International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 10 Issue 7 July - 2026, Pages: 38-48

A CLIPS-Based Knowledge-Based Expert System for Cybersecurity Incident Diagnosis and Response

Muhammad Isleem, Taha Al-Jaro, Samy S. Abu-Naser2

Department of Information Technology,
Faculty of Engineering and Information Technology,
Al-Azhar University, Gaza, Palestine

abunaser@alazhar.edu.ps

***Abstract**: Cybersecurity incident triage requires analysts to combine heterogeneous evidence from endpoint, network, identity, email, and application sources under severe time pressure. This paper presents the design and implementation of a knowledge-based expert system that supports the diagnosis of common cybersecurity incidents and recommends immediate response actions. The prototype is implemented in CLIPS using production rules, structured facts, candidate scoring, conflict resolution, and an explanation-oriented output. Its knowledge base covers eight incident classes: ransomware, phishing compromise, brute-force attack, distributed denial-of-service, malware infection, data exfiltration, insider threat, and web application attack. Indicators are represented as facts, while rules infer one or more candidate incidents. A final rule selects the highest-scoring candidate and returns the incident type, severity, supporting evidence, and a prioritized response recommendation. The implementation contains 19 production rules and was evaluated through 12 controlled scenarios, including complete, partial, competing, and insufficient-evidence cases. The system produced the expected result in 12 of 12 scenarios. Across 360 repeated timing runs, mean inference time was 0.036 ms and maximum inference time was 0.119 ms in the test environment. These results demonstrate functional correctness and very low rule-engine overhead for the designed cases, while the study also emphasizes that the evaluation is a prototype verification rather than a real-world accuracy benchmark. The proposed system illustrates how transparent, maintainable, and auditable rule-based reasoning can complement security analysts and provide explainable decision support during early incident triage.*

Keywords: knowledge-based systems; expert systems; CLIPS; cybersecurity; incident response; rule-based reasoning; explainable decision support.

1. INTRODUCTION

Cybersecurity operations centers receive a continuous stream of alerts from multiple tools. The analyst must decide whether an event is benign, suspicious, or part of a confirmed incident, and must also select an appropriate containment action. This task is difficult because the evidence is distributed across different sources, the same indicator may appear in several incident types, and the consequences of delayed or inconsistent decisions can be significant. NIST incident-response guidance therefore emphasizes preparation, detection, response, and recovery as integrated risk-management activities rather than isolated technical steps [1], [2].

Decision support is especially valuable during initial triage. Research involving cybersecurity threat and incident managers found that practitioners must balance detailed technical investigation with a broader operational picture, and that structured decision aids can support more consistent assessment and response [6]. A knowledge-based system is appropriate for this setting when the reasoning can be expressed as explicit relationships between observable indicators, incident categories, severity levels, and response recommendations.

Rule-based expert systems differ from statistical classifiers because their knowledge is encoded directly as interpretable production rules. In CLIPS, facts are matched against the left-hand side of rules, and the inference engine executes the actions of activated rules [4]. This approach offers transparency: the system can report the evidence that triggered a conclusion and the rule score used to prioritize competing candidates. Such transparency is important in security operations, where analysts need to understand and validate a recommendation before applying potentially disruptive containment actions.

The objective of this research is to design and implement a CLIPS-based expert system for early cybersecurity incident diagnosis and response. The system focuses on eight frequently encountered categories and is intended as an educational decision-support prototype, not as an autonomous security-control platform. Its main contributions are: (1) a structured representation of cybersecurity indicators as CLIPS facts; (2) a production-rule knowledge base containing complete and partial evidence patterns; (3) a score-based conflict-resolution mechanism for competing diagnoses; (4) an explanation-oriented output that presents incident type, severity, evidence, and response action; and (5) a controlled functional evaluation using normal, ambiguous, and insufficient-evidence scenarios.

2. MATERIALS AND METHODS

2.1 Development Environment

The expert system was written in CLIPS 6.4-compatible syntax. The knowledge base is stored in a standalone .clp file containing deftemplate and defrule constructs. For repeatable evaluation, the CLIPS engine was invoked through clipspy 1.0.6, a Python interface to the CLIPS engine. The automated test harness reset the environment, asserted scenario indicators, executed the inference cycle, extracted the resulting diagnosis fact, and compared it with the expected outcome. This arrangement does not change the rule semantics; it only automates repeated execution and measurement.

2.2 Knowledge Acquisition and Scope

The domain knowledge was derived from established incident-response concepts, common security-operations practices, NIST guidance, and the MITRE ATT&CK vocabulary. NIST CSF 2.0 provides a high-level structure for governing, identifying, protecting, detecting, responding, and recovering from cybersecurity risk [2]. MITRE ATT&CK organizes adversary behavior into tactics and techniques and provides a shared language for describing attack objectives and observable activity [3]. The prototype converts selected operational indicators into a compact rule base suitable for a course project.

The scope is intentionally limited to early triage. The system does not parse raw packet captures, execute malware, inspect user content, or perform automated containment. Instead, it accepts already-observed indicators such as “files encrypted,” “credentials entered,” “traffic spike,” or “unusual destination.” A value of yes indicates that an analyst or an upstream security tool has confirmed the indicator. This separation keeps the knowledge-based reasoning explicit and avoids presenting the prototype as a replacement for endpoint detection, network monitoring, digital forensics, or professional judgment.

2.3 System Architecture

Figure 1 shows the architecture. Evidence from an analyst or monitoring source is converted into indicator facts and placed in working memory. The CLIPS inference engine matches those facts against production rules stored in the knowledge base. Activated rules assert candidate incidents with a score, severity, supporting evidence, and a response recommendation. A final selection rule chooses the candidate with the greatest score, while a fallback rule returns an undetermined result when no candidate has sufficient evidence.

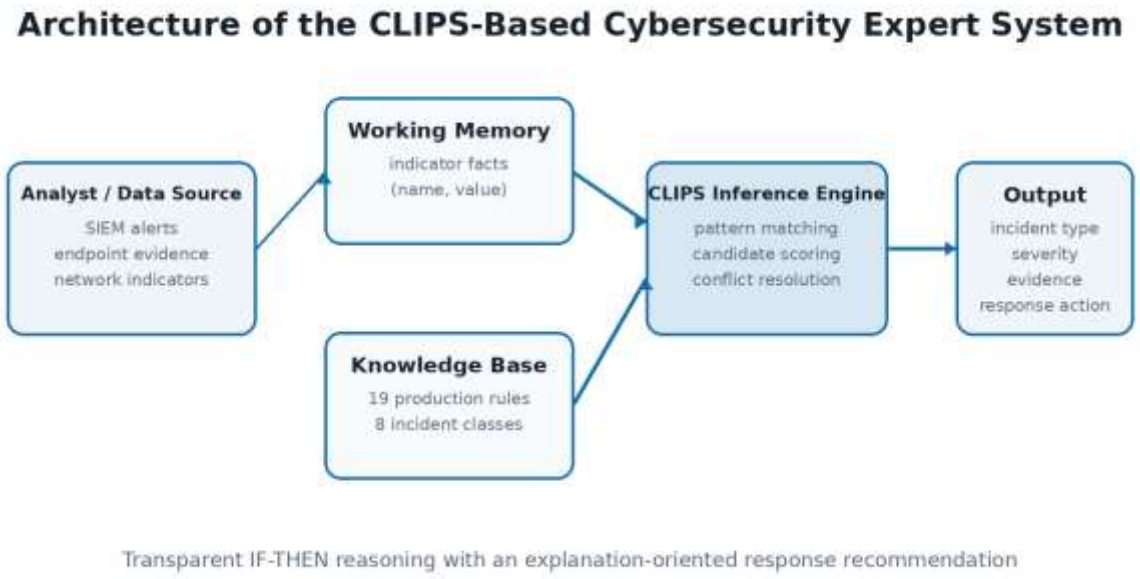

Figure 1. Architecture of the proposed CLIPS-based cybersecurity expert system.

2.4 Incident Classes and Indicators

Table 1. Incident classes represented in the knowledge base

Incident class	Core indicators	Severity	Primary response direction
Ransomware	Encrypted files; ransom note; changed extensions	Critical	Isolate host, protect shares, preserve evidence, verify backups
Phishing compromise	Suspicious email; clicked link; credentials entered	High	Reset credentials, revoke sessions, inspect mailbox, enforce MFA
Brute-force attack	High failed logins; same account targeted; many sources	High	Lock account, rate-limit sources, review successful access
Distributed denial-of-service	Traffic spike; service unavailable; distributed sources	Critical	Activate mitigation, filter upstream, preserve flow records
Malware infection	Unknown process; antivirus alert; persistence change	High	Isolate endpoint, collect evidence, quarantine or reimage
Data exfiltration	High outbound data; unusual destination; sensitive files accessed	Critical	Contain egress, revoke access, assess affected data
Insider threat	Privileged abuse; unusual hours; mass file access	High	Restrict account, preserve audits, coordinate escalation
Web application attack	Server errors; SQL patterns; unauthorized database query	Critical	Block requests, isolate application, patch and rotate credentials

2.5 Inference Workflow

The inference workflow contains four stages. First, observed indicators are asserted as structured facts. Second, complete-evidence and partial-evidence rules create candidate incidents. Complete patterns receive higher scores than partial patterns. Third, the conflict-resolution rule selects a candidate for which no higher-scoring candidate exists. Finally, the selected diagnosis is printed together with the evidence and a response recommendation. If no candidate exists, an insufficient-evidence rule advises the analyst to collect additional endpoint, network, identity, email, and application data.

The numeric score is a deterministic priority value and must not be interpreted as a statistical probability. Its purpose is to order candidates when several rules are activated. For example, confirmed phishing evidence receives a score of 95, while a partial brute-force pattern receives 64. If both patterns are present, phishing is selected because it has the higher rule score. A production deployment would require expert review of these values, uncertainty management, and calibration against real cases.

2.6 Safety and Operational Boundaries

The system provides recommendations rather than executing actions. Security containment can affect business availability and legal obligations, so every output is intended for review by an authorized analyst. The knowledge base avoids offensive instructions and focuses on defensive actions such as isolation, credential revocation, log preservation, patching, and escalation. Evidence preservation is included because premature cleanup can destroy information required for investigation and reporting.

3. LITERATURE REVIEW

3.1 Knowledge-Based and Rule-Based Security Systems

CLIPS was developed as a rule-based programming language for expert systems and other applications in which heuristic knowledge is easier to express and maintain than a purely algorithmic solution [4]. Its production-system model separates domain knowledge from execution control: developers specify facts and rules, while the inference engine determines which rules are applicable. This separation is valuable for cybersecurity because incident-handling knowledge changes over time and can be updated without redesigning the entire application.

Rule-based detection is closely related to signature-based or misuse detection. Khraisat et al. classify intrusion-detection approaches into signature-based and anomaly-based families and describe signature-based systems as knowledge-based mechanisms that match current activity against known attack patterns [7]. The strength of this method is interpretability and effectiveness for known behaviors; its limitation is reduced ability to detect genuinely novel attacks. The present work does not attempt to replace anomaly detection. It demonstrates how explicit expert knowledge can support interpretation and initial response after indicators have already been observed.

3.2 Decision Support for Incident Response

Incident response requires more than recognizing an attack label. Analysts must investigate context, contain damage, preserve evidence, communicate with stakeholders, eradicate the cause, and support recovery. NIST SP 800-61 Rev. 3 integrates incident-response considerations with cybersecurity risk management and CSF 2.0 [1]. This orientation informed the response recommendations in the knowledge base: each diagnosis includes immediate containment and investigation actions rather than only naming the incident.

Van der Kleij et al. studied decision support for cybersecurity threat and incident managers and found that these professionals must simultaneously consider detailed evidence and the larger operational context [6]. Their findings support the use of structured decision aids that provide cues and critical-thinking steps. The expert system proposed here operationalizes a narrow portion of that idea by linking evidence patterns to transparent diagnoses and recommended actions.

3.3 Explainability and Human Oversight

Modern intrusion-detection research increasingly uses machine-learning and deep-learning models; however, opaque predictions can reduce analyst trust. Neupane et al. identify explanation as a major requirement for intrusion-detection systems used by security operations personnel and discuss the need for human-centered explanation design [8]. Capuano et al. similarly review explainable artificial intelligence in cybersecurity and emphasize the challenge of making complex models understandable to decision makers [9].

A rule-based system is a white-box alternative for a constrained domain. Its reasoning can be traced directly to the matched facts and the rule that fired. This interpretability does not automatically guarantee correctness, because the rules may be incomplete or poorly designed, but it makes validation and revision easier. The proposed system therefore reports the supporting indicators and score, and it returns an undetermined result rather than forcing a classification when evidence is insufficient.

3.4 Research Gap

Many cybersecurity studies focus on large-scale detection performance, while educational expert-system projects often stop at a simple one-rule/one-diagnosis mapping. The gap addressed in this paper is the design of a compact but structured cybersecurity expert system that handles full evidence, partial evidence, competing incident candidates, and insufficient evidence. The score-based selection and explanation output provide a clearer demonstration of knowledge representation and inference than a flat menu-based diagnostic program.

4. KNOWLEDGE REPRESENTATION

4.1 Fact Representation

Observed evidence is represented using the indicator template. Each fact contains a symbolic name and a three-valued status: yes, no, or unknown. The implemented test scenarios assert only confirmed yes facts; the remaining indicators are absent. This open-world design prevents the system from treating a missing fact as a confirmed negative observation.

```
(deftemplate indicator
   (slot name (type SYMBOL))
   (slot value (type SYMBOL)
         (allowed-symbols yes no unknown)))
```

4.2 Candidate and Diagnosis Templates

Rules do not immediately print a conclusion. Instead, they assert candidate facts. A candidate contains an incident type, a priority score, a severity label, the evidence that supported the rule, and a response recommendation. The diagnosis template has the same fields and represents the final selected result. This intermediate representation enables conflict resolution when several incident patterns are present.

```
(deftemplate candidate
   (slot type (type SYMBOL))
   (slot score (type INTEGER))
   (slot severity (type SYMBOL))
   (multislot evidence)
   (slot recommendation (type STRING)))
```

4.3 Production Rules

Each incident class has a complete-evidence rule and, where appropriate, a partial-evidence rule. The ransomware rule shown below fires only when encrypted files, a ransom note, and changed file extensions are present. The not condition prevents duplicate candidates of the same type. The rule then asserts a critical candidate with a score of 100 and a response recommendation.

```
(defrule ransomware-full
   (declare (salience 50))
   (indicator (name files-encrypted) (value yes))
   (indicator (name ransom-note) (value yes))
   (indicator (name extensions-changed) (value yes))
   (not (candidate (type ransomware)))
   =>
   (assert (candidate
      (type ransomware)
      (score 100)
      (severity critical)
      (evidence files-encrypted ransom-note extensions-changed)
      (recommendation
       "Immediately isolate the host, disable shared drives,
        preserve forensic evidence, activate the incident-response
        plan, and recover only from verified clean backups."))))
```

4.4 Conflict Resolution

Several candidate facts may be generated from a single scenario. For example, stolen credentials may produce phishing evidence and later failed-login activity. The final selection rule matches a candidate only when no other candidate has a greater score. Because the rule also requires that no diagnosis already exists, only one final result is asserted. Salience values ensure that candidate-generation rules execute before selection and that the output rule executes last.

```
(defrule select-highest-scoring-candidate
   (declare (salience -100))
   ?c <- (candidate (type ?type) (score ?score)
                    (severity ?severity)
                    (evidence $?evidence)
                    (recommendation ?recommendation))
   (not (candidate (score ?higher&:(> ?higher ?score))))
   (not (diagnosis))
   =>
   (assert (diagnosis (type ?type) (score ?score)
                      (severity ?severity)
                      (evidence $?evidence)
                      (recommendation ?recommendation))))
```

4.5 Explanation Facility

The explanation facility is implemented through the contents of the diagnosis fact and the final print rule. It reports what the system concluded, how severe the incident is, which indicators supported the conclusion, the deterministic score used in ranking, and what the analyst should do next. Figure 2 shows an actual execution for a ransomware scenario.

Figure 2. Actual CLIPS execution for complete ransomware evidence.

4.6 Handling Competing and Incomplete Evidence

Figure 3 illustrates a scenario containing complete phishing evidence together with two brute-force indicators. The phishing candidate receives 95, while the partial brute-force candidate receives 64; consequently, the engine selects phishing compromise. Figure 4 demonstrates the fallback behavior. A traffic spike alone does not satisfy the partial DDoS rule, so the system returns an undetermined diagnosis and asks for additional evidence.

Figure 3. Highest-score conflict resolution when phishing and login indicators coexist.

Figure 4. Undetermined output when the available evidence is insufficient.

5. SYSTEM EVALUATION

5.1 Evaluation Design

The evaluation tested functional correctness, conflict resolution, fallback behavior, and inference overhead. Twelve scenarios were designed: eight complete-evidence cases covering every incident class, one partial ransomware case, two competing-evidence cases, and one insufficient-evidence case. Each scenario was executed by resetting the CLIPS environment, asserting its indicator facts, running the inference engine, and comparing the diagnosis with the expected result.

For timing, all 12 scenarios were repeated 30 times, producing 360 inference measurements. Timing included the CLIPS run cycle after facts had been asserted; file loading and Python startup were excluded. The environment used Python 3.13.5 and clipspy 1.0.6 on a Linux x86_64 platform.

5.2 Functional Results

Table 2. Controlled functional test results

ID	Scenario	Expected	Actual	Score	Result
TC-01	Complete ransomware evidence	ransomware	ransomware	100	Pass
TC-02	Credential phishing compromise	phishing-compromise	phishing-compromise	95	Pass
TC-03	Distributed brute-force attempt	brute-force-attack	brute-force-attack	88	Pass
TC-04	Distributed denial-of-service	distributed-denial-of-service	distributed-denial-of-service	96	Pass
TC-05	Endpoint malware with persistence	malware-infection	malware-infection	91	Pass
TC-06	Confirmed data exfiltration pattern	data-exfiltration	data-exfiltration	98	Pass
TC-07	Privileged insider-risk pattern	insider-threat	insider-threat	89	Pass
TC-08	SQL-oriented web application attack	web-application-attack	web-application-attack	94	Pass
TC-09	Partial ransomware evidence	ransomware	ransomware	72	Pass
TC-10	Phishing evidence dominates login noise	phishing-compromise	phishing-compromise	95	Pass

ID	Scenario	Expected	Actual	Score	Result
TC-11	Insufficient isolated evidence	undetermined	undetermined	0	Pass
TC-12	Exfiltration evidence dominates insider risk	data-exfiltration	data-exfiltration	98	Pass

The system produced the expected output in all 12 controlled scenarios. This corresponds to 100% rule-conformance accuracy for the designed test set. The result confirms that the implemented rules, scoring mechanism, fallback rule, and test harness behave consistently with the specified knowledge base. It does not establish 100% accuracy on real cybersecurity incidents, because the test cases were authored to verify the implementation and were not sampled from an independent operational dataset.

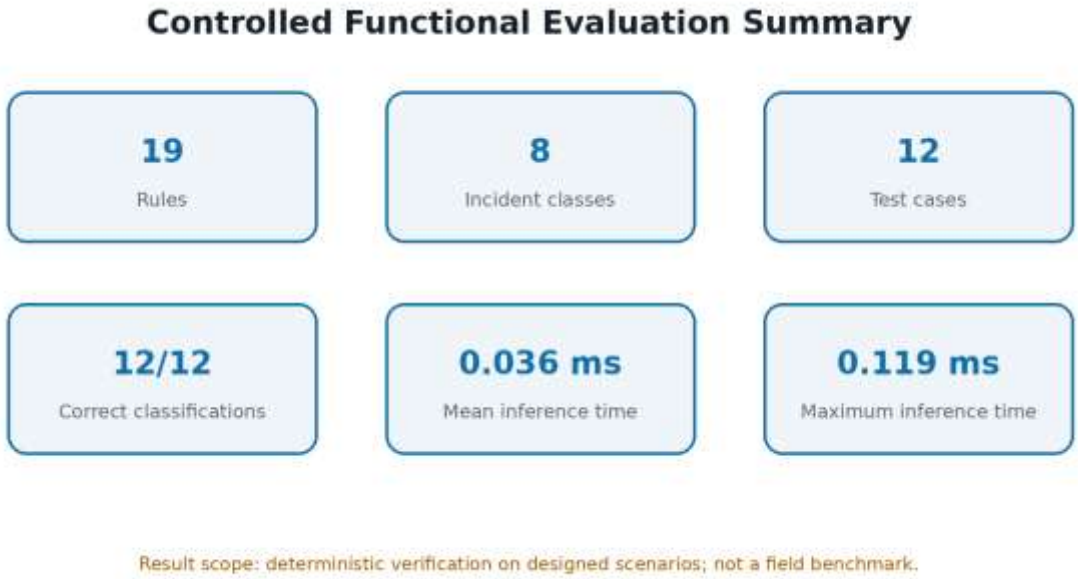

Figure 5. Summary of the controlled functional evaluation.

5.3 Inference Performance

Across 360 repeated runs, the mean inference time was 0.036 ms, the median was 0.031 ms, and the maximum observed time was 0.119 ms. These values show that a small production-rule knowledge base introduces negligible computational overhead in the test environment. In practice, total response time would be dominated by evidence collection, analyst review, external integrations, and organizational procedures rather than rule matching.

5.4 Discussion

The evaluation demonstrates four useful behaviors. First, complete patterns yield high-priority diagnoses with specific response guidance. Second, partial patterns allow the system to provide a suspected diagnosis without requiring every indicator. Third, the highest-score rule resolves competing candidates in a predictable and explainable manner. Fourth, the fallback rule avoids unsupported classification. Together, these behaviors are more suitable for decision support than a system that always forces one answer.

The main benefit is transparency. Every conclusion is connected to a short set of human-readable conditions, and the response recommendation can be reviewed and modified independently. This is useful for education, policy encoding, and controlled operational playbooks. The main weakness is coverage: new tactics, unusual combinations, and noisy telemetry may fall outside the rules. Rule-based systems also require maintenance when technologies, threats, and organizational procedures change.

5.5 Limitations and Threats to Validity

The test scenarios are synthetic and relatively small. They validate the software logic but do not measure false-positive rates, false-negative rates, analyst workload, or effectiveness in a live security operations center. The indicator values are assumed to be reliable, whereas real telemetry can be incomplete, contradictory, delayed, or manipulated. The deterministic scores are expert-authored priorities rather than probabilities. Moreover, the response actions are generic and may not fit every organization, legal environment, asset criticality, or business-continuity requirement.

Future validation should involve cybersecurity practitioners, historical incident reports, and blind test cases. A more advanced implementation could use certainty factors, fuzzy values, Bayesian evidence, or a hybrid architecture that combines anomaly detection with transparent rules. Integration with SIEM or SOAR platforms would also require authentication, access control, logging, change management, and safeguards against unsafe automated actions.

6. CONCLUSION

This research designed and implemented a CLIPS-based knowledge-based expert system for cybersecurity incident diagnosis and response. The prototype represents security indicators as facts and uses production rules to generate candidate incidents for eight categories. A score-based selection rule resolves competing diagnoses, and the explanation output presents severity, supporting evidence, and a defensive response recommendation. The system therefore demonstrates the principal components of a knowledge-based system: knowledge acquisition, knowledge representation, a knowledge base, an inference engine, conflict resolution, and an explanation facility.

Controlled testing covered 12 complete, partial, competing, and insufficient-evidence scenarios, all of which produced the expected implementation-level result. The rule engine also executed with very low overhead in the test environment. These findings support the feasibility of transparent rule-based decision support for narrow incident-triage tasks, while not claiming real-world predictive accuracy.

The most important future work is domain validation. Security analysts should review the rules, scores, severities, and recommendations; real incident cases should be used to evaluate error rates; and the knowledge base should be expanded through a controlled update process. Additional improvements include uncertainty handling, integration with MITRE ATT&CK technique mappings, automatic ingestion of SIEM indicators, multilingual explanation interfaces, and human-in-the-loop feedback. With those extensions, the prototype could evolve from a course implementation into a more comprehensive and auditable incident-response decision-support framework.

References

1. A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication 800-61 Revision 3, Apr. 2025. doi: 10.6028/NIST.SP.800-61r3.
2. National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
3. MITRE, "Enterprise Tactics," MITRE ATT&CK. Available: https://attack.mitre.org/tactics/ (accessed July 9, 2026).
4. G. Riley, CLIPS Reference Manual, Volume I: Basic Programming Guide, Version 6.4.2. Secret Society Software, LLC, Jan. 16, 2025.
5. J. C. Giarratano, CLIPS 6.4 User's Guide. Secret Society Software, LLC, 2025.
6. R. van der Kleij, J. M. Schraagen, B. Cadet, and H. Young, "Developing decision support for cybersecurity threat and incident managers," Computers & Security, vol. 113, art. 102535, 2022. doi: 10.1016/j.cose.2021.102535.
7. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, art. 20, 2019. doi: 10.1186/s42400-019-0038-7.
8. S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities," IEEE Access, vol. 10, pp. 112392-112415, 2022. doi: 10.1109/ACCESS.2022.3216617.
9. N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey," IEEE Access, vol. 10, pp. 93575-93600, 2022. doi: 10.1109/ACCESS.2022.3204171.
10. Azaab, S., et al., "A proposed expert system for selecting exploratory factor analysis procedures", Journal of the College of Education, vol. 4, no. 2, pp. 9-26, 2000.
11. Abu Amuna, Youssef M, et al., "The Role of Knowledge-Based Computerized Management Information Systems in the Administrative Decision-Making Process", International Journal of Information Technology and Electrical Engineering, vol. 6, no. 2, pp. 1-9, 2017.
12. Abu Naser, Samy S., "A methodology for expert systems testing and debugging", 1993.
13. Abu Naser, Samy, et al., "Variable Floor for Swimming Pool Using an Expert System", International Journal of Modern Engineering Research (IJMER), vol. 3, no. 6, pp. 3751-3755, 2013.
14. Abu-Naser, Samy S., et al., "An expert system for men genital problems diagnosis and treatment", International Journal of Medicine Research, vol. 1, no. 2, pp. 83-86, 2016.
15. Almurshidi, Suheir H, et al., "Expert System For Diagnosing Breast Cancer", 2018.
16. Dahouk, Ahmed Wahib, et al., "A Proposed Knowledge Based System for Desktop PC Troubleshooting", International Journal of Academic Pedagogical Research (IJAPR), vol. 2, no. 6, pp. 1-8, 2018.
17. Abu-Naser, Samy S., et al., "An expert system for feeding problems in infants and children", International Journal of Medicine Research, vol. 1, no. 2, pp. 79-82, 2016.
18. Khella, Randa, et al., "Rule Based System for Chest Pain in Infants and Children", International Journal of Engineering and Information Systems, vol. 1, no. 4, pp. 138-148, 2017.
19. Nassr, Mohammed S, et al., "Knowledge Based System for Diagnosing Pineapple Diseases", International Journal of Academic Pedagogical Research (IJAPR), vol. 2, no. 7, pp. 12-19, 2018.
20. Almadhoun, Hamza Rafiq, et al., "Banana Knowledge Based System Diagnosis and Treatment", International Journal of Academic Pedagogical Research (IJAPR), vol. 2, no. 7, pp. 1-11, 2018.
21. Abu-Naser, Samy S., et al., "An expert system for endocrine diagnosis and treatments using JESS", Journal of Artificial Intelligence; Scialert, vol. 3, no. 4, pp. 239-251, 2010.
22. Musleh, Musleh Mounir, et al., "Rule Based System for Diagnosing and Treating Potatoes Problems", International Journal of Academic Engineering Research (IJAER), vol. 2, no. 8, pp. 1-9, 2018.
23. Elqassas, Randa, et al., "Expert System for the Diagnosis of Mango Diseases", International Journal of Academic Engineering Research (IJAER), vol. 2, no. 8, pp. 10-18, 2018.
24. Alajrami, Mahmoud Ali, et al., "Onion Rule Based System for Disorders Diagnosis and Treatment", International Journal of Academic Pedagogical Research (IJAPR), vol. 2, no. 8, pp. 1-9, 2018.
25. Barhoom, Alaa M, et al., "Black Pepper Expert System", International Journal of Academic Information Systems Research (IJAISR), vol. 2, no. 8, pp. 9-16, 2018.
26. Kashkash, KA, et al., "Expert system methodologies and applications-a decade review from 1995 to 2004.", Journal of Artificial Intelligence, vol. 1, no. 2, pp. 9-26, 2005.
27. Al Rekhawi, Hazem A, et al., "Rickets Expert System Diagnoses and Treatment", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 149-159, 2017.
28. Ashqar, Belal A M, et al., "Image-Based Tomato Leaves Diseases Detection Using Deep Learning", International Journal of Academic Engineering Research (IJAER), vol. 2, no. 12, pp. 10-16, 2019.
29. Qwaider, Sabreen R, et al., "Expert System for Diagnosing Ankle Diseases", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 89-101, 2017.
30. Nabahin, Amal, et al., "Expert System for Hair Loss Diagnosis and Treatment", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 160-169, 2017.
31. Al-Qumboz, Mohammed N Abu, et al., "Spinach Expert System: Diseases and Symptoms", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 3, pp. 16-22, 2019.
32. Abu Ghali, Mahmoud J, et al., "Expert System for Problems of Teeth and Gums", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 198-206, 2017.
33. Mettleq, Alaa Soliman Abu, et al., "A Rule Based System for the Diagnosis of Coffee Diseases", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 3, pp. 1-8, 2019.
34. Aldaour, Ahmed F, et al., "An Expert System for Diagnosing Tobacco Diseases Using CLIPS", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 3, pp. 12-18, 2019.
35. Elsharif, Abeer A, et al., "An Expert System for Diagnosing Sugarcane Diseases", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 3, pp. 19-27, 2019.
36. Dheir, Ibtesam, et al., "Knowledge Based System for Diagnosing Guava Problems", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 3, pp. 9-15, 2019.
37. Al-Shawwa, Mohammed, et al., "Knowledge Based System for Apple Problems Using CLIPS", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 3, pp. 1-11, 2019.
38. Salman, Fatima M, et al., "Expert System for Castor Diseases and Diagnosis", International Journal of Engineering and Information Systems (IJEAIS), vol. 3, no. 3, pp. 1-10, 2019.
39. AbuEl-Reesh, Jihan Y, et al., "A Knowledge Based System for Diagnosing Shortness of Breath in Infants and Children", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 102-115, 2017.
40. Abu-Saqer, Mohammed M, et al., "Developing an Expert System for Papaya Plant Disease Diagnosis", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 4, pp. 14-21, 2019.
41. Alshawwa, Izzeddin A, et al., "An Expert System for Coconut Diseases Diagnosis", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 4, pp. 8-13, 2019.
42. El-Mashharawi, Hosni Q, et al., "An Expert System for Sesame Diseases Diagnosis Using CLIPS", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 4, pp. 22-29, 2019.
43. El Kahlout, Mohammed Ibraheem, et al., "An Expert System for Citrus Diseases Diagnosis", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 4, pp. 1-7, 2019.
44. Elsharif, Abeer A, et al., "Hepatitis Expert System Diagnosis Using Sl5 Object", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 4, pp. 10-18, 2019.
45. Dheir, Ibtesam M, et al., "Knowledge Based System for Diabetes Diagnosis Using SL5 Object", International Journal of Academic Pedagogical Research (IJAPR), vol. 3, no. 4, pp. 1-10, 2019.
46. Al-Shawwa, Mohammed O, et al., "A Proposed Expert System for Diagnosing Skin Cancer Using SL5 Object", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 4, pp. 1-9, 2019.
47. El-Mashharawi, Hosni Qasim, et al., "An Expert System for Arthritis Diseases Diagnosis Using SL5 Object", International Journal of Academic Health and Medical Research (IJAHMR), vol. 3, no. 4, pp. 28-35, 2019.
48. Abu-Naser, Samy S., et al., "A Proposed Expert System For Guiding Freshman Students In Selecting A Major In Al-Azhar University, Gaza.", Journal of Theoretical & Applied Information Technology, vol. 4, no. 9, 2008.
49. Mrouf, Ahmad, et al., "Knowledge Based System for Long-term Abdominal Pain (Stomach Pain) Diagnosis and Treatment", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 71-88, 2017.
50. Mansour, Aysha I, et al., "Knowledge Based System for the Diagnosis of Dengue Disease", International Journal of Academic Health and Medical Research (IJAHMR), vol. 3, no. 4, pp. 12-19, 2019.
51. Mansour, Aysha I, et al., "Expert System for the Diagnosis of Wheat Diseases", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 4, pp. 19-26, 2019.
52. Mettleq, Alaa Soliman Abu, et al., "Expert System for the Diagnosis of Seventh Nerve Inflammation (Bell's palsy) Disease", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 4, pp. 27-35, 2019.
53. Salman, Fatima M, et al., "Thyroid Knowledge Based System", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 5, pp. 11-20, 2019.
54. Alajrami, Mahmoud Ali, et al., "Grapes Expert System Diagnosis and Treatment", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 5, pp. 38-46, 2019.
55. El Kahlout, Mohammed Ibraheem, et al., "Silicosis Expert System Diagnosis and Treatment", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 5, pp. 1-8, 2019.
56. Al-Qumboz, Mohammed N Abu, et al., "Kidney Expert System Diseases and Symptoms", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 5, pp. 1-10, 2019.
57. Abu-Saqer, Mohammed M, et al., "Knowledge Based System for Uveitis Disease Diagnosis", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 5, pp. 18-25, 2019.
58. El Agha, Massoud, et al., "Polymyalgia Rheumatic Expert System", International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 4, pp. 125-137, 2017.
59. Alshawwa, Izzeddin A, et al., "An Expert System for Depression Diagnosis", International Journal of Academic Health and Medical Research (IJAHMR), vol. 3, no. 4, pp. 20-27, 2019.
60. Aldaour, Ahmed F, et al., "Anemia Expert System Diagnosis Using Sl5 Object", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 5, pp. 9-17, 2019.
61. Abu-Nasser, Bassem S, et al., "Rule-Based System for Watermelon Diseases and Treatment", International Journal of Academic Information Systems Research (IJAISR), vol. 2, no. 7, pp. 1-7, 2018.
62. Ahmed, Adel, et al., "Knowledge-Based Systems Survey", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 7, pp. 1-22, 2019.
63. Masri, Naser, et al., "Survey of Rule-Based Systems", International Journal of Academic Information Systems Research (IJAISR), vol. 3, no. 7, pp. 1-23, 2019.
64. Abu-Naser, Samy S, et al., "A Proposed Expert System for Skin Diseases Diagnosis", Journal of Applied Sciences Research, vol. 4, no. 12, pp. 1682-1693, 2008.
65. Salman, Fatima, et al., "Rule based System for Safflower Disease Diagnosis and Treatment", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 8, pp. 1-10, 2019.
66. Khalil, Ahmed J, et al., "Apple Trees Knowledge Based System", International Journal of Academic Engineering Research (IJAER), vol. 3, no. 9, pp. 1-7, 2019.
67. Albatish, Islam Mohammad, et al., "Modeling and controlling smart traffic light system using a rule based system", pp. 55-60, 2019.
68. Abu-Naser, Samy S, et al., "An Expert System for Genital Problems in Infants", WWJMRD, vol. 2, no. 5, pp. 20-26, 2016.
69. Abu-Naser, Samy S, et al., "An expert system for shoulder problems using CLIPS", World Wide Journal of Multidisciplinary Research and Development, vol. 2, no. 5, pp. 1-8, 2016.
70. Salman, Fatima M, et al., "Expert System for COVID-19 Diagnosis", International Journal of Academic Information Systems Research (IJAISR), vol. 4, no. 3, pp. 1-13, 2020.
71. Abu-Naser, Samy S, et al., "Ear Diseases Diagnosis Expert System Using SL5 Object", World Wide Journal of Multidisciplinary Research and Development, vol. 2, no. 4, pp. 41-47, 2016.
72. Almadhoun, Husam R, et al., "An Expert System for Diagnosing Coronavirus (COVID-19) Using SL5", International Journal of Academic Engineering Research (IJAER), vol. 4, no. 4, pp. 1-9, 2020.
73. Abu-Naser, Samy S, et al., "A Ruled Based System for Ear Problem Diagnosis and Treatment", World Wide Journal of Multidisciplinary Research and Development, vol. 2, no. 4, pp. 25-31, 2016.
74. Abu-Naser, Samy S, et al., "An expert system for nausea and vomiting problems in infants and children", International Journal of Medicine Research, vol. 1, no. 2, pp. 114-117, 2016.
75. Abu Naser, Samy, "An Agent Based Intelligent Tutoring System For Parameter Passing In Java Programming", Journal of Theoretical & Applied Information Technology, vol. 4, no. 7, 2008.
76. Abu-Naser, Samy Saleem, et al., "An Expert System For Diagnosing Eye Diseases Using CLIPS.", Journal of Theoretical & Applied Information Technology, vol. 4, no. 10, 2008.
77. Elhabil, Basel Y, et al., "An Expert System for Ankle Problems", International Journal of Engineering and Information Systems (IJEAIS), vol. 5, no. 4, pp. 57-66, 2021.
78. Elhabil, Basel Y, et al., "Expert System for Hib Problems", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 5-16, 2021.
79. Abu-Naser, Samy S, "Sl5 Object: Simpler Level 5 Object Expert System Language", International Journal of Soft Computing, Mathematics and Control (IJSCMC), vol. 4, no. 4, pp. 25-37, 2015.
80. Samhan, Lamis F, et al., "Expert System for Knee Problems Diagnosis", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 4, pp. 59-66, 2021.
81. Alkahlout, Mohammed A, et al., "Expert System Diagnosing Facial-Swelling Using CLIPS", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 29-36, 2021.
82. Mansour, Aysha I, et al., "Expert system for the diagnosis of high blood pressure diseases", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 23-28, 2021.
83. Alkahlout, Mohammed A, et al., "Knowledge Based System for Diagnosing Throat Problem CLIPS and Delphi languages", International Journal of Academic Engineering Research (IJAER), vol. 5, no. 6, pp. 7-12, 2021.
84. Alfarra, Amjad H, et al., "An Expert System for Neck Pain Diagnosis", rnal of Academic Information Systems Research (IJAISR), vol. 5, no. 7, pp. 1-8, 2021.
85. Aish, Mohammed A, et al., "Lower Back Pain Expert System Using CLIPS", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 57-67, 2021.
86. Al-Masawabe, Marah M, et al., "Expert System for Short-term Abdominal Pain (Stomach Pain) Diagnosis and Treatment", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 37-56, 2021.
87. Mansour, Aysha I, et al., "An Expert System for Diagnosing Cough Using SL5 Object", International Journal of Academic Engineering Research (IJAER), vol. 5, no. 6, pp. 13-27, 2021.
88. Abu-Jamie, Tanseem N, et al., "Diagnosing Cough Problem Expert System Using CLIPS", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 79-90, 2021.
89. Alkahlout, Mohammed A, et al., "Throat Problems Expert System Using SL5 Object", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, pp. 68-78, 2021.
90. Hamadaqa, Mohammed Hazem M, et al., "Hair Loss Diagnosis Expert System and Treatment Using CLIPS", International Journal of Academic Engineering Research (IJAER), vol. 5, no. 5, pp. 37-42, 2021.
91. Alsaqqa, Azmi H, et al., "Knowledge Based for Tooth Problems", International Journal of Academic Information Systems Research (IJAISR), vol. 5, no. 5, 2021.
92. Abu-Naser, Samy Salim, et al., "A proposed Expert System for Foot Diseases Diagnosis", American Journal of Innovative Research and Applied Sciences, vol. 2, no. 4, pp. 155-168, 2016.
93. Abu-Naser, Samy S., et al., "Male Infertility Expert system Diagnoses and Treatment", American Journal of Innovative Research and Applied Sciences, vol. 2, no. 4, 2016.
94. Radwan, Hanan IA, et al., "A Proposed Expert System for Passion Fruit Diseases", International Journal of Academic Engineering Research (IJAER), vol. 6, no. 5, pp. 24-33, 2022.
95. Sababa, Raed Z, et al., "A Proposed Expert System for Strawberry Diseases Diagnosis", International Journal of Engineering and Information Systems (IJEAIS), vol. 6, no. 5, pp. 52-66, 2022.
96. Al-Qadi, Mohanad H, et al., "Developing an Expert System to Diagnose Tomato Diseases", International Journal of Academic Engineering Research (IJAER), vol. 6, no. 5, pp. 34-40, 2022.
97. AlQatrawi, Mohammed JA, et al., "Rule Based System for Diagnosing Lablab Problems", International Journal of Academic and Applied Research (IJAAR), vol. 6, no. 5, pp. 249-256, 2022.
98. El-Habibi, Mohammed F, et al., "A Proposed Expert System for Obstetrics & Gynecology Diseases Diagnosis", International Journal of Academic Multidisciplinary Research (IJAMR), vol. 6, no. 5, pp. 305-321, 2022.