International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

DIGITAL DOCUMENT SIGNATURE

Shankar Narayan[1], Shaikh Shadab[2], Prajakta Gaikwad[3], Hammad Sayyed[4], Kalidas Bhawale[5]

[1,2,3,4]*Computer Engineering, DRIEMS College of Engineering, Neral, Karjat*
[5]*Project Guide: Mr. Kalidas Bhawale*

Abstract - *In this era of technology and revolution there are many ways and tools to tamper anyone's document (Offer letter, certificate, insurance paper, etc.) and make it looks like any different person's document. Digital Document Signature provides a solution for different sectors of MNC's, organizations and individuals to compose, store, share and verify the documents. DDS generated documents contain a unique barcode which helps another organizations and individuals to verify the validity of a document.*

Key Words: Security, Digital Document, Integrity, Signature, Security, Centralize verification.

1. INTRODUCTION

Digital Document Signature is a web application provides security to all the documents which are implemented and composed. The associates of the documents will get the lifetime access to their digital documents and any authority can verify it by the verification panel provided to them. All the mandatory tools required to create an interactive and professional document related to any sector such as Education, Healthcare, Pharma, Manufacturing, IT, etc. is provided under the document creation panel. This web application mainly focuses on the Authentication, Integrity and Non- repudiation to electronic documents. Digital Document Signature provides a solution for different sectors of MNC's, organizations and individuals to compose, store, share and verify the documents.

1.1 Objective

The main objective of DDS is to provide a cheaper validation and verification of the documents by preventing forgery. Most of the big companies like Google have this software for their own purpose. If any company wants this then it has to pay a huge amount which is not feasible for small and startup companies.

We have developed this project and our objective is to provide this to small companies that cannot afford this software at a cheaper price, so even small companies can buy and validation and verification can be done easily. Since forgery of many documents is easily done in today's world, this software will help prevent it in a large scale manner. We have achieved this security of validation and verification by using MD5 algorithm. It uses a complex method of security. So even if the hacker is able to steal the document he cannot forge it.

1.2 Purpose

The main purpose of this project is to provide valid authentication of a given document at low cost. We are also enhancing the security by using SHA -256 algorithm. SHA-256 is a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. It is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. It uses SSL certificate to ensure data has not been modified by any means. This means that even if the digital document is attacked by hacker then also he cannot use it.

2. SYSTEM DESIGN

The digital document signature is the website which is designed and developed in PHP and MySQL. User interface (UI/UX) or front end of this website is developed in html, CSS, bootstrap, JavaScript, JQuery, and Ajax. Backend of document digital signature is developed in PHP. Digital document signature used MySQL database to store the data. We have also used different algorithm to secure the data like base64 encryption decryption method and hashing technique like sha256.

3. EXISTING SYSTEM

In the existing system, the document which is creating is not verified and even document which they are creating doesn't have any validation like QR code from end point. Due to this anyone can do fraud and scam easily. Some company or Organization does there document works manually in word or in other software they do not have any proper management of document whatever they are creating. So in feature if they want the past data to do verification most of them they can't do. Because of some reason like for example one company they stored their data or documents on the desktop if desktop get a format or crash them all data will be lost. So to overcome this problem we have developed and design the system in which user can build their document with proper validation so one can do scam or fraud. Whatever document that user will create will be stored with proper management so they can use that data in future.

When a company creates a document manually after the creation of a document they have to send that document manually to the user from email. In our system we have given the option to do that task in one click.

Disadvantages of Existing System:

- Not available for small company/Organization.
- Anyone can do scam or fraud easily.
- No database to store data.
- Document, create manually.
- Sending Document on Email Manually.
- Not secure.

4. PROPOSED SYSTEM

In our project the main purpose is validation and verification of the documents that an individual has. We have used 2 algorithms for the security of our documents one is MD5 algorithm and second is sha256 algorithm.

MD5 Algorithm was developed with the main motive of security as it takes an input of any size and produces an output if a 128-bit hash value. This encryption of input of any size into hash values undergoes 5 steps and each step has its a predefined task.

MD5 Algorithms are useful because it is easier to compare and store these smaller hashes than to store a large text of variable length. The MD5 algorithm is a widely used algorithm for one way hashes that are used to verify without necessarily giving the original value.MD5 Algorithm is used by UNIX systems to store the passwords of the user in a 128-bit encrypted format. But from many years MD5 has prone to hash collision weakness, i.e. it is possible to create the same hash function for two different inputs. MD5 provides no security over these collision attacks. Hence we are also using SHA -256 Algorithms.

SHA-256 is one of the most secure hashing functions in the market.

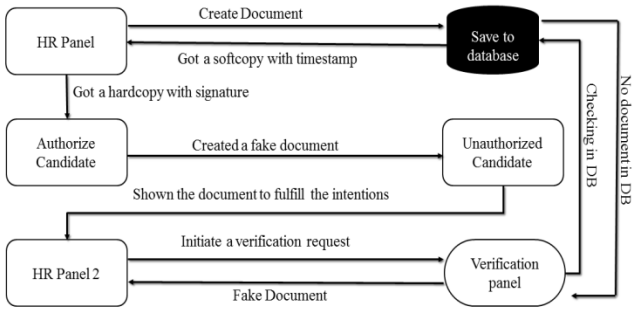

Fig -1: System overview

The US government requires its agencies to protect certain sensitive information using SHA-256. Three properties make SHA-256 this secure. First, it is almost impossible to reconstruct the initial data from the hash value.

A brute-force attack would need to make 2256 attempts to generate the initial data. Second, having two messages with the same hash value (called a collision) is extremely unlikely. With 2256 possible hash values (more than the number of atoms in the known universe), the likelihood of two being the same is infinitesimally, unimaginably small. Since we are using both these algorithms to secure our documents the chances of getting forget document becomes almost impossible.

Here are some screenshots:

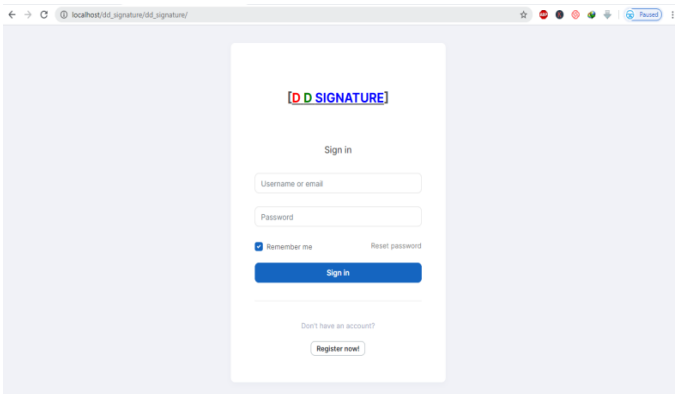

Fig -2: Sign in page

This is the sign in page of our web application also known as index page. When the user visit he first needs to sign in with his credentials or else needed to create an account through the signup page.

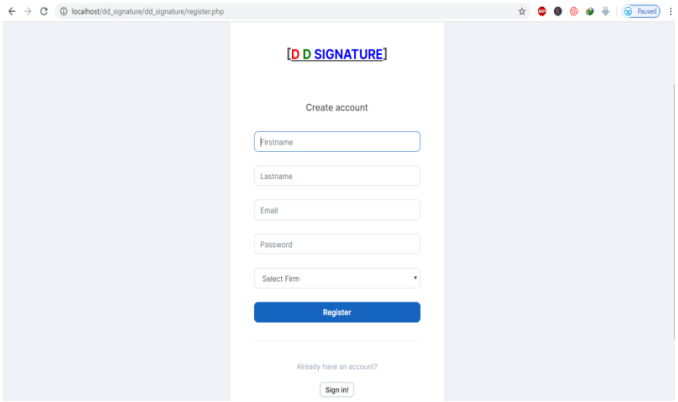

Fig -3: Sign up page

This is the registration page from which an individual, organization or a company needed create an account for further usage of services.

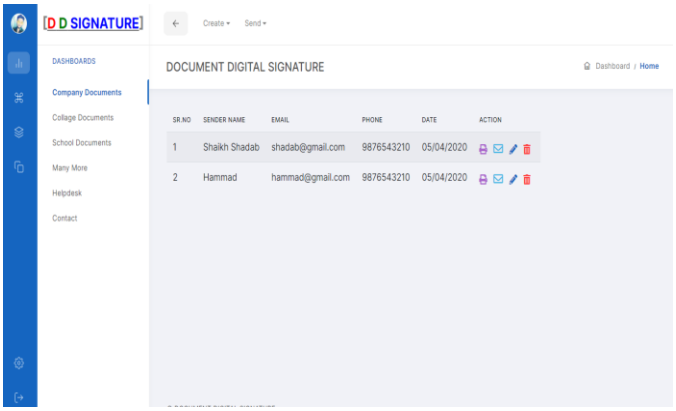

Fig -4: Dashboard

This is dashboard page for the admin of company from where he can manage all the documents created in the past and user can create any kind of document he want with the proper authentication system.

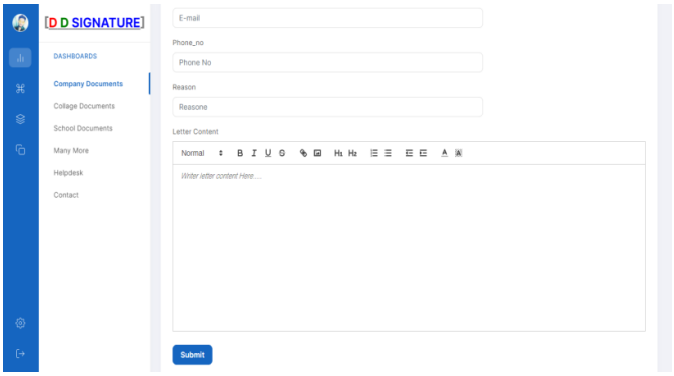

Fig -5: Document Composer Form

This is the form where user can compose the document it includes a jquery text editor which gives many features to customize the design of document and helps to make it interactive.

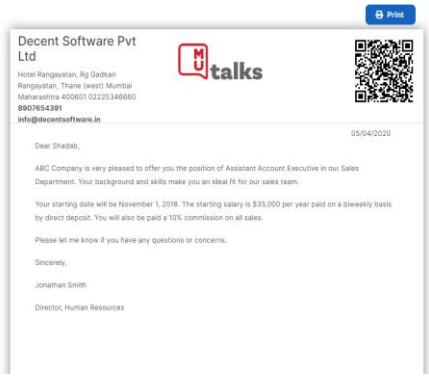

Fig -6: Document Preview

This is the preview of the document which is created by Composer. It contains brand name of the company, logo, barcode for authentication and all the necessary details of the company.

5. FEATURES

- User get interface to directly compose the digital document.
- Each document has its own unique id which signed and seal by composers unique private key.
- Interface to sign and seal other documents which are not composed on our platform/website.
- User can verify the documents originality.
- Reliable.
- Simple and easy to use.

6. FUTURE SCOPE

In future we are planning to add more features including payment via QR code scanning. Besides that this website can be used by government and non-government organizations for collection of funds for useful purposes. It can also be used in library for sales and purchase activities. It can also be used for donation purpose for government or non-government organizations like schools, hospitals etc.

7. CONCLUSION

Digital Document Signature project is an attempt to solve the present problem of document forgery in an efficient and reliable way. If any company wants this then it has to pay a huge amount which is not feasible for small and startup companies. We have developed this web application and our objective is to provide this to small companies that cannot afford this software at a cheaper price, so even small companies can buy and validation and verification can be done easily.

ACKNOWLEDGEMENT

We are thankful towards our college Dilkap Research Institute of Engineering and Management Studies, Department of Computer Engineering, for giving us the opportunity to do this innovative work. Would also like to show our gratitude to prof. Kalidas Bhawale, for sharing his pearl of wisdom with us during the course of this project work.

REFERENCES

[1] Hornbæk, kasper, & Erik, frøkjær. (2001). Reading of electronic documents.

[2] IEEE Recommended Practice for Software Requirements Specifications – IEEE Std 830- 1998.

[3] Blandford, ann, suzette keith, lain connell, & helen edwards. (2004). Analytical usability evaluation for digital libraries.

[4] http://stackoverflow.com

[5] http://www.w3schools.com

[6] http://www.php.net

[7] http://www.mysql.com