Ettest: Secured Online Attestation

Sidhant Khokhar, Ankit Bengani, Jothi Kumar

Dept of Computer Science, SRM University,
Potheri, Kattankulathur, Tamil Nadu 603203

sb7152@srmist.edu.in ab3988@srmist.edu.in jothikuc@srmist.edu.in

Abstract—***Document Authentication is one of the most tedious as well as important job in today's world. We need attested documents in each and every sphere of our life and attestation is needed even in schools and colleges while submitting documents, certificates, or any other attestable papers.***

But with the pandemic and the fear of transmitting the disease, many firms and institutions moved to online form of attestation, one which is more convenient in today's fast-moving world.

Ettest aims to provide a more secure and flexible platform for the same work. The Ettest system handles the security and authenticity of the procedure by verifying registering user's identity and maintaining user session, identity verification is done on registration through sending an encrypted link through a QR code, session management is done through JAVA Spring Boot which assigns an access token every time a request is made to the system, and the database are managed with the help of mySQL servers.

The main security goals namely user verification, user authenticity and integrity. It will help small business organizations as well as educational institutes environments positively, since it reduces the risk of tampering and fraudulent activities, and also minimizes the human efforts required in achieving the attestation of any concerned authority.

Ettest have successfully achieved user verification by sending an encrypted link through QR code on the organization specific mail for the user, which is decrypted at the user's end using symmetric key algorithm through a mobile app, authentication and integrity by maintaining user's request session, which is done through JWT, Json Web Tokens, which provide access of each service to the users.

Keywords—Attestation, Authentication, Authorization, Authority, Encrypted, Verification, Integrity.

I. INTRODUCTION

There exists a number of methods in which a user identity can be verified be it login name or login password. These methods can however be easily tampered with, which compromises the integrity and user security. In this day and age, more and more organizations and institutes are moving to an online method of attestation [1].

The longhand transcribed signature has always been a part of our lives since the old times to this modern era, and it is considered as a person's identity or a means to give someone approval [2]. To get a document attested, one must visit the concerned authority in person, but in today's world because of the ongoing pandemic, it is not advised nor feasible as this increases the chances of transmitting the disease. Also, it is an inefficient approach since it is quite human efforts intensive. Most of the institutions or companies are closed physically, in case if someone wants their document to get attested, they'll have to rely on either email or a telephonic conversation with the concerned person, this is both time consuming and inefficient.

Also, there's the risk of fraudulent, identity tampering and fabricating activities which makes the applicant as well as the authority to be verified. Hence, the institutes and the organizations need a cheap yet fast reliable way which is secured in nature to verify user identity, and maintain integrity and authenticity of the procedure.

II. LITERATURE REVIEW

This paper surveys recent literature related to online modes of document circulation, signatures and management.

A comparison among these can be seen below, different systems are compared based on security, efficiency, its ability to keep the procedure authentic, cost and ease of adapting to the system.

It is quite easy to notice that most of these systems although are efficient but lags certain features and requirements, hence this paper strives to use the best of existing works and combine efficient and more robust features to achieve high efficiency and flexibility in one system.

In 2018, the Secure Sign was introduced which made e-signatures secure using technologies such as AES Encryption, user fingerprints and user id embedding in the documents using QR barcode [1]. Although the system was secure and tamper proof to an extent, the idea was very basic and did not even allow more than one person to sign it, making it less feasible. The system did not think of id theft and session management.

Verification of documents and resume is an important step in job recruitment and admission procedure [3]. The proposed system removed the need of verification of these documents manually. However, the system lacked the use of access rights which made it more difficult to manage the users.

Certificates are the most important documents in a person's life, they are the proof of accomplishments. However, these documents can be easily forged due to ineffective anti-forge mechanism [4]. It was proposed to generate and maintain certificates using Hyperledger, and IPFS. The system was made immensely complex with the use of Hyperledger, and the use of IPFS caused a lot of bandwidth wastage.

In 2020, an approach was made to form digital signatures as well as the software creating signatures and methods to secure it [5]. However, it is difficult to compare the developed model with the existing models also because of lack of ease to get

commercial signatures.

III. PROCESS FLOW

Ettest system strives to design an efficient yet flexible system which can prevent identity fabrication and tampering, which will allow remote party i.e., the applicant to get their document attested. Moreover, it provides conflict resolving methods in case of disputes.

Ettest system helps the user to ask for attestation from the list of available registered authorities, it allows the authorities to attest the documents from the comfort of their homes and an option to resolve conflict in case of a dispute.

It allows the admin to manage the registered applicants and the authorities.

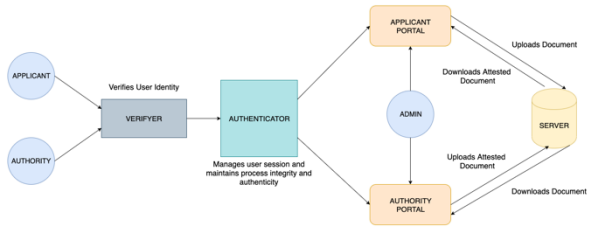

Figure 1.

The detailed architecture can be seen in figure 1, each registering entity will go through the following stages:

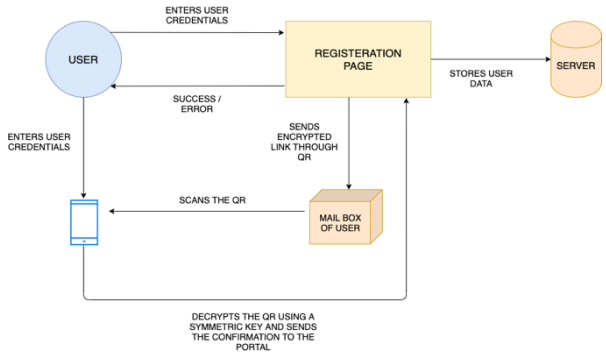

Figure 2.

A. Registration

For a user to fully access and use the system, they must be registered on the system first. This is a one-time process, where the user is asked to enter their credentials along with the organization or educational email given to them by the institute or the organization, A check is made to see if the user does so, in case user provides a personal email they are shown an error, upon successful submission of details, an encrypted link which is embedded in a QR is sent to the user's email, where with the help of our custom android app the user can scan the QR code.

On opening the app, the user is asked to enter his userID and password which is used to calculate a symmetric key, which then is used to decrypt the link obtained from scanning the QR, upon successful scanning, the user is redirected to the respective portal that they registered for; hence the registration process completes and user data is added to the database, initiating the authenticator. The detailed architecture can be seen in Figure 2. The encryption and decryption both the processes are carried out using Advanced Encryption Standard algorithm.

B. Authenticator

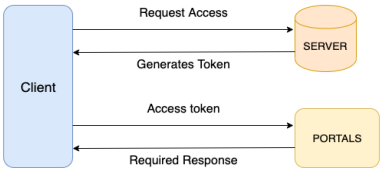

FIG : AUTHENTICATOR

Once the user logs into the portal, he is given a token generated only when the QR scanning is successful using the mobile app. The token is a refreshing token, which means that after every 15 minutes the previous token will be disabled and a new token will be generated if the user is still signed in. For every service the user wants to access, along with the api call, the token will be sent in the header. Once the token is validated by the authenticator service, only then can the service be called. The authenticator will not only act as an authentication service but also as the gateway for all the services, The architecture can be seen in Figure : Authenticator.

C. At Applicant Side

An applicant can log in the system where they are allowed to upload the document and are presented with the list of available registered authorities, to which they can send their document for attestation.

The uploaded document along with the user data is sent to the database, and a notification to the concerned authority sent.

D. At Authority Side

An authority can log in the system where they are presented with a list of available documents to be attested and they are given an option to raise conflicts if they don't agree with a particular document.

The authority can either download, physically sign a copy and send the scanned copy to back to the applicant or they can digitally sign the document. The updated document is then sent to the database.

Upon successful attestation the applicant will receive a completion notification.

IV. RESULTS

Ettest successfully fulfils the security and flexibility goals which are prevention of identity fabrication, authenticity and process integrity. To add more to the points Ettest doesn't allow anyone without a valid educational or organizational email to be registered, it also sends the encrypted registration link in a QR code hence preventing any sort of tampering by the user, upon successful scanning Ettest is able to verify the identity of the user, because of this scanning of QR procedure, Ettest is also immune to brute force attacks since each request can only be initiated upon successful scanning of QR. Then to maintain the integrity and the authenticity the user Ettest uses an Authenticator which generates and maintains user access tokens, which makes the system secure as well as abstract, as the authenticator works not only as an authentication medium but also as a gateway to all the services.

V. CONCLUSIONS

This setup presents an easy to use yet secure method of getting one's document attested without the need to be physically present at a place, hence consumes a lot less time and minimizes human efforts.

Although the system is quite flexible it is secured enough to be taken up by institutes and organizations to replace the physical means for document attestation. Furthermore, it allows a user to get multiple signatures from different authorities on a single document. Ettest will influence the current modes of attestation quite positively and in a complementing manner, by preventing fraudulent or mischievous activities such as identity fabrication, brute force attacks, tampering and misuse of data. The Ettest system saves time of both the applicant as well as the authority and is cost effective as there's no travelling involved.

To conclude the system will help users to get their documents attested and the authorities to attest the documents from the comfort of their homes in a secured and efficient manner.

VI. FUTURE WORK

To add more to this project in future we recommend addition of block chain to introduce hierarchy management in authorities, for example let us consider a student needs his document to be attested by his class teacher, the vice principal and then finally by the principal, the user can only apply for the signatures of other authorities only after the authority ranking below them has approved and attested the document, i.e. student will only allowed to apply for vice principal's attestation only after the class teacher's attestation so on and so forth.

One more additional feature can be to parse the entire document to be attested. Document parsing not only saves time but it also creates a better understanding of the document which is being submitted for attestation. In future the user can also be allowed to create an online safe-house for all the documents attested or unattested. This way the user won't have to worry about managing the documents.

REFERENCES

[1] Al Anood K. Alzahrani, Malak K. Alfosail, Maryam M. Aldossary, Muneera M. Almuhaidib, Sarah T. Alqahtani Nazar A. Saqib, Khalid A. Alissa, Norah A. Almubairik. "Secure Sign: Signing Documents Online", 31st December 2018, 21st Saudi Computer Society, National Computer Conference (NCC).

[2] Y.Cho, J.jung. "Online Signature Recognition Based on Pseudo-Inked Signature Image Template", 2017 International Journal of Humanoid Robotics.

[3] Hani Sami Brdesee. "An Online Verification System of Students and Graduates Documents and Certificates: A Developed Strategy That Prevents Fraud Qualifications", April-June 2019, International Journal of Smart Education and Urban Society, Vol. 10, Issue 2.

[4] Raghav, Nitish Andola, Rakhi Verma, S. Venkatesan, Shekhar Verma. "Tamper-Proof Certificate Management System", 6-8 December 2019, IEEE Conference on Information and Communication Technology

[5] Nikita I. Chesnokov, Denis A. Korochentsev, Larissa V. Cherckesova, Olga A. Safaryan, Vladislav E. Chumakov, Irina A. Pilipenko. "Software Development of Electronic Digital Signature Generation at Institution Electronic Document Circulation", 15th October 2020, 2020 IEEE East-West Design & Test Symposium (EWDTS)