APPLIED SCIENCE LETTER
Vol. 1, No.2, April (2011), pp.01–05

EFFICIENT MANAGEMENT OF DIGITAL CERTIFICATES USING CLOUDAND DATABASE

Jagan Mohan Reddy.M[1], M. SWATHI, V. SAHASRA, A. CHARISHMA[4], B. RUTHWIK REDDY[5]

Abstract - *Academic Awards issued by Academic Institutions will be made easier to issue, save, access, and verify digitally through the use of digital certificates. DCM is a special, innovative, and forward-thinking effort with the "Digital India" theme that aims to digitally empower educational records.DCM strives to realize the goal of providing digital academic certificates to every Indian. This draws young people from India and gives them access to digital, online, trusted, verifiable certificates that can be accessed securely at all times. DCM promises to eliminate the challenges and inefficiencies associated with gathering, managing, and displaying physical paper certificates.DCM is an all-inclusive system for providing properly identified and registered students with online certificates. The authenticity of certificate records is ensured by DCM's direct integration with the boards and universities that grant certificates.*

***KEYWORDS*: Digital certificate, Innovative, Trusted, Authenticity, Progressive initiative, well identified**

1. INTRODUCTION

The DCM (Digital Certificate Management) program is a novel, forward-thinking move toward the digital enabling of educational records. In order to make it simple to apply for jobs, loans for higher education, and other opportunities, DCM will create an online portfolio of all education certificates from Academic Institutes (Universities, Institutes, and Boards). This portfolio will be trusted and easily verifiable. DCM interacts with Boards and Universities directly, guaranteeing the authenticity of certificate records.Academic institutions will gain a technological advantage thanks to DCM. They don't need to make any investments, pay any charges, or put in any maintenance work if they issue and retain all of their data electronically. In a safe online approach, the university or board will directly lodge the academic awards in the DCM system. Online verifiability, a key component of DCM, acts as a potent deterrent.

2. EXISTING SYSTEM

All the certificates of different universities are maintained manually i.e. (hard copy). Therefore, it is difficult to handle these certificates by the students. It results in no security, chance of creating fake certifications, there is no proper way of validating the certificates. The figures given below i.e., [fig 1][fig 2] represents the hard copy of the certificate. Therefore, they are printed by the


Karnataka Secondary Education Examination Board
Certificate

board of educations and are sent to the respective institutions. Those institutions handle those hard copy certificates to the students. It is a time consuming as well as a risky process because it leads to missing or damage of the certificates.

Fig [1]: Hard Copy of Educational Certificate

ISSN 2454 - 7239
Copyright ©2022

ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ, ಬೆಳಗಾವಿ
VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM
KARNATAKA, INDIA

Certifies that

SUMIT BHOWMIK

ಬ್ಯಾಚಲರ್ ಆಫ್ ಇಂಜಿನಿಯರಿಂಗ್

ಪದವಿಗೆ ಅಗತ್ಯವಾದ ಅರ್ಹತೆಗಳನ್ನು ಳ್ಳವರೆಂದು ಪರಿಗಣಿತವಾಗಿರುವ ಕಾರಣ
ಮೇಲೆ ಕಾಣಿಸಿದ ಪದವಿಗೆ ಅವರನ್ನು ಅಂಗೀಕರಿಸಲಾಗಿದೆ.

has been duly admitted to the Degree of

Bachelor of Engineering

in recognition of the fulfilment of requirements

for the said degree through

ವಿದ್ಯಾಲಯದ ಹೆಸರು Name of the College	:	Sri Siddhartha Institute of Technology, Tumkur (Autonomous College)
ಪರೀಕ್ಷಾ ಕ್ರಮ ಸಂಖ್ಯೆ University Seat Number	:	1SS07CS122
ವಿಷಯ / Subject	:	Computer Science & Engineering
ಶ್ರೇಣಿ Class	:	First Class

A 012996

ವಿಶ್ವವಿದ್ಯಾಲಯದ ಮುದ್ರೆಯೊಂದಿಗೆ ಕೊಡಲ್ಪಟ್ಟಿದೆ
Given under the seal of the University

ಬೆಳಗಾವಿ
Belgaum

ದಿನಾಂಕ
Date : April 05, 2013

ಕುಲಪತಿ
VICE CHANCELLOR

Fig [2]: hardcopy of the Other University certificate

2.1 DISADVANTAGES OF EXISTING SYSTEM

- Less Secure
- need to print & distribute certificates
- risk of losing, spoiling, damaging the Certificate
- Immediate availability of certificates is an issue
- Chances of creating fake certificates

APPLIED SCIENCE LETTER
Vol. 1, No.2, April (2011), pp.01–05

Fig [3]: Damaged Certificate

PROPOSED SYSTEM

DCM is a complete system for Issuing OnlineCertificates to Well Identified and Registered Students.DCMintegrates directly with Boards / Universities who issue Certificates and hence ensures Authenticity of Certificate Records. Certificates will be stored in the third-party cloud securely in the encrypted format. Therefore, the below fig
[4] represents the soft copy of a certificate in a webpage.

Fig [4]: soft copy of the certificate in a web page

FIGURE [5]: BLOCK DIAGRAM

Fig [1] Description: Certificates will be uploaded by the board of higher authorities. Those certificates are storedin the cloud. Each student will be having a unique user id and password through which they can access their accountand can view the certificate.
Academic Institutions - Such Universities / Boards / Academic Institutes / Assessment Bodies as are identified by MHRD / UGC will join DCM system. These institutions will sign model agreement proved by MHRD & UGC.
Role & Responsibilities

- Join DCM System
- facilitate students to register on DCM
- Collect & Verify Student's Aadhaar / DCM ID
- Provide Master Data (Courses, Subjects, Colleges/Schools, etc.) and Certificate Templates
- Provide digitally signed data to Depository - Upload awards and seed with Aadhaar / DCM ID
- Advise all Certificate Verification Users to refer toDCM

Students / Certificate Owners – Online & Simple Aadhaar based registration. If Aadhaar not available, Student can submit registration details online. Student needs to approach his / her Academic Institution to Verifythe details.

- Easily register online on DCM using Aadhaar based registration. Provide your Aadhaar Numberand consent.
- Your Aadhaar details are presented on the screen,create your User ID, Password and its done.
- If Aadhaar is not available, register all your detailson the system, upload your photo and signature image and create your preferred user ID and password. DCM will issue DCM ID. In this case, present the details to the Academic Institution to

ISSN 2454 - 7239
Copyright ©2022

verify the details.

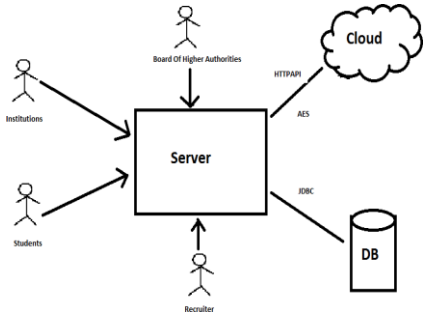
- Registration & Publication of ImportantInformation
- List of Academic Institutions - Eligible &Participating
- List of Affiliated Colleges / Institutes / Schools
- List of Courses Conducted
- This will provide a single point of all important information about Participating Academic Institutions and their Course and Awards details.

Cloud:

In this module certificates will be stored in the third partycloud securely in the encrypted format.

Verification Users (Employer Companies, VISAConsulates, Academic Institutes etc.)

- Online, Quick and Reliable Verification ofCertificates
- Audit Trail of all Verification results
- Access to Authenticated Copy of Certificates
- No risk of relying upon fake and forgedCertificates.
- Reduces Cost, Time and Efforts for Verification
- Proper records for all expenses incurred forVerification



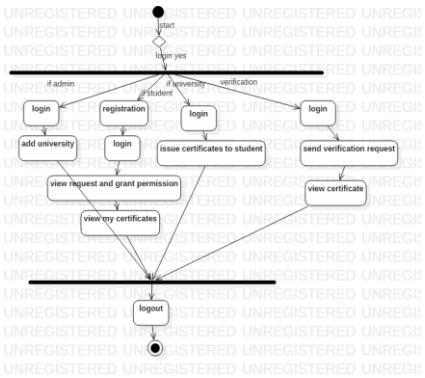


Fig [6]: Activity diagram

Fig [6] Description: This is the activity diagram which shows the activities which are performed. people who want to login are basically divided into four cases

- If admin
- If student
- If university
- verification

Case [1]: If admin:-can login and then add university andwill logout.

Case [2]:If student :-first registration must be done thencan login to the account and can view request and grantpermission .they will having only read option .they can'tedit the certificate. And then they can logout.

Case [3]:If university :-can login and issue or upload thecertificate to the student and can logout. they will have read and edit option.

Case [4]; Verification :-in case of verification of certificates

They can login and should send verification request andcan view the certificate. Therefore, they will have only read option.

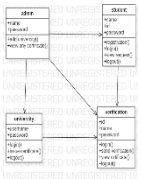


Fig [5]: Block Diagram

Fig [7]: class diagram

3. CONCLUSION

ISSN 2454 - 7239
Copyright ©2022

We are implementing this digital certificate management system which is easy to handle.There will be no manipulations, forgery (chance of creating fake certificates). Immediate availability of Certificates upon upload by Academic Institute - No need to visit anywhere to apply and collect. Online, Permanent Record of Certificates available at all times. No risk of losing, spoiling, damages the Certificate. it also provides security for the certificates by encrypting the data by storing in the cloud. Anytime, Convenient access to Certificates. Verified Certificate Records can be provided to any employer, bank; no need for photocopies, notarization, presentation of original copies etc.

REFERENCES

[1] KL Ginter, VH Shear, FJ Spahn, DM Van Wie… - US Patent …, 2006 - Google Patents The present inventions provide an integrated, modular array of administrative and support services for electronic commerce and electronic rights and transaction **management**. These |administrative and support services supply a secure foundation for conducting financial …

[2] M Tarpenning, B Kavanah, B Slesinsky - US Patent 6,513,117, 2003 - Google PatentsA delivery **system** for managing security keys uses three key pairs to establish, register, move and revoke rights in a device to view protected information. The first and second key pairs cooperate to establish secure **certificate** containing a device public and private key …

[3] P England, JD DeTreville, BW Lampson - US Patent 6,327,652, 2001 - Google Patents… Alternatively, if the rights manager **certificates** on the components are short-lived and must be renewed … a version that is found to be untrustworthy will not have its **certificate** renewed … to the boot block, one exemplary embodiment suitable for use with a **digital** rights **management** …

[4] B Multerer, KS Schwartz, K Stebbens - US Patent 6,134,658, 2000 - Google Patents… G06— COMPUTING; CALCULATING; COUNTING; G06F—ELECTRIC **DIGITAL** DATA PROCESSING; … is presently no capability to manage authentication **certificates** for multiple …The authentication **certificate management system** therefore automates the **certification** process, from …

[5] S Ramasubramani, PF King - US Patent 6,233,577, 2001 - GooglePatents…A **digital certificate**,orsimply **certific ate**, is issued by a **Certification** Authority (CA) and signed with … **digital certificates** is defined by the CCITT X.509 international standard; thus **certificates** can be … A **digital certificate** uses public key encryption techniques that are based on a pair of …

[6] Q Liu, R Safavi-Naini, NP Sheppard - Proceedings of the Australasian …,2003-dl.acm.org… user's identity for example by having the user present a valid **digital certificate**, charge his … electronic information or content that uses encryption, **digital** signature and **digital certificates** to ensure … situation in the domain of DRM, focusing on the US **Digital** Millennium Copyright

[7] T Enokida - US Patent 6,981,139, 2005 - GooglePatents In a **digital certificate management system**, a client/server **system** is connected to a **digital certificate management** apparatus capable of communicating with clients and servers. Mutual authentication is performed between the clients and the servers by using **digital** …

[8] T Moses, R Vandergeest - US Patent 6,108,788, 2000 - Google PatentsA receiver validates the **digital** signature by reference to the received **certificate** …Such **certificate management system** and method should facilitate variable **certificate** content specification by a subscriber and also issue variable content-based **certificates** to facilitate …

[9] LC Puhl, DH Vogler, EA Dabbish - US Patent 6,223,291, 2001 - Google Patents… in a wireless electronic commerce **system** comprising a wireless network operator **certification** authority having … at least first and second attribute authorities, having respective first and second **digital certificates** that are dependent from the root public key **certificate**, where the …

[10] P Baratti, P Squartini - US Patent 6,574,612, 2003 - Google Patents… License **certificate** files may contain some encryption or checksum information that allow the license server to verify their … US20060206712A1(en) *, 2005-03-10, 2006-09-14,