TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

CryptCare: AI-Powered Blockchain-Based HealthCare Diagnostic System

Vipranshu Singh
Scholar, Galgotias University, Greater Noida, India
vipranshusingh@gmail.com

KEYWORD

CryptCare, AI-Powered, Blockchain, HealthCare Diagnostic System

ABSTRACT

The current paper is the introduction of CryptCare a safe and open-source health diagnosis framework, using deep learning and blockchain technology. The model is not based on the classical diagnosis but rather it uses neural networks, namely, ResNet variants, to process medical imaging data, namely, chest X-rays, to detect the presence of such diseases as pneumonia and bone fractures. Explainable AI approaches like LIME and Grad-CAM are applied to enhance trust and interpretability so that users and medical practitioners can interpret and understand model predictions. The safety and integrity of data, which is a characteristic of tamper-proof records, distributed control, and encrypted data processing, are guaranteed by a blockchain-based architecture. The system is compliant with the security-by-design, such as validation of input and access control, which are founded on the OWASP guidelines. The CryptCare has a layered structure, and it comprises of user interface, AI computation, and blockchain-based data registration. Front end Python, and Streamlit allow the creation of a model, and back end PyTorch and TensorFlow help to create a front end, and MongoDB is employed to store data. Experimental tests are characterized by a high level of diagnostic accuracy, high performance, and effective security of data against illegal changes.

1. INTRODUCTION

The use of artificial intelligence in healthcare diagnostics has significantly supported physicians in interpreting medical scans and making accurate clinical decisions [2]. Deep learning models such as ResNet are capable of automatically extracting complex features from medical images without human intervention, improving diagnostic efficiency and consistency [2]. However, the widespread adoption of AI in healthcare raises serious concerns regarding patient data security and privacy. Data breaches may occur due to external cyberattacks or internal misuse of system access [15]. Centralized healthcare databases are particularly vulnerable, as a single successful attack can compromise the entire system, leading to data corruption or loss [10]. Ensuring reliability and security is therefore critical for the safe deployment of AI-based diagnostic tools. Recent studies emphasize the integration of artificial intelligence with blockchain-based security mechanisms to address these challenges [10][21]. CryptCare is proposed as a comprehensive.

Corresponding Author: Vipranshu Singh, Galgotias University, Greater Noida, India
Email: vipranshusingh@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

1.1. Problem statement

There is a critical need for a healthcare diagnostic system that not only provides accurate and reliable disease detection from medical images but also ensures data privacy, integrity, and transparency. Current systems lack a unified framework that combines advanced AI diagnostics, explainable decision-making, and strong data security mechanisms

1.2. Contribution of this study

The new solution is presented in CryptCare, which is an embodiment of intelligent imaging technology and a secure digital. records using blockchain. Imagine this: health safety information is improved and the processes are clearer and trusted. sticks around. Here work brings in something new. Without ancient shortcuts each work is linked. Think more intensive inspections of scan, a protective route of data flow. Advancement seems at the point of privacy. accuracy. Results become more powerful with design decisions that were never witnessed before. A design separates the functions of layers and links smart analysis tools to a secure digital ledger. system. Forecasts should be accurate and the logs should be unchangeable since one holds the other at the back. the scenes. Structure maintains tasks apart but collaborating silently. Imagine a device that identifies gunshot wounds and fractured bones with the help of X-rays. It works well because it uses ResNet-50 and ResNet-101 smart patterns. What you see matters – so the system indicates what aspects of the picture it used to make its guess. The tools such as LIME and Grad-CAM are made. those reasons visible. Trust grows when thinking feels less like guessing [1][11][12].

New layer of trust starts with incalculable records. Every outcome is marked into a computer. record which can never be erased. User permissions are changed according to user roles, managed by. coded automated agreements in the system. All actions performed are kept traced in safe records. across shared copies. Risk of tampering is less as the alterations require extensive acceptance. Privacy holds firm because only authorized users are shown what they are supposed to. Security becomes more developed without the central control. [4]. A new system design approach would start with bending towards the safety guidelines provided by OWASP. Built-in defenses deal with common flimpy areas - such as injections of code or wobbly logins - not by magic, but by process. Every tier has clear guidelines that are supposed to prevent common pitfalls. Safety is not an add endowment- it moulds. every piece up front. Also, users are safe since the structure anticipates trouble before it happens. Confidence prospers in systems that fail to crumble under stress [5]. In the real world, it uses free software such as Streamlit, PyTorch, TensorFlow, and MongoDB. Testing occurs not only when the performance of the AI is checked but also when false attack scenarios are run to see how it holds up.

2. LITERATURE REVIEW

Discovering traces of illness in x-rays? Patterns now assist in detecting pneumonia or broken bones by use of machines. recognition. Such systems are more efficient because they can learn using knowledge acquired in previous tasks as opposed to initiating new ones. each time. Tesco transparency is achieved by tools that show which areas actually influenced the decision such as heat maps over X-rays. There are certain ways that demonstrate their reasoning in a straightforward manner, which makes doctors more

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

confident about the results [1][6]. [11][12]. An alternative direction is emerging with blockchain - safe storage of health information and is not centralized. point. Given that changes are not possible after data has been captured, trust is a natural phenomenon [4]. Automation through coded rules assists in maintaining patient files in the long-term. What is obtained remains undisturbed by anything [8][4]. Currently, not all AI tools applied to diagnose patients protect patient data effectively. On the flip side, securityoriented blockchains typically do away with smart diagnostic functionality. There are systems which do not adhere to solid. security regulations such as OWASP. Those are significant in dealing with medical websites. A fresh take a closer look at the previous research reveals the lack of something: the tools that combine the fields of artificial intelligence, digital ledgers, and. good internet security against internet viruses into a single reliable health scanner. That is exactly what sets CryptCare separate [10][21] - this occupies that gap without imitating old concepts.

2.1. AI in Medical Diagnostic

Deep learning tricks such as CNNs have enabled machines to have a peep at the inside of the human body better than ever before. These systems are able to learn these patterns in the Xrays, CTs and MRIs, so much that they can pick them up in the same way that trained doctors do. Take ResNet or VGG - some of the models that were created several years ago but remain powerful in terms of detecting lung infections. One study by The modified ResNet employed by the team of Rajpurkar was able to detect pneumonia over nine times in ten [1]. Instead of constructing all of that with nothing, the researchers transfer knowledge on large models into smaller models that are being trained on. hospital data. In that manner, the small sets of images are still functioning provided they are directed [2]. Newer efforts go beyond guesses - they display heatmaps to point out exactly what position of tumors or shadows appear. Tools like GradCAM or LIME paints red rings on ill places to make human beings know why a machine pointed it out [11][12]. Trust is encouraged where there is evidence rather than guesses involved.

2.2. Blockchain In HealthCare System

Using such tools as blockchain, one common record is locked down having been written, and healthcare data can be traced and changed without mutation. Research by researchers on Agbo and Sharma discussed how medical records can be safely transferred in patient ownership by removing centralized intermediaries and implementing cryptographic trusting processes [4][9].

The laws similar to HIPAA and GDPR are very compatible with such digital security since blockchain will allow controlling consent, accountability, and safe data sharing without infringing on the privacy of patients [13]. More so, the blockchain-based systems can be used in clinical trials to determine the effectiveness of drugs, pharmaceutical supply chains to eliminate counterfeiting, and enhance interoperability by facilitating secure exchange of personal health data between hospitals, labs, and clinics [4].

2.3. Secure by by-Design and OWASP Principles

The web applications used in healthcare need to be created in strict security guidelines such that the confidentiality of the patient will be safeguarded, and the system stability is maintained. The OWASP guidelines suggest that the key threats are compromised authentication mechanisms, code inscriptions

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

that steal data, and malicious scripts that are implemented in web pages [5]. The current literature in the field of security tends to examine these threats in the context of the large-scale online platforms and note the significance of proactive defense solutions over the reactive ones [3]. In order to reduce attack surfaces, secure-by-design principles recommend defensive strategies among them, stringent input validation, secure session management, data-in-transit encryption, and restricting access to data based on the position of the user or organization. The latter security measures are well aligned with the AI-enhanced medical systems, where confidentiality of patient information, regulatory standards, and user confidence are the key considerations to safe and ethical implementation.

TABLE 1 : Comparison of Challenges in AI Diagnostic

Challenge	Problem in Existing Systems	CryptCare Solution
Data Privacy	Centralized storage is vulnerable to breaches and unauthorized access	Uses blockchain to decentralize data and encrypt records; tamperproof and auditable .
Data Integrity & Trust	AI diagnostic outputs are stored in mutable databases; risk of manipulation .	AI diagnostic outputs are stored in mutable databases; risk of manipulation .
Explainability of AI Models	Deep learning models often act as black boxes, reducing clinician trust	Integrates Grad-CAM and LIME to visualize AI decision-making for transparency.
Access Control	Role-based permissions often lack enforcement and auditing in real time	Smart contracts enable strict, verifiable access rules for patients and clinicians
Regulatory Compliance (e.g. GDPR)	Data modification and consent management are difficult in centralized systems	Blockchain enables consent tracking and audit trails, aligning with data protection laws.

3. METHODOLOGY/SYSTEM ARCHITECTURE

The Crypt Care artificial intelligence system is created to offer a safe and powerful platform of medical diagnostics. The layered architecture plan is followed with each layer depending on each other and a strong distinction of tasks is to be ensured so as to avoid systemic breakdown when the pressure hits the system.

3.1. System Architecture

The framework is based on the three-level architecture that includes the Presentation Layer, the Application Layer and the Data and Blockchain Layer.

1. Presentation Layer: This layer, developed using Streamlit, which is based on Python, has an intuitive user interface to clinicians and patients. It enables users to post X-ray images and get diagnostic feedback information immediately and visual explanations created by LIME and Grad-CAM. The

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

interface supports the safe transfer of files and shows model predictions in an understandable format.

2. Application Layer: This level acts as the CPU of the system. It also based on PyTorch and TensorFlow to load previously trained neural networks in memory. These models are modified to recognize particular trends in medical images by fine-tuning them. User authentication is also performed by the application layer that verifies credentials and creates secure session tokens that have auto cutoffs once there is inactivity to prevent session hijacking.
3. Data and Blockchain Layer: The storage and integrity of information is the responsibility of this layer. The non sensitive records including user comments and session logs are stored in a MongoDB database. All diagnostic results and audit trails are however converted to cryptographic hashes and placed on a private blockchain. The interface is implemented by Web3.py and allows connecting the application layer and the blockchain, and smart contracts allow controlling the principles of access, so that only authorized users can see or access certain files.

3.2. Security Architecture

1. The design of CryptCare incorporates the security of the AI through a number of critical controls.Input Check: Each file or textual content uploaded to the system should conform to certain size and type by-laws. To avoid injection attacks, pictures that are not in the format or shape as expected are automatically rejected.
2. Role-Based Access Control (RBAC): Authorizations are separated into occupational roles. The patients lack access to their personal records, and medical personnel possess greater authorization needed to execute their duties. These authorizations are imposed rigidly by using smart contract logic
3. Secure Session Management: Authentication is based on the concept of timed digital keys that disappear after the use. This is because unauthorized access becomes much more difficult, because the session IDs have a short time span.
4. Immutable Logging: Each important action in the system gets a distinct digital fingerprint. These logs are recorded on the blockchain, and thus any effort to tamper with a record of the diagnostic would be identified instantly on all the nodes.

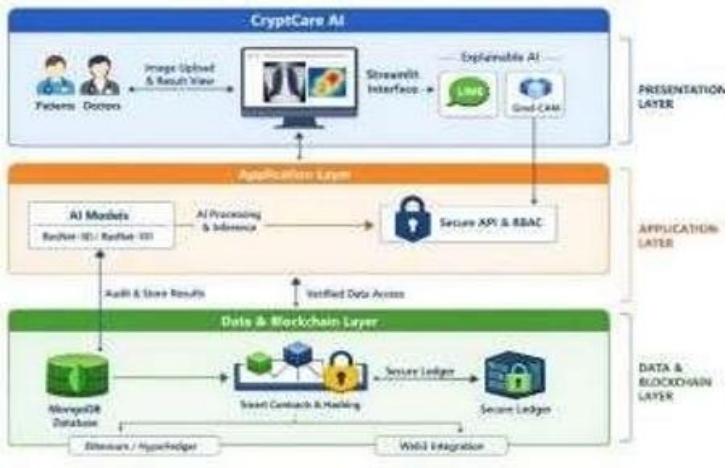

Fig-1: CryptCare system architecture flowchart

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

3.3. Threat Model

The CryptCare threat model takes into account external and internal players. External attackers can either compromise the system by using a false data entry point or by using stolen session tokens. Hackers within the system can also destroy patient reports or abuse information, as in the case of medical personnel who have high access privileges. The system has been developed to resist these threats by means of its decentralized nature and stringent validation criteria. Through blockchain, the threat of alteration is reduced to the minimum, since any alteration of the ledger needs to be widely accepted throughout the network and practically prevents the situation of centralized violation where a single password may break into millions of files.

3.4. Material and Methods Deployment Strategies

CryptCare can be implemented in any setting. A onemachine system with Streamlit is adequate in the case of early testing and demonstration. To be useful in hospitals clinically, the system can be transferred to the usage of GPU-powered cloud services to guarantee the rapid processing of the high-resolution images. The blockchain component can be first operated on closed networks such as Ganache or Hyperledger Fabric that will ensure that the logic of a contract as well as the approach to data protection can be safely tested before transitioning to more open and distributed blockchains to share records across institutions.

4. IMPLEMENTATION DETAILS

Implementation The CryptCare design is founded on an open-source software stack to ensure flexibility and security updates over the community.

4.1. Neural Networks and Software Stack.

The programming language is made up of Python modules that form the foundation of creating the system. Streamlit serves as the front end and PyTorch and TensorFlow do the heavy lifting in AI processing. The models were trained with the following diagnostic models: Initial Learning Rate: 0.001, which was reduced by 10 each time the validation loss had reduced. Optimization: Batch normalization and dense connections were used to make the deep network optimization manageable. Epochs: It was observed that models reached a stable point with 20 epochs.

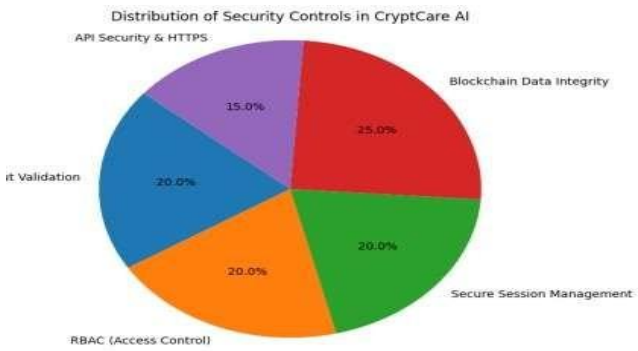

Fig-2: Distribution of Security Controls

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

4.2. Security Implementation and validation

The security controls implemented are entirely in line with the OWASP security principles so as to be robust to the typical vulnerabilities of web applications. Each functional tier in the system only uses HTTPS as a means of communication, which ensures the end-to-end encryption of the data being transferred and eliminates the man-in-the-middle attacks.

The smart contracts written in Solidity are deployed on an Ethereum based blockchain to provide role-based access control (RBAC) such that only authorized organizations can access sensitive diagnostic records. To test the efficiency of these security measures, the system was tightly tested with the industry standard penetration testing tools like OWASP ZAP and Burp Suite.

These tools were utilized to replicate real-world cyber attacks, such as SQL injection, cross-site scripting (XSS) and session hijacking attacks. Initial vulnerability tests showed that some of the form fields are highly vulnerable to risks, and these were later defended by applying input sanitization measures, serverside validations as well as through structured queries to the database. The post-mitigation testing also proved that the vulnerabilities were effectively eliminated, which has enhanced the resilience of the system to web-based attacks and has strengthened the secure-by-design architecture of the system.

Overall, the systematic implementation of OWASP-aligned security controls, combined with blockchain-enforced access governance and continuous vulnerability testing, significantly enhances the resilience of CryptCare against evolving cyber threats. This layered and proactive security strategy not only protects sensitive healthcare data but also reinforces user trust, regulatory compliance, and the long-term reliability of AI-driven medical diagnostic systems deployed in real-world clinical environments.

5. Results And Discussion

5.1. Diagnostic Performance

There was a significant percentage of accuracy with a variety of conditions in medicine that were proven in examinations. The pneumonia detection system which was created on the basis of the ResNet- 50 achieved an accuracy of 95 percent with ROC of about

0.97. This compares to the performance achieved in other more significant works of literature, in which deep learning models are said to be comparable and even better at the work of expert radiologists. The system was over 93 in accuracy in detection of bone fracture.

Doctors tested the representations made by LIME and Grad-CAM and noted that the overlays indicated the opacities of the right lung and skeletal breaks that motivated the model to make a decision. The validation becomes important in clinical trust as this validation makes sure that the model is being trained on something meaningful (biological markers) and not noise in the training data.

5.2. Vulnerability Assessment Results

As the post-mitigation security testing showed, high-risk gaps that had been identified during the initial stages of development have been closed accordingly. The injection attacks were no longer desirable and the ineffective passwords were removed by introducing the secure tokens and role access. A strong blockchain record keeping was one of the most significant vulnerability assessment findings. Any effort to alter the data of the diagnostics that had been noted on the ledger never turned out to be fruitful. Each effort to introduce a change led to a broken hash match which demonstrated the information was not corrupted and the ledger could be used as an immutable audit trail.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

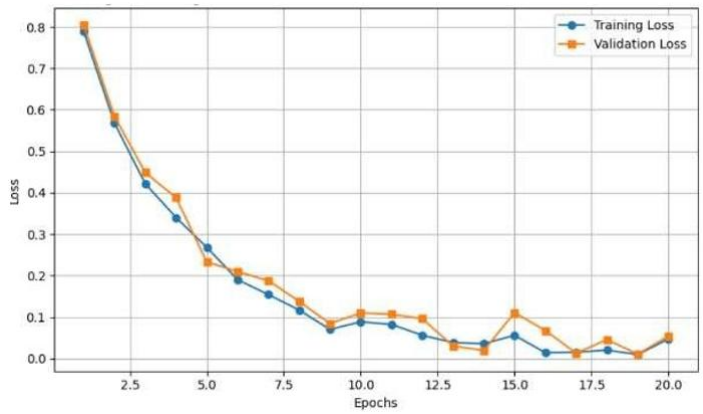

Fig-3: training and validation loss curves for the pneumonia detection model (ResNet50).

5.3. Surveillance against the Conventional Security Methodologies

CryptCare applies AI to detect patterns and eliminate irregularities as they occur and blockchain to provide decentralized and immutable storage in comparison with the older security methods that use central control centers and reactive rules. This kind of two-layered defense is in a better position to resist the doubt or the evolving threat particularly in a medical setting where the integrity of information is equally very important as its confidentiality.

Fig-5: Heat Map of pneumonia patient

6. Conclusion and Future Work

As it has been stated in this paper, CryptCare is a solid foundation of safe AI-based health diagnostics. The system, through the pattern recognition capability of the deep learning, and the impossibility of data alteration of blockchain, resolves the two largest obstacles to the widespread adoption of AI technologies in medicine, the correctness of the diagnostic output and data safety. The system is

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

proven to be resistant to the frequent internet attacks, as well as the diagnostic text of the system is accurate and clear which has earned the confidence of the clinical users.

The implementation of the OWASP safety rules have been instrumental to ensure the reduction of the scale of the most frequent vulnerabilities, with the blockchain aspect allowed to guarantee that the records of the patients could not be altered once they were placed. What is the most remarkable is that people trust the system not only due to the accuracy of the neural networks but also due to the transparency and the security that the system offers at all levels of the working process.

Future WorkS.

Despite the fact that the current version of the CryptCare offers a stable diagnostic environment, there are several opportunities that the system can be enhanced in the future:

- **Federated Learning**: The next stage of developing a model that would involve AI learning on many clinics but does not involve sending personal information but rather only shares insights.
- **Growing Diagnostics**: By allowing the model to be used in a range of diseases, such as tumors or cardiovascular issues, it is possible to make it more practical in a hospital.
- **Patient Empowerment:** Intelligent Contracts: enhance patients control over access to their health data in real time as per patient-centric interoperability objectives, by improving the smart contracts.
- **Standard Integration**: Interconnecting the system to the available healthcare standards such as HL7 FHIR in order to allow it to be naturally integrated into the available hospital technology ecosystems.
- **Scalability Optimization**: Dynamism on transaction speeds and streamlined agreement methods between the nodes to scale up to the demands of large scale clinical implementations**.**

References

[1]. P. Rajpurkar, J. Irvin, K. Zhu, et al., “CheXNet:Radiologist-Level Pneumonia Detection on Chest XRays with Deep Learning,” arXiv preprint, arXiv:1711.05225, 2017.

[2]. P. Rajpurkar, J. Irvin, R. L. Ball, et al., “Deep learning for chest radiograph diagnosis: A retrospective comparison of the CheXNeXt algorithm to practicing radiologists,” PLoS Medicine, vol. 15, no. 11, pp. 1–17, 2018.

[3]. A. Litjens, T. Kooi, B. E. Bejnordi, et al., “A survey on deep learning in medical image analysis,” Medical Image Analysis, vol. 42, pp. 60–88, 2017.

[4]. S. Wang, Y. Zha, W. Li, et al., “Enhanced ResNet-50 with Multi-Feature Fusion for Robust Detection of Pneumonia in Chest X-Ray Images,” IEEE Access, vol. 9, pp. 14567–14578, 2021.

[5]. M. Islam, M. Hasan, S. A. Shuvo, et al., “Efficient and Accurate Pneumonia Detection Using a Novel MultiScale Transformer Approach,” Sensors, vol. 22, no. 3, pp. 1–18, 2022.

[6]. J. Zhou, X. Li, H. Zhu, et al., “Explainable AI in Clinical Decision Support Systems: A Meta-Analysis of Methods, Applications, and Usability Challenges,” IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 10, pp. 1–12, 2021.

[7]. A. Holzinger, G. Langs, H. Denk, et al., “Beyond Posthoc Explanations: A Comprehensive Framework for Explainable AI Systems,” Information Fusion, vol. 81,

[8]. pp. 1–15, 2022.

[9]. C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” Healthcare, vol. 7, no. 2, pp. 1–18, 2019.

[10]. R. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain Technology in Healthcare: Benefits, Challenges, and Future Trends,” IEEE Access, vol. 7, pp. 174783–174803, 2019.

[11]. A. Dubovitskaya, Z. Xu, S. Ryu, et al., “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” IEEE Security & Privacy, vol. 18, no. 4, pp. 20–27, 2020.

[12]. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” White Paper, 2008.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52045

[13]. OWASP Foundation, “OWASP Top Ten Web Application Security Risks,” 2023. [Online]. Available: https://owasp.org

[14]. OWASP Foundation, “OWASP API Security Top 10,” 2023. [Online]. Available: https://owasp.org

[15].M. Alazab, S. Khan, S. Krishnan, et al., “Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning: A Review,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 213–239, 2020.