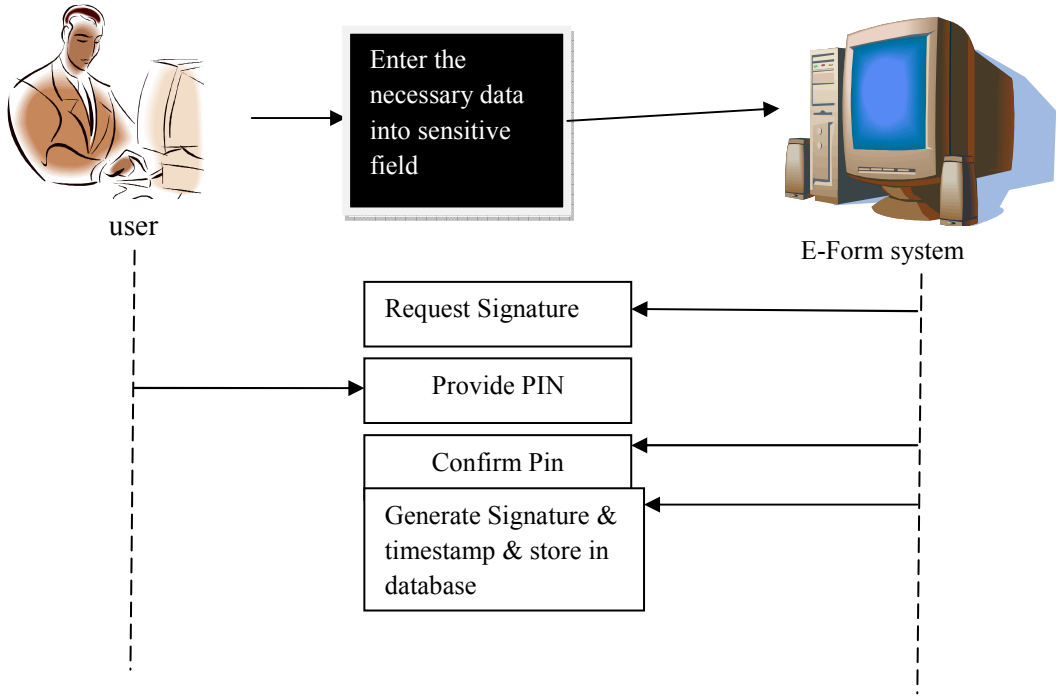

Figure 2 showing the transactions that make up the document signing process

5. VERIFYING THE E-FORM

In the case of a context, the owner of the registration system can always prove to the user of the e-form that the timestamp is intact and the cipher text can be decrypted to show the original signature criterion especially in the case of a legal issue.

5.1. COMPARISON TO EXISTING METHODS

As regards E-Form Processing for educational institutions, the issue security has been treated with certain peculiarities which is usually because they are intended to be open systems and security is believed to have an inverse relationship with usability (Okesola and Ogunseye, 2010).

6. CONCLUSION & FUTURE WORK

In this work, we have been able to able to propose a conceptual model that can cover up for the major pitfalls of e-forms. The deniability afforded e-form users can be reduced to the barest minimum by the signing model proposed in this work which can serve as a framework to developers. The model should find use even beyond educational institutions and future work should focus on strengthening the signature criterion and look at how digital signature strategies can be combined to ensure ease of use and provide more accountability from users.

REFERENCES

[1]. Algorithmic research (2010), Think Twice Before You Sign Anything Again - 12 Business Cases for Digital Signatures. Online at http://www.arx.com/digital-signature-eBook

[2]. EnTrust (2003), Guide To Enabling E-Government: Secure E-Forms And Data Capture. EnTrust Inc. 2003

[3]. Adobe systems incorporated (2006), Digital signature in PDF Language

[4]. Elaine Barker (2009), "Recommendation for digital signature timelines" NIST Special Publication 800-102

[5]. Folorunso Olusegun, Ogunseye Oluwafemi S., Sharma Sushil K. (2006), An exploratory study of the critical factors affecting the acceptability of e-learning in Nigerian Universities, Information Management and Computer Security, Emerald Publishing pg 496-505

[6]. Okesola J.O, Ogunseye O.S. (2010) "A Congenial Access Control Technique for Knowledge Management Systems". Global Journal of Computer Science and Technology, Pg 2. Vol 10 Iss. 14 ver 1.

ABOUT THE AUTHORS

Gbenga O. Ogunsanwo is an experienced Network analyst and administrator in the ICT Unit of Tai Solarin University of Education which he currently coordinates. He Obtained his first degree in computer science from Ogun State University (now Olabisi Onabanjo University), He also has a Masters in ICT (MICT) which he obtained from the University of Agriculture Abeokuta and is looking to his PhD in Computer Science. His previous works and research interest are E-Signing and Digital Signatures, encryptions, Human Computer Interactions, Access Control etc.

Oluwafemi S. Ogunseye is a seasoned researcher with publications in most of the world's top Computer Science Journal, He obtained his first and second degrees in Computer Science, from the University of Agriculture Abeokuta, and is currently working for the Government as a Programmer for the ICT Unit and as a Lecturer/Researcher. He is an MCITP, MCSA and a Linux+ with vast academic and professional experience. His areas of Interest includes Knowledge Based Systems, Information and Computer Security, Visualization, Machine Learning, Heuristics and Active Heuristics, Human Computer Interaction, etc.