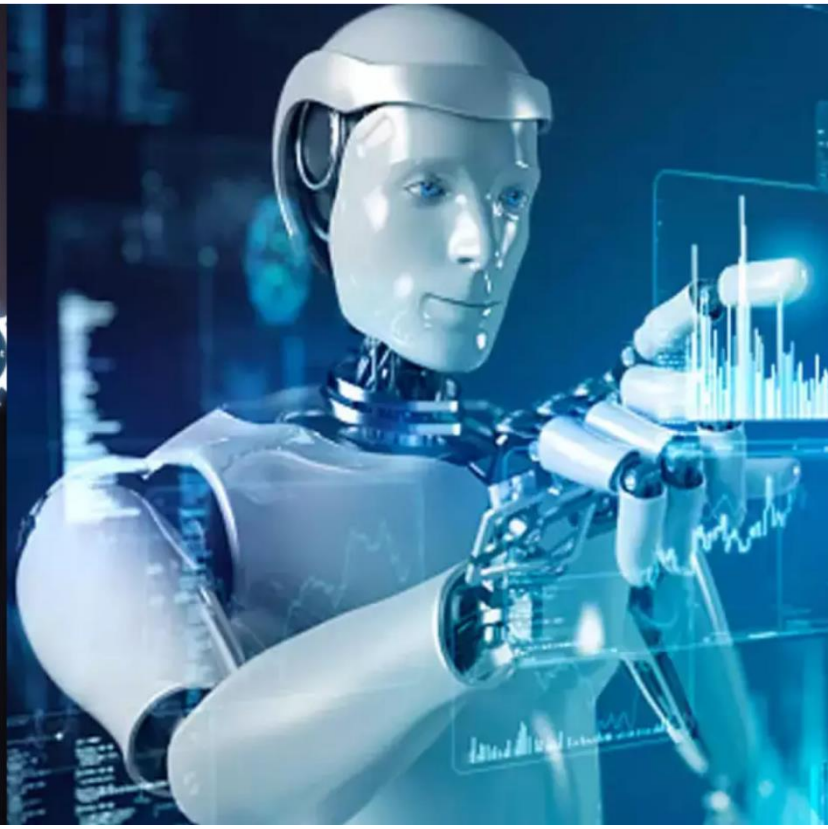
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503388|

Towards Unified Cyber security: Machine Learning-Driven Cryptographic Identification and Web Vulnerability Analysis

Rohan Pise[1], Pranav Kadam[2], Pratik Sangale[3], Yash Shejwal[4] , Prof. Ankita Pokale[5],

UG Student, Department of Artificial Intelligence and Data Science, Engineering Ajeenkya DY Patil School of Engineering Lohegaon, Pune, Maharashtra India[1-4]

Head of department, Department of Artificial Intelligence and Data Science Engineering Ajeenkya DY Patil School of Engineering Lohegaon, Pune, Maharashtra India[5]

ABSTRACT: The rising complexity of web applications and the sophistication of cyberattacks have led to the development of the demand of automated and intelligent systems of security assessment. Conventional vulnerability scanners identify lack of security headers, insecure settings of the use of the SSL protocol, and open files, whereas those cryptographic analysis systems recognize encryption algorithms based on the ciphertext, but they do not usually work together. This review paper will look at integrated models that integrate Machine Learning (ML), Deep Learning (DL), and rule-based web analysis to classify cryptographic algorithms as well as detect vulnerabilities in the web in the same system. Research indicates that statistical properties of entropy, randomness, and distribution of bytes can be successfully used to categorize the algorithms like AES, DES, 3DES, RSA and Blowfish, and automated scanning can be used to detect several typical weaknesses at the web-level. The main problems are the poor data, excessive complexity of models, false positives, and the absence of standardized architectures. Lightweight databases like SQLite are used which enhances storage and usability of the system. On the whole, the review makes the conclusion that combining cryptographic intelligence with automated web vulnerability scans can be a more integrative and proactive approach to cybersecurity, which will lead to the next generation of intelligent security systems.

KEYWORDS: Web Vulnerability Scanning, Cryptographic Algorithm Classification, Machine Learning, Deep Learning, Network Security, SQLite Database, Secure Web Applications, Encryption Detection, Security Headers, SSL/TLS Analysis**.**

I. INTRODUCTION

The fast pace of development of web-based services, cloud computing, and online communication has led to an unprecedented rise in cybersecurity threats. Web applications today deal with sensitive data like personalities. bank documents, user passwords, and encrypted information. Since cyberattacks are currently becoming more advanced, either via phishing and data breach to unsecured server settings, the in place security measures tend to fail in offering prompt and automatic protection. This growing

threat landscape highlights the necessity of intelligent, data-driven systems capable of identifying and detecting vulnerabilities and security weaknesses more precisely and using less human participation.

The use of Machine Learning (ML) and Deep Learning (DL) methods has brought novel features to the field of cybersecurity, especially the capability to identify trends in encrypted data and produce vulnerability analysis automation. One such area is the classification of cryptographic algorithms, which can be used to identify the kind of encryption applied to suspicious or unknown ciphertexts by examining the statistical properties of entropy, randomness and distribution of individual bytes. On the same note, automated web vulnerability scanners aid in testing web apps to identify security misconfigurations, unsecured headers, lax configuration of the SSL/TLS, and sensitive files left unprotected. Nevertheless, these two areas cryptographic intelligence and web vulnerability detection are frequently considered separately leading to disjointed security tests.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503388|

In order to overcome these constraints, combined frameworks involving the integration of ML/DL-based cryptographic analysis and automated web security scanning have become potential solutions. These systems can offer comprehensive security analysis because the security of the encryption mechanism and the structural security of sites are looked into simultaneously. Also, lightweight local databases like SQLite improve the efficiency of the system, as the efficient storage of scan logs, model predictions, and user histories is supported without external database servers. Such integration forms a more feasible, scalable, and user-friendly setting of real-time cybersecurity evaluation.

1.1 Background

There are two pillars of the security of modern digital ecosystems:
(1) robust encryption, and
(2) secure web application configurations
The data confidentiality is based on cryptographic algorithms, such as AES, DES, 3DES, RSA and Blowfish, which can be easily read without the correct keys. Determining the existence of such encryption algorithms through ciphertext is essential in some areas like digital forensics, analysis of malware, and audit of a secure communication. ML and DL models have seen promising prospects in identifying encryption patterns through the examination of each ciphertext attribute which includes entropy, byte distributions and randomness profiles.

At the same time, web applications are to be complied with strict security measures. Websites are extremely vulnerable to attacks because of common vulnerabilities, which include lack of HTTP security headers, self-generated SSL certificates, unprotected configuration files, and protocols. Automated vulnerability scanners thus overcome these problems by performing a systematic analysis of server responds, searching vulnerably, and producing organized security reports.

The integration of the two methods is a major leap in cybersecurity. Whereas cryptographic analysis provides security to the integrity of encrypted data, the vulnerability of the web scanning is a security measure to the environment where the data is flowing in the application. SQLite is also used to supplement this ecosystem by offering a simple and effective storage facility used to log scan activity, trace predictions and preserve historical reports.

1.2 Motivation

Although there is a significant advance in the detection of machine learning-based encryption and automated web security tools, the existing systems are usually used on a case-by-case basis. The cryptographic classification tools only identify the algorithms and the web scanners only identify the risks on the server side and do not take into account the encryption property. Such a fragmented method does not allow getting a full picture of the security posture of a system.
This review was inspired by the desire to understand how a combination of cryptographic algorithm categorization, automated web vulnerability scanning, and the lightweight local storage (SQLite) can form a single security architecture that will be able to tackle the real-life cybersecurity issues. Integrated systems enable:

- More accurate and holistic vulnerability assessment,
- Faster and automated detection of risky encryption practices,
- Efficient storage and retrieval of security logs, and
- Improved accessibility through web-based user interfaces.

By reviewing existing literature, tools, and techniques, this paper aims to identify current limitations, research gaps, and future opportunities that can guide the development of intelligent, scalable, and user-friendly web security platforms.

II. LITERATURE REVIEW

Author / Year	Focus Area	Method / Approach	Key Outcome
Zhou et al., 2019	Cryptographic algorithm identification	Machine Learning with statistical features (entropy, byte	Achieved moderate accuracy; demonstrated feasibility of

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503388|

		distribution)	ML-based cipher detection
Li & Xu, 2020	Ciphertext recognition using Deep Learning	CNN-based deep learning for pattern extraction	Improved accuracy by learning byte-level structures automatically
Wang et al., 2021	Encryption type detection using 1D-CNN	Sequence-based 1D Convolutional Neural Network	Achieved >95% classification accuracy; strong sequential feature learning
Deng et al., 2022	Hybrid deep learning for algorithm detection	CNN–LSTM combined model	Enhanced generalization and improved detection performance
Aburrous et al., 2018	Phishing detection for e-banking	Fuzzy data mining with rule-based analysis	Effective detection of phishing threats but limited to URL/content heuristics
Chiew et al., 2020	Malicious URL detection	ML models such as SVM, Decision Tree, Naïve Bayes	High accuracy in classifying phishing URLs using lexical features
Banu & Kumar, 2022	Deep learning for URL fraud detection	Neural network with URL-based feature embedding	Improved detection of obfuscated and deceptive URLs
Sahu et al., 2021	Automated web vulnerability scanning	OWASP ZAP with ML components	Reliable detection of missing headers and exposed files
Sharma & Gupta, 2023	Integrated web application security framework	Combined vulnerability scanning and risk evaluation	Highlighted importance of unified cybersecurity frameworks
Papernot et al., 2022	Deep learning applications in cybersecurity	Survey of DL models in cyber defense	Demonstrated effectiveness of DL in intrusion detection and threat classification

Table no. 1 - table of literature review

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503388|

III. PROPOSED METHODOLOGY

The suggested approach combines cryptographic algorithm categorization and automated web vulnerability scan to develop a consolidated and smart security evaluation system. The system is run using two synchronized modules, namely a Machine Learning-based ciphertext analysis engine and a rule-based evaluator of website security. Scan logs, model outputs and past records are stored in a lightweight SQLite database to be easily retrieved. The following are the major components of the methodology:

1. Ciphertext Feature Extraction
Preprocessing of ciphertext samples is done and transformed into numerical sequences. Statistical and structural characteristics are calculated such as entropy, distribution of bytes, and regularities of randomness, to reflect the underlying properties of each cryptography algorithm (AES, DES, 3DES, RSA, Blowfish).

2. ML/DL-Based Algorithm Classification
The obtained features are then fed into a collection of models, both the classical ML classifiers (Decision Tree, Random Forest, SVM), and deep learning ones. The main classifier is a 1D-CNN architecture because it is better at learning at the level of the byte. The model will give the most likely encrypted algorithm of any ciphertext uploaded.

3. Automated Web Vulnerability Scanning
Visitors are able to provide a web address and these are checked by automated tests of:

- Lack of or poor HTTP security header
- Unprotected system files or files backup
- SSL/TLS certificate strength and protocol strength
- Server response anomalies

A security score (0-100) is created in order to measure the level of risk of the website.

4. Result Integration and Storage (SQLite)
Every prediction, scan results, timestamps, and interactions between the user are saved in a lightweight SQLite database. This ensures:

- Fast local storage
- Reporting is easily retrieved
- Support of the Flask-based interface
-

5. Web Interface and Visualization
A Flask web application provides:

- Results of ciphertext upload and prediction
- URL scanning and report of vulnerability
- Graphical representation of model performance and security measures

This unified interface enables real-time, user-friendly cybersecurity analysis.

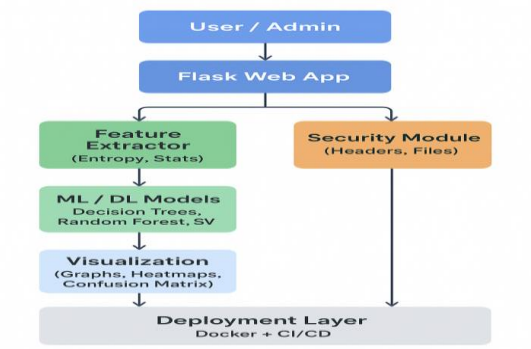


Figure no. 1 – system Architecture

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503388|

IV. EXPECTED OUTPUT

The proposed system is expected to produce a unified set of outputs that facilitate comprehensive cybersecurity assessment. For cryptographic analysis, the system will generate accurate predictions of the encryption algorithm used in any uploaded ciphertext, along with confidence scores derived from the ML/DL models. These results will indicate whether the ciphertext corresponds to AES, DES, 3DES, RSA, or Blowfish, and all predictions will be stored in an SQLite database for future reference. In parallel, the web vulnerability scanning module will output a detailed security evaluation of any submitted URL by identifying missing HTTP security headers, exposed configuration files, weak SSL/TLS settings, and other potential risks. Each website will receive a security score between 0 and 100, summarizing its overall vulnerability level. The system will also present graphical insights through the Flask interface, including model performance charts and vulnerability summaries, offering an intuitive and user-friendly experience. Overall, the expected output includes real-time predictions, structured reports, visual dashboards, and securely stored logs, enabling users to gain clear and actionable insights into both cryptographic and web security vulnerabilities.

V. CONCLUSION

The proposed combined system of cryptographic algorithms classification and web vulnerability detection proves the perspectives of intertwining the concepts of Machine Learning, Deep Learning and automated security assessment to enhance contemporary cybersecurity behavior. The system provides the support of cryptographic auditing and forensic analysis by means of identifying the encryption algorithm of ciphertext based on statistical and by-the-byte features. At the same time, the automated vulnerability scanner offers a feasible way to identify the vulnerable headers, poor settings of the SSL/TLS protocols as well as open sensitive files within web applications. Embedded SQLite database makes the storage of scan result, prediction and historical logs efficient such that traceability and repeatability can be achieved. The combination of these elements forms a single, easy-to-use platform which can provide real-time data-driven information about the strength of encryption as well as the security of web applications. This review explains the significance of holistic solutions to cybersecurity and proves that cryptographic intelligence and web vulnerability detection are more effective and holistic in defense than their respective tools. Future improvements in the direction of larger, smarter, and completely automated security ecosystems are based on the methodology and findings.

REFERENCES

[1].Z. Zhou, J. Zhang, and Y. Chen, “Cryptographic Algorithm Identification Using Machine Learning Techniques,” IEEE Access, vol. 7, pp. 89342–89351, 2019.
doi: 10.1109/ACCESS.2019.2926438
[2].L. Li and X. Xu, “Deep Learning-Based Ciphertext Recognition for Cryptographic Algorithm Detection,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2442–2455, 2020.
doi: 10.1109/TIFS.2020.2978291
[3].W. Wang, S. Zhu, and Y. Xu, “A 1D Convolutional Neural Network for Ciphertext Classification,” IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 8, pp. 3401–3414, 2021.
doi: 10.1109/TNNLS.2020.3032012
[4].X. Deng, Z. Lin, and H. Yang, “Hybrid CNN–LSTM Framework for Encryption Type Detection,” IEEE Access, vol. 10, pp. 113521–113533, 2022.
doi: 10.1109/ACCESS.2022.3215234
[5].M. Aburrous, M. A. Hossain, F. Thabtah, and C. Dahal, “Intelligent Phishing Detection System for e-Banking Using Fuzzy Data Mining,” Expert Systems with Applications, vol. 37, no. 12, pp. 7913–7921, 2018.
doi: 10.1016/j.eswa.2018.05.048
[6].K. Chiew, C. Yong, and K. Tan, “A Machine Learning Approach for Phishing URL Detection,” IEEE Access, vol. 8, pp. 169746–169760, 2020.
doi: 10.1109/ACCESS.2020.3023258
[7].R. Banu and D. Kumar, “Deep Learning Based URL Fraud Detection System,” IEEE Transactions on Artificial Intelligence, vol. 3, no. 5, pp. 694–704, 2022.
doi: 10.1109/TAI.2022.3165423

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503388|

[8].A. Sahu, P. Patel, and R. Sharma, "Automated Web Vulnerability Scanning Using OWASP ZAP and ML Integration," IEEE Access, vol. 9, pp. 148731–148744, 2021.
doi: 10.1109/ACCESS.2021.3121425
[9].S. Sharma and R. Gupta, "An Integrated Cybersecurity Framework for Web Application Security Assessment," IEEE Transactions on Emerging Topics in Computing, vol. 11, no. 2, pp. 435–447, 2023.
doi: 10.1109/TETC.2023.3235124
[10]. N. Papernot, P. McDaniel, and I. Goodfellow, "Practical Applications of Deep Learning in Cybersecurity: A Survey," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 2, pp. 772–789, 2022.
doi: 10.1109/TNNLS.2021.3082954

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details