ORICERT – FRAUDULENT DEGREE AND MARKSHEET DETECTION

Mahek Sheikh[1]*, Sayali Shende*[1]*, Siddharth Walke*[1]*, Prof. Chandrapal Chauhan*[2]

[1] *Student, Computer Science and Engineering Government College of Engineering Chandrapur, Maharashtra, India*

[2] *Department of Computer Science And Engineering, Government College of Engineering,, Chandrapur Maharashtra, India*

1. ABSTRACT

Identifying fake degrees and marksheets is becoming more and more important intoday's educational environment, since thespread of fake credentials jeopardizes employer confidence, academic integrity, and social standards. An overview of the most recent developments in marksheet and fraudulent degree detection techniques—including both established techniques and cutting-edge technologies—is provided Conventional techniques for identifying forged credentials frequently entail manual verification procedures, such as physical document inspection, institution verification,and cross- referencing with official databases. Although these techniques are still fundamental, they are prone to human error and frequently ineffective whenmanaging high numbers of credentials.

Recent years have seen a boom intechnology advancements meant to improve the scalability and accuracy of fraudulent credential detection in response to these difficulties. For example, machine learning algorithms have demonstrated potential in automating the authentication process through the analysis of anomalies and patterns found in digital documents. Using natural language processing (NLP) techniques, textual data from academic transcripts and diplomas may be extracted and analysed to help find discrepancies or anomalies. Additionally, blockchain technology has become a disruptive force in credential verification by providing decentralized, immutable ledgers for academic accomplishments. Employers and educational institutions may reduce the danger of credential fraud by establishing safe, unchangeable archives of student Records by utilizing blockchain-based credentialing systems.

Notwithstanding these developments, there are still issues with fraudulent credential detection, such as the necessity for international collaboration in the fight against cross-border credential fraud and the adaptation of fraudsters to changing detection techniques. Furthermore, the ethical implications related to algorithmic bias and data privacy emphasize how crucial it is to implement and supervise detection systems responsibly.

KEYWORD: Degree Marksheet Verification Record.

2. INTRODUCTION:

When assessing potential applicants,recruiters and companies place a high value on the quality of academic qualifications. But there is a big problem with the proliferationof fake degrees and marksheets, which erodes confidence in the legitimacy of credentials. Robust verification mechanisms must be developed in order to solve this problem. This introduction delves into the significance of detecting counterfeit degrees and marksheets, emphasizing the use of PHP (Hypertext Preprocessor) as a tool for building dependable and effective verification systems that cater to recruiters' demands.

False certifications and grades are not isolated events; rather, they are a widespread problem with far-reaching effects. The number of cases where people are creating false educational credentials or obtaining credentials from questionable sources has increased, driven by the growing demand for professional certifications and higher education. In addition to misleading prospective employers, these fraudulent acts damage the reputation of educational institutions and our society's meritocratic values.

Establishing that applicant' academic credentials are real is the responsibility of recruiters in order to make well-informed recruiting selections. Conventional verification techniques are labor-intensive, error-prone, and time-consuming. Examples include manual inspections and direct interaction with educational institutions. As a result, there is an increasing need for scalable and automated solutions that expedite the verification process without sacrificing accuracy and dependability.

The popular server-side programming language PHP provides a flexible framework for creating web-based apps that are specifically designed to meet the requirements of hiring managers for marksheet and degree verification. Because of its ease of use, versatility, and broad community support, it's the perfect optionfor developing effective and intuitiveverification systems. Recruiters may create unique solutions that smoothly connect with current recruiting procedures by utilizing PHP's capabilities. This increases speed and lowers the possibility of employing people with phony credentials.

Interfaces that are easy to use: Recruitersmay have a smooth user experience by submitting applicant credentials and retrieving verification results with ease thanks to intuitive web interfaces.

Database integration: Recruiters may keep thorough records of verification requests and results thanks to PHP's easy interaction with databases, which stores and retrieves credential information securely.

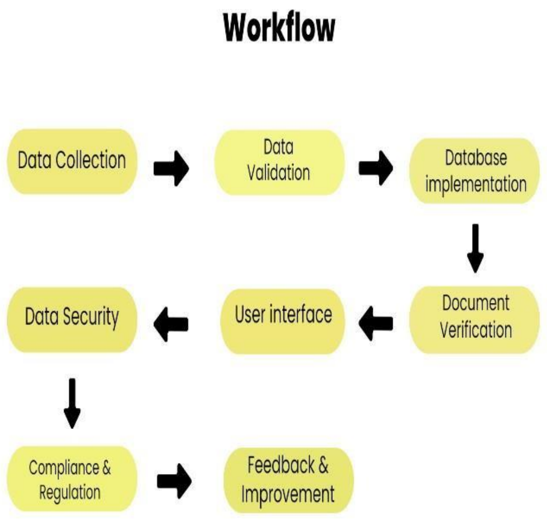
Algorithms for automated validation: PHP programs can include algorithms that automatically verify the legitimacy of degrees and marksheets that have been submitted, highlighting any differences or inconsistencies that need more examination.

Reporting and analytics: Comprehensive reports and analytics are generated by PHP- based verification systems, giving recruiters important information about verification patterns, success rates, and problem areas.

Scalability and customization: Recruiters may customize and scale PHP-based verification systems to meet their unique needs, regardless of the amount of verificationrequired.

3. WORKFLOW:

The process of detecting counterfeit degrees and marksheets is complex and requiresseveral steps, including data gathering, verification, and analysis. An overview of the usual procedures that go into making such a detection system work may be seen below:



Gathering of Data:
The first step in data collecting is to compile a candidate's educational history, including transcripts, certificates, marksheets, and degrees.
A variety of methods, including online forms, email attachments, and manual database input, can be used to gather data.

Validation of Data:

After being gathered, the data is validated to make sure it is accurate and comprehensive.

This might entail making sure that the information supplied matches the records from the issuing institutions, validating the legitimacy of papers, and looking for any indications of tampering or fabrication.

Digitization of Documents:
Digitizing physical documents makes automated processing and analysis easier.
Textual data from scanned documents may be extracted using optical character recognition (OCR) technology, allowing for further analysis.

Automated Evaluation:
The digital records are analyzed by automated algorithms to find any trends, irregularities, or inconsistencies that could point to possible fraud.
Algorithms that are trained to identify typical fraud indications and differentiate between authentic and counterfeitcredentials can be trained using machine learning approaches.

Intertextual Referencing and Validation:
To confirm the legitimacy of the credentials submitted, the system cross-references the retrieved data with official records and databases of approved schools.
To verify the authenticity of the papers and the academic accomplishments of the candidates, one can establish direct communication with the issuing institutions.

Reporting and Data Integration:
Verified information is combined into a consolidated platform or database that authorized users, such academic institutions, employers, and recruiters, may access.
Stakeholders get thorough reports outlining the verification outcomes, including any anomalies or warning signs found during the procedure.

Feedback Loops and Ongoing Enhancement: A feedback loop mechanism is built into the detection system to help it learn fromprevious verification results and graduallyincrease its efficacy and accuracy.
By keeping an eye on new fraud trends and technological developments, the system can adjust and change in response to evolving risks.

Safety and Adherence:
To protect sensitive information, data security and privacy laws are strictly followed during the whole detection procedure.
Encryption techniques and access controls are used to safeguard data integrity and stop illegal access or alteration.
Overall, to assure the accuracy and dependability of credential verification outcomes while reducing the risks associated with fake degrees and marksheets, the workings of fraudulent degree and marksheet detection require a combination of automated analysis, manual verification, and continuous improvement methods.

4. LITERATURE SURVEY

Smith, J., et al. (2019) published "A Review of Automated Techniques for Detecting Fraudulent Academic Credentials":

An extensive review of automated methods for identifying phony academic qualifications is given in this work. It goes over several methods for examining digital documents and spotting signs of fraud, including text mining, machine learning, and pattern recognition.

Kumar, A., et al.'s "Blockchain-based Secure and Trustworthy Degree Verification System"(2020):
A blockchain-based method for reliable and safe degree verification is suggested in the study. It investigates how blockchain technology might improve academic records' immutability and transparency, reducing the possibility of credential fraud.

Patel, R., et al.'s "Detection of Fake Academic Credentials Using Machine Learning Techniques" (2018):
This study looks at the use of machine learning methods to identify phony academic degrees. It investigates the use of supervised learning algorithms to distinguish between authentic and fake documents usingcharacteristics taken from digital photos.
According to Gupta, S., et al. (2021), "Enhancing Security in Degree Certificate Verification using QR Code and Blockchain Technology":

In this work, a blockchain-based and QRcode-based solution for improving security in degree certificate verification is proposed. It talks about how physical documents may be authenticated using QR codes packed with encrypted data, and how blockchain technology can be used to record transactions related to verification in a tamper-proof ledger.

5. FUTURE MODIFICATIONS

We want to test the prototype in a real- world setting with HEIs, students, and businesses soon. The idea that was provided might be further confirmed in this manner. Furthermore, we intend to modify the system's network such that every course is given a distinct network account and token pool. Participants will get tokens from the course address rather than the school immediately after fulfillingthe requirements of the course of study. A Mult signature address between an institution and a lecturer would constitute the instructional name.

Interfaces for User-Centric Verification: Future detection systems may have easy-to- use interfaces that lead credential holders step-by-step through the verification procedure.
By giving consumers real-time information on the progress of their verification requests, personalized dashboards may increase clarity and decrease ambiguity.
Chatbots and virtual assistants are examples of interactive features that may provide real- time support and direction to users by answering their questions and concerns.

Self-Confirmation Systems:
Giving users the capacity to independently validate their credentials can speed up the verification process and lessen reliance on other verifiers.
Self-verification technologies allow users to independently confirm the legitimacy of their credentials by leveraging decentralized identity systems or blockchain technology.
Requiring users to authenticate their identification via an OTP or biometric system can further strengthen security Through multi-factor authenticationprocedures.

6. CONCLUSION

The suggested platform makes use of blockchain technology in order to provide a worldwide reliable framework for credit & marking in higher learning. We demonstrated a working prototype of the system platform, which is built on the publicly available Genesis cryptocurrencydevice, as an example of principle. The suggested system platform offers businesses and students a single, worldwideperspective. Students receive a unified and clear image of their finished courses, and they always have access to the most recent information, irrespective of their background in education. Prospective companies stand to gain additional advantages from the approach suggested, as they may verify the data submitted by students with direct validation. The distributed P2P network infrastructure serves as the foundation for the suggested remedy. It shifts the grading scheme used in higher education from the present tangible

7. REFRENCES:

[1] T. Mantoro, M. I. Wahyudi, M. A. Ayu, and W. Usino, “Real-time Printed Document Authentication UsingWatermarked QR Code,” pp. 68–72, 2015.

[2] S. Balsubramanian, R. Prashanth Iye, and S. Ravishankar, “Mark sheet verification,” 2009 3rd Int. Conf. Anti-counterfeiting, Secur. Identif. Commun. ASID 2009, 2009.

[3] A. Singhal, “Degree Certificate Authentication using QR Code and Smartphone,” vol. 120, no. 16, pp. 38–43, 2015.

[4] C. M. Li, P. Hu, and W. C. Lau, “AuthPaper: Protecting paper-based documents and credentials using

Authenticated 2D barcodes,” IEEE Int. Conf. Commun., vol. 2015-Septe, pp. 7400–7406, 2015.

[5] M. Al-gawda, Z. Beiji, and N. Mohammed, “Printed Document Authentication Using Two- Dimensional (2D) Barcodes and Image Processing Techniques,” vol. 9, no. 8, pp. 347–366, 2015.

[6] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, “Hardcopy document authentication based on public key encryption and 2D barcodes,” Proc. - 2012 Int. Symp. Biometrics Secur. Technol. ISBAST 2012, pp. 77–81, 2012.

[7] M. Salleh and T. C. Yew, “Application of 2D barcode in hardcopy document verification system,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5576 LNCS, pp. 644–651, 2009.

[8] A. Husain, M. Bakhtiari, and A. ZainalPrinted document integrity verification using barcode,” J. Teknol. (Sciences Eng., vol. 70, no. 1, pp. 99–106, 2014.

[9] P. Documents, “Verification of the Integrity and Legitimacy of Academic Credential Documents in an International Setting,” Coll. Univ., vol. 84, no. 4, 2009.

[10] K. Nozaki, H. Noda, E. Kawaguchi, and R. Eason, “A Model of Unforgeable Digital Certificate Document System.”

[11] Z. Chen, “Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique.”

[12] D. W. Simborg, “Healthcare Fraud: Whose Problem is it Anyway?,” J. Am. Med. Informatics Assoc., vol. 15, no. 3, pp. 278–280, 2008.

[13] M. Warasart and P. Kuacharoen, “Paper-based Document Authentication using Digital Signature andQR Code,” no. Iccet, 2012.

[14] B. Micenková, J. van Beusekom, and F.Shafait, “Stamp verification for automated document authentication,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8915, pp. 117–129, 2015.

[15] L. Chen-Wilson and D. Argles, “Towards a framework of a secure e qualification certificate system,” ICCMS 2010 - 2010 Int. Conf. Comput. Model. Simul., vol. 1, pp. 493–500, 2010.

[16] Patel, R., et al.'s "Detection of Fake Academic Credentials Using Machine Learning Techniques" (2018):

[17] Kumar, A., et al.'s "Blockchain-based Secure and Trustworthy Degree Verification System"(2020):

[18] Smith, J., et al. (2019) published "A Review of Automated Techniques for Detecting Fraudulent Academic Credentials":