JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Automated Certificate Storage and Finder System Creation using SQL

#1 M Sabari Ramachandran , Asst Prof , Mohamed Sathak Engineering College /
#2 S Hazra , Asst Prof , Mohamed Sathak Engineering College , Kilakarai /
3 G Balamurugan , Asst Prof , Mohamed Sathak Engineering College , Kilakarai/
#4 N Balasubramanian , Associate Prof ,Dept of MCA, Mohamed Sathak Engineering College
#5 M Mohamed Rafi , Professor & Head , Mohamed Sathak Engineering College , Kilakarai

Abstract— The purpose of this paper is to create a SQL based certificate uploader, finder under database management system for the same. The provision to upload the certificate, prove the authenticity of the certificate and scrutiny for the certificates on behalf of the states and the central governments will be taken into and that is a considerable point of action. Importance of maintaining the certificates comes in handy when the accomplishment of the same is done by govt authenticated institutes. Taking the certificates and verification of the same for each and every notification and process of registration will seem to be too difficult at instance. Hence a dedicated, secured and authenticated system for the updating, storing and authentication of the certificates with a provision to find the certificate by using a random search will be more useful. That is being done in this paper.

***Index Terms*—Certificate Storage, Cyber Attack, SQL**

I. INTRODUCTION

With the ever-increasing use of Internet, the risk of security of user information is a great concern. Web Applications may steal the user data such as Certificates, Mobile numbers, Emails, Bank details, transactional passwords and much more are on high roads. With more than2.9M Web Applications, in google play store, so is the threat and necessity to save critical information such as Certificates and more on a secure storage system that will prove to be authentic. Apart from web applications, Cyber-attacks on User data or information by the web applications is growing concern. The following figure 1 gives the details of the ever-increasing attacks in cyber net on account of user account and information derivatives such as certificates.

Information is the essential vita for any individual or a business or opportunity. Information such as certificates are vital and have to be stored in a authentic location. There has to be a system that has to be developed so that they can be easily accessed and necessary information is provided to the government of the authorities they have intended to provide authorization.

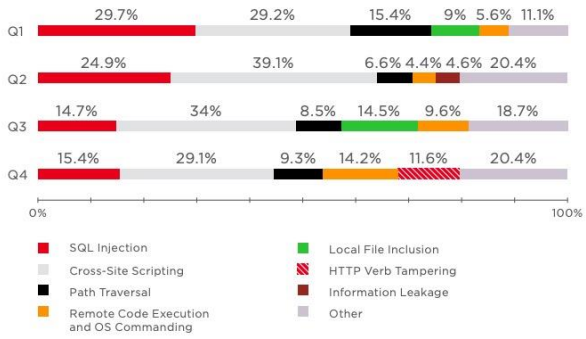


Fig 1. Web attack Statistics 2021

II. EXISTING WORK AND SYSTEM

Existing works in detecting and finding the certificates in websites are merely based on programming techniques. Most of them employed open loop technologies ie feedback recognition systems implementations were not deployed.

Systems that are used randomly employed certain datasets on anomaly applications to be categorized and fed into the systems for comparison with the existing application. These methods, though seemed to be effective, had its own advantages and disadvantages. The main disadvantage is that; it will not be able to add new specifications to the certificates. Only certain limited certificates can be uploaded and verified based upon the language they deploy to maintain the same.

Moreover, the accuracy level in finding out the

correct one or retrieving the correct certificate is around 50- 60%. This level of performance shall not be applicable for companies or organizations. Hence a robust authentic certificate verification system which is not subject or prone to attacks in the need and this has been implemented in this paper.

Vulnerability of attacks on websites are increasing. Given the above vulnerability ratio for a span of 10 years, it has become a haunting task for the individual to store their vital information without specialized web application techniques. The existing systems propose checking for web apps from the total list of applications in the cloud and then filter them based on the query.

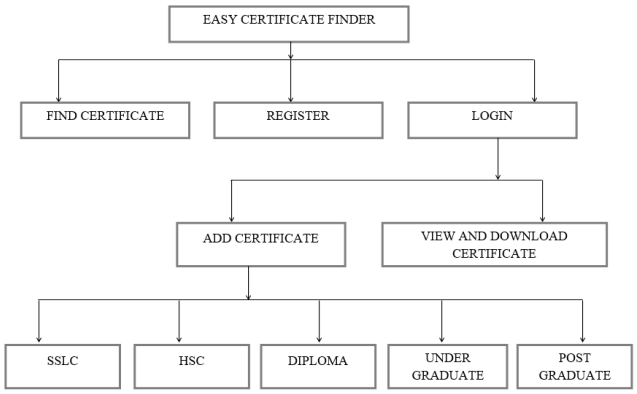


Fig 2 . The Proposed system diagram of existing system

Certificates originating from the user creates a log file, it is then processed using the standard data processing systems and is stored in the database. A random number is generated and stored as a recovery number. Whenever a query is raised this number is verified and the certificate is retrieved.

III. PROPOSED SYSTEM

In this paper we have come up with idea of using machine learning approaches for detecting the cyber-attacks in websites. First we have to gather dataset of past malicious websites as training set and with the help of Support vector machine algorithm and decision tree algorithm make up comparison with training dataset and trained dataset we can detect the cyber-attack on web applications with close a round 90% result.

A novel implementation scheme to collect the certificate is to create a system process, access them using the Algorithm, prune the available data and classify them into requirements. With help of SQL DB, we intend to make a comparison between the generated number and the provided number, so that we can make the SQL DB to be generated at a regular instance of time domain.

A. CERTIFICATE UPLAOD DATASET:

The uploading of the certificates is the primary task in the application. This forms the primitive stage of the application so that we can gather them using the reference number anytime later during the search aspect. Certificate Data from the individuals or companies having firewalls protected data classified as, all the data is sorted and stored in the database to be compared.

B. FILE LEVEL DEDUPLICATION

The process of comparing an uploaded file to that of the file backup is call the de duplication. This will prevent the time and the process consumption. A random file that has been generated is stored File-level data deduplication compares a file to be backed up or archived with copies that are already stored. This is done by checking its attributes against an index. If the file is unique, it is stored and the index is updated only a pointer to the existing file is stored. The result is that only one instance of the file is saved, and subsequent copies are replaced with a reference that points to the original file.

Column Name	Data Type	Allow Nulls
id	int	☐
name	nvarchar(MAX)	☑
username	nvarchar(MAX)	☑
password	nvarchar(MAX)	☑
mailid	nvarchar(MAX)	☑
contactno	nvarchar(MAX)	☑
altcontactno	nvarchar(MAX)	☑
address	nvarchar(MAX)	☑

Another one match checking looks within a file and saves unique iterations of each block. All the blocks are broken into chunks with the same fixed length. The primary idea behind the data de-duplication of the existing comparable datasets is to reduce the load on the server or application. This de duplication also reduces the memory consumed by the application, thus making the cyber-attack detection process less time consuming.

C. ACCURACY COMPARISION

The obtained certificates have to be cross checked if the process is working fine. An insight into the data classification detected 98% accuracy for

Thus a system with the provisions to upload , enable random number generation , verify and re download the same using a search query has been implemented , cross checked and verified for the highest level of accuracy for the same .

IV. SOFTWARE SYSTEM

A. Visual Studio

The project is developed using the Microsoft Visual Studio is an IDE (Interactive Development Environment) which means that it is a piece of software which binds a compiler, linker, debugger, code editor, GUI designer and other Powerful tools together. This in better than having each of them separately. You just need to press a single button and it will compile and link it and then put it under debugger, which if done manually will require you to input command line arguments to each compiler and debugger and linker..

V. RESULTS & COMPARISION GRAPHS

Checked graphical illustrations of the implementation are listed below.

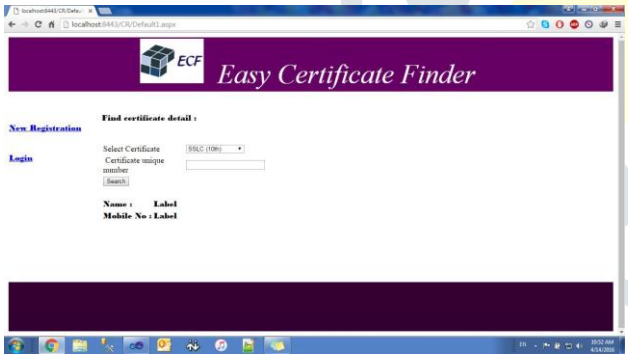
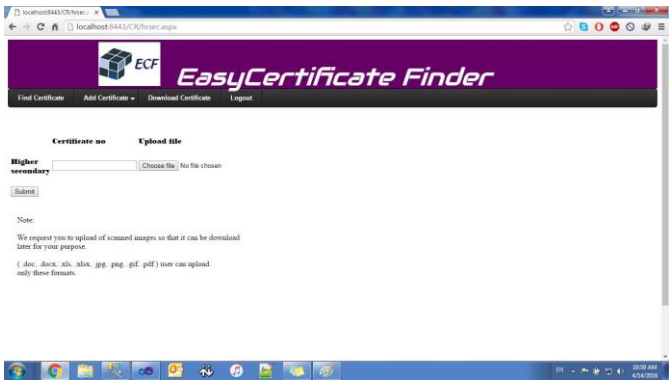
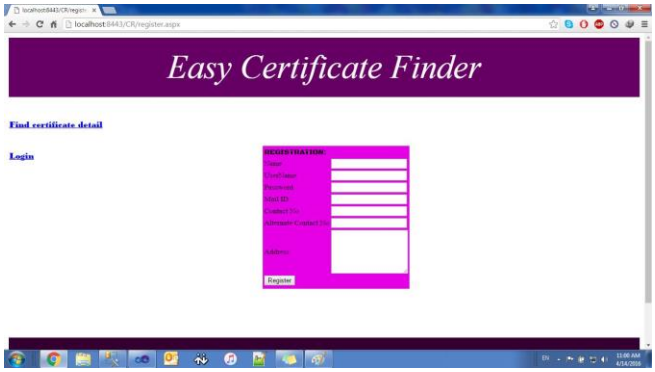


Fig 9. Screenshot of Registration





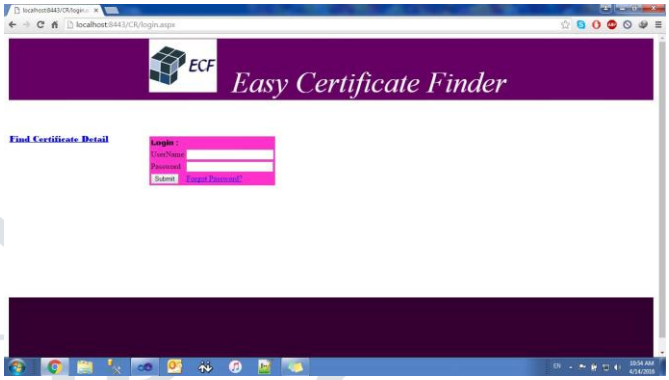


Fig 10. Graphical representation of Certificate Search

VI. CONCLUSION

We have designed, tested and implemented a rigorous application system that reduces the manual work of admin as well as project manager and the certificate details about the employees, projects, efforts, departments, etc. maintained and organized more efficiently. The authorized user is given permission to view the efforts and can modify/resolve efforts. Time consuming processes are made simple with the design . Accuracy of the certificate match and fetching is also found to have profound results.

VII. REFERENCES

1 E. Balagurusamy ,Programming in c# A Prime , Tata McGraw Hill Education Private Limited , third edition , (2001),pp 123 – 149.
Matthew Mac Donald, the Complete Reference ASP.NET, Tata McGraw Hill Education, First Edition, (2002), pp 62 – 111.

2 Wallace B. McClure Scott Cate Etna, Beginning Ajax with ASP.NET, Wiley India Pvt Limited, First Edition, (2008), pp 256 – 270.

3.Jenkins G.M. and Walt's D.G, Finance & Accounts Analysis and its Applications, Tata McGraw Hill, New Delhi, Second Edition, (1968) , pp 145 -153.

4.Gerald V Post, Fundamentals of Database Management Systems, Jacamar Publications, New Delhi, Third Edition, (2005), pp 223-247.

5.Jennifer Wisdom, Database Systems: The Complete Book (Goal Series), Macmillan Publishers, New Delhi, Fourth Edition (2000), pp 112-167.