International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Ettest: Secured Online Attestation

Sidhant Khokhar
Dept of Computer Science
SRM University
Chennai, India

Ankit Bengani
Dept of Computer Science
SRM University
Chennai, India

C. Jothi Kumar
Dept of Computer Science
SRM University
Chennai, India

***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, but moving such this procedure online comes with it's fair share of security risks.

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 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].

Document's attestation is one of the means by which credibility of a document can be established. Although the owner of the document is often held responsible for the credibility of the document, but at times it is needed to be attested by an concerned authority. The main intention for getting a document attested is to authorize it. Attestation is mostly provided in either stamps or hand written signatures, by the respective person or the institution.

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, or in the worst case scenario they'd have to visit the concerned authority in person, which due the current circumstances is difficult and hazardous.

University students in specific find it difficult institutionally and geographically to get their document attested and have to rely on traditional means such as: electronic mail, physical mail or visiting the authority in person [3]. Also, there's the risk of fraudulent, identity tampering and fabricating activities which needs the applicant as well as the authority to be verified.

Misuse of document is a reality in today's world and the current system is people dependent, it depends on the people involved during submission and retrieval handle a document which increases the risk of breaching the privacy of the applicant [4].

A privacy breach is said to happen when the data of a person is accessed, modified, disclosed or used without that person's approval, the consequences of privacy breach can be serious such as Identity theft, Defamation, Mental stress and Disruption of any services the data is related to. Organizations and institution are also susceptible to privacy breaches.

Frugality is also something that comes to mind when we adapt a new system, most of the organizations and institution are small scaled and because of this reason they have to be frugal while incorporating services for the comfort of their employees and students.

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.

The architecture of Ettest aims to solve the above listed issues in an adjustable, efficient and secured manner.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

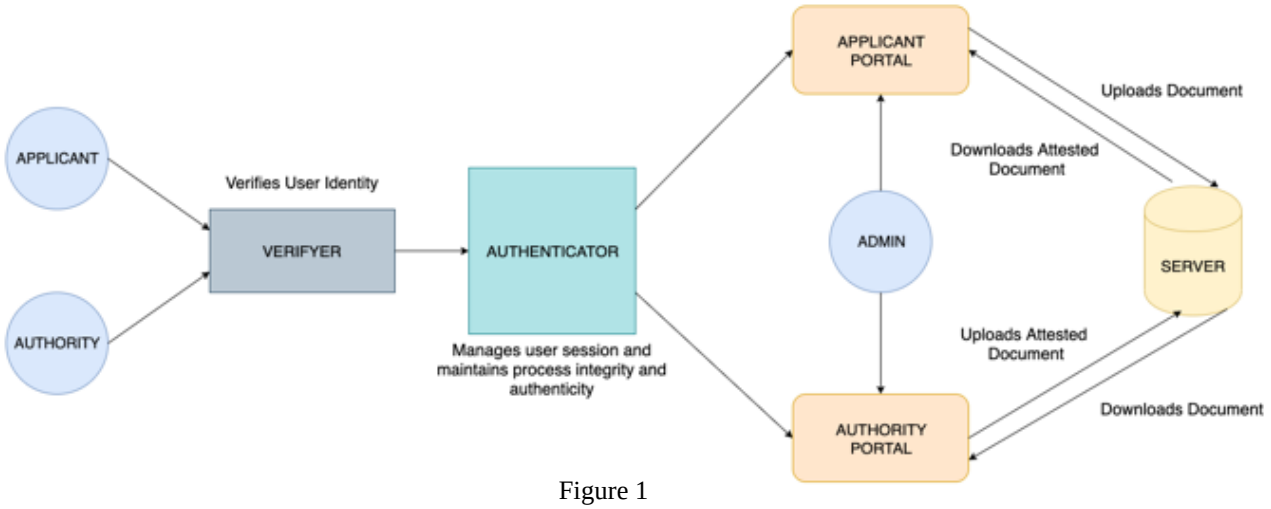

Figure 1

II. Literature Survey

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]. The system reduced the risk of frauds and forgery, and could be used over a wide range of areas. 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. There was no use of PDF417 which could have been more efficient as it generates a QR for a greater number of characters.

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. It allowed the university to stay in touch with the students and the system improved the job recruitment procedure. However, the system lacked the use of access rights which made it more difficult to manage the users. Scaling up would be a major setback.

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 mechanisms [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]. The addition of additional security modules increased the crypto stability of the system. However, it is difficult to compare the developed model with the existing models also because of lack of ease to get commercial signatures.

In 2014, a study revealed some major vulnerabilities in the OAuth 2.0 system [6]. The study revealed how an attacker can control a user's account without having their username or password. This study marked the importance of two factor authentication.

In [7], document authentication based on paper is presented. The document and author are verified by the use of QR code and digital signature. However, the problem lies when the documents are forged as it is very easy to print and scan documents cheaply and no means of document verification can be applied to detect such fraud unless there is a benchmark against which these documents can be judged.

After comparing all these proposed systems one can easily conclude that the systems could not focus on all the important aspects of an online attestation portal. The system proposed by us focuses on maintaining the security of the users using a double secure module and providing access rights. The access rights will enable exclusive access to different kinds of users (students, authority and admin). Also the users will have only certified documents uploaded and the admin in the middle can at any time look into the matter, and check for the authenticity of the paper. The flow of the proposed system is given below.

III. SYSTEM ARCHITECTURE AND 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. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

A. Registration

Define 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.

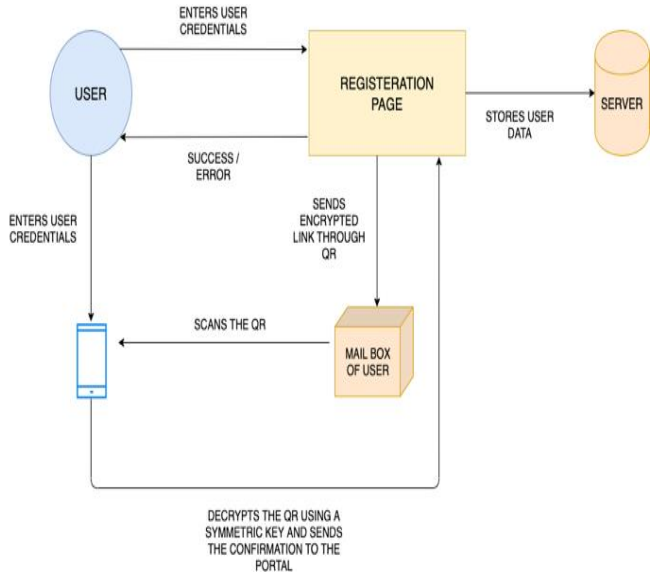

Figure 2

On opening the app, the user is asked to enter his user ID 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

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.

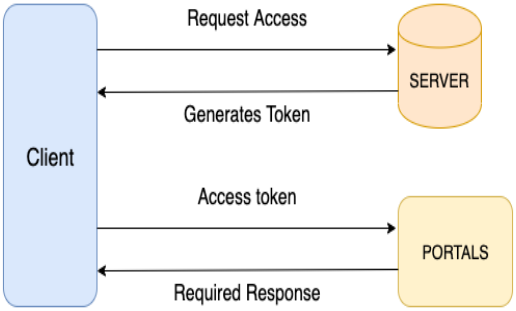

Figure Authenticator

The authority can download the document, then attest and finally upload the updated document. The updated document is then sent to the database. Upon successful attestation the applicant will receive a completion notification, then the applicant can download the attested document.

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.

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. CONCLUSION

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.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

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 WORKS

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.

Another additional feature can be, to parse the entire document that needs 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.

Apart from these we could extend the support to IOS platform for our mobile application, currently it is limited to android platform only. That would help us extend the usability of the portal as it would support a wider group of people.

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).

[6] Wanpeng Li and Chris J. Mitchell, Security issues in OAuth 2.0 SSO implementations In Sherman S. M. Chow, Jan Camenisch, Lucas Chi Kwong Hui, and Siu-Ming Yiu, editors, Information Security - 17th International Conference, ISC 2014, Hong Kong, China, October 12-14, 2014. Proceedings, volume 8783 of Lecture Notes in Computer Science, pages 529–541. Springer, 2014.

[7] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Signature and QR Code," ICCET, 2012.