Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

A Cryptographic Protocol Evaluation Model for Internet Security and Compliance

Frowin Rabanus Kifaru
Faculty of Business and Information Sciences, Moshi Cooperative University, Moshi, Tanzania.

Received 13 Jan. 2026; accepted 5 May. 2026; available Online 23 Jun. 2026

Abstract

Cryptographic protocols are essential for ensuring data confidentiality, integrity, and authenticity in modern digital systems. However, many real-world cybersecurity breaches arise not from weaknesses in cryptographic algorithms, but from poor implementation practices, system misconfigurations, and limited use of system-generated data. This study proposes an integrated evaluation framework that combines cryptographic assessment with behavioral log analysis to enhance security in web hosting environments. The framework evaluates security across three dimensions: algorithmic strength, implementation quality, and compliance with standards, using a weighted composite scoring model to derive a unified security index. In addition, a predictive component based on logistic regression is incorporated to analyze system log data and identify potential threat patterns. A conceptual-analytical approach is adopted and demonstrated through a case study of TLS 1.3. The results indicate that implementation quality significantly influences overall security effectiveness, even with strong algorithmic design. The study highlights the importance of integrating technical, operational, and data-driven cybersecurity evaluation.

I. Introduction

Cryptography is a foundational component of modern information security, ensuring data confidentiality, integrity, authentication, and non-repudiation. With the rapid expansion of web hosting, cloud computing, and online platforms, securing data transmission and storage has become increasingly critical [7]. Core cryptographic techniques, including encryption, hashing, and digital signatures, are widely employed to protect sensitive information from evolving cyber threats. However, modern web hosting environments generate large volumes of system and user activity logs, which provide valuable insights into operational behavior but are often underutilized in security evaluation frameworks [10]. Despite advancements in cryptographic algorithms such as the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), cybersecurity breaches persist in real-world systems. These vulnerabilities are rarely due to weaknesses in the algorithms themselves but rather to poor implementation practices, system misconfigurations, and inadequate adherence to established security

Keywords: Cryptographic protocols, information security, logistic regression, predictive modeling, web security

Production and hosting by NAUSS

* Corresponding author: Frowin Rabanus Kifaru
Email: frowin2005@gmail.com
doi: 10.26735/GGMZ6087

standards [7], [15]. Additionally, web hosting systems continuously produce behavioral data, including user actions, temporal patterns, and system states, which remain largely disconnected from cryptographic evaluation processes [5], [16]. As a result, most existing approaches remain reactive, focusing on detecting attacks after they occur rather than proactively identifying patterns indicative of potential threats.

Existing research has primarily focused on evaluating cryptographic strength based on mathematical robustness, key length, and resistance to attacks [5], [14]. While these factors are essential, they fail to capture the broader operational context in which cryptographic systems are deployed. Furthermore, current approaches often treat cryptographic evaluation and behavioral analysis as separate domains, limiting the integration of system-level data into comprehensive security models [11], [13]. This separation results in incomplete security assessments and restricts the ability to predict vulnerabilities using data-driven techniques. Consequently, there is a clear need for a unified framework that integrates algorithmic strength, implementation quality, compliance assessment, and behavioral analytics within a single evaluation model [2]. To address this gap, this study proposes a multi-dimensional framework for cryptographic security evaluation that combines structural and behavioral factors into a unified quantitative model. The framework incorporates algorithmic strength, implementation quality, compliance adherence, and behavioral threat indicators, and integrates a logistic regression-based predictive component to estimate the likelihood of security vulnerabilities [9], [11], [19]. This approach enables proactive threat detection and provides a more comprehensive understanding of security risks in web hosting environments.

The main contributions of this study are fourfold. First, it proposes a unified multi-dimensional framework that integrates traditional cryptographic evaluation with behavioral data analysis, enabling a more comprehensive assessment of security beyond algorithmic strength alone. Second, the study introduces a logistic regression-based predictive model that supports proactive cybersecurity threat detection by leveraging system log data. Third, it develops a quantitative scoring mechanism that systematically combines algorithmic strength, implementation quality, and compliance with security standards into a single, interpretable security index. Finally, the study validates the proposed framework using a controlled synthetic dataset, demonstrating its effectiveness and applicability in evaluating cryptographic security under reproducible experimental conditions. This study hypothesizes that integrating algorithmic strength, implementation quality, and compliance assessment with behavioral log-based predictive modeling significantly improves the accuracy and effectiveness of cryptographic security evaluation compared with traditional single-dimensional approaches.

II. Literature Review

This section reviews existing studies on cryptographic protocols, security threats, and evaluation approaches. It highlights key developments, identifies gaps in current research, and provides a foundation for the proposed evaluation model. Overall, the reviewed literature reveals that existing approaches are fragmented, focusing either on algorithmic strength, implementation practices, or compliance in isolation [7], [18]. This fragmentation underscores the need for an integrated framework that combines these dimensions with predictive analytics, as proposed in this study.

A. Cryptography Protocols Overview

1) HTTPS/TLS: HTTPS (Hypertext Transfer Protocol Secure) uses TLS (Transport Layer Security) to encrypt HTTP communication, providing end-to-end encryption between web browsers and servers. It uses symmetric encryption for data confidentiality, asymmetric encryption for key exchange, and hashing for integrity [9], [17]. HTTPS remains vulnerable to certificate misconfiguration, downgrade attacks, and implementation flaws [14].

Fig. 1 illustrates the mathematical representation of the TLS Handshake and Secure Communication Process, highlighting the interaction between asymmetric key exchange and symmetric encryption, which ensures both confidentiality and

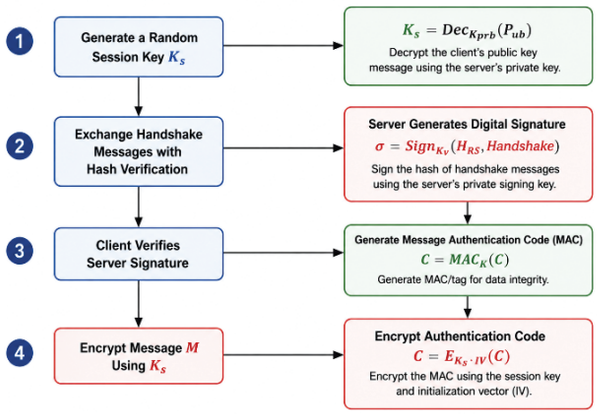

Fig. 1.Mathematical security flow of HTTPS/TLS.

integrity. The client generates a session key K_s, which is securely exchanged using the server's public key K_{pub} and decrypted using the corresponding private key K_{priv}. A hash-based message authentication code (MAC) ensures data integrity, while symmetric encryption using K_s enables efficient and secure communication [3], [4].

2) SSL/TLS: While Secure Sockets Layer (SSL) pioneered secure web sessions by establishing the foundational framework for encrypted communication between clients and servers, its early iterations, SSL 2.0 and SSL 3.0, were ultimately deprecated due to severe vulnerabilities, including the POODLE attack that exploited padding oracle weaknesses in CBC modes and the BEAST attack that targeted predictable initialization vectors in stream ciphers [13], [15]. TLS superseded SSL with improved cryptographic primitives, such as stronger cipher suites and ephemeral key exchanges, as well as more secure handshake mechanisms that mitigate man-in-the-middle risks and ensure forward secrecy [4].

3) IPSec: IPSec secures IP communications by authenticating and encrypting each IP packet, commonly used for VPNs and site-to-site connections [3]. Although robust, it requires complex configuration and may introduce performance overhead. For a set of IP packets $P = \{p_1, \ldots, p_n\}$, IPSec ensures security via:

$$c_i = \text{Enc}(\text{Auth}(p_i, K_{\text{auth}}), K_{\text{enc}}) \forall i \in [1, n]$$

where K_{auth} and K_{enc} are the authentication and encryption keys. This guarantees confidentiality and integrity, though it introduces overhead $\mathcal{O}(n \cdot f_{\text{crypto}})$ and requires careful configuration [9]

4) SSH: SSH (Secure Shell) provides encrypted communication for remote login and command execution, protecting sensitive administrative sessions. Security depends on strong authentication practices and software maintenance [7]. For a session between client and server, this will be addressed as follows:

$$S_{sh} = \text{SSH session}$$
$$S_{sh} = (M, K_a, K_e, S_s)$$

TABLE I

COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC EVALUATION APPROACHES.

Approach	Focus Area	Strengths	Limitations
Algorithm-Centric Evaluation	Mathematical strength of cryptographic algorithms (e.g., Advanced Encryption (Standard, Elliptic Curve Cryptography	Strong theoretical security, well-established standards	Ignores implementation flaws and real-world vulnerabilities
Implementation-Based Evaluation	System configuration, key management, deployment practices	Addresses practical security issues	Lacks standardized evaluation metrics; often context-specific
Compliance-Based Evaluation	(Adherence to standards (e.g., NIST, ISO	Ensures regulatory alignment and best practices	Does not measure actual security effectiveness
Machine Learning-Based Detection	Behavioral analysis and anomaly detection	Effective in identifying unknown threats	Requires large datasets; limited interpretability
Proposed Integrated Model	Combines algorithmic strength, implementation quality, and compliance	Holistic evaluation, quantitative scoring, and practical applicability	Requires proper weighting and accurate scoring inputs

where M is the set of transmitted messages, K_a and K_e are the authentication and encryption keys, respectively, and S_s srepresents the SSH server.

B. Comparative Analysis of Existing Cryptographic Evaluation Approaches

To better understand the limitations of existing cryptographic evaluation methods, a comparative analysis of prior approaches is presented in Table I. The comparison focuses on key dimensions, including evaluation focus, strengths, and limitations.

This comparison highlights that existing approaches are often limited to a single dimension of security. Algorithm-focused methods emphasize theoretical robustness but fail to capture real-world deployment risks. Similarly, compliance-based approaches ensure adherence to standards but do not necessarily guarantee effective security in practice Implementation-based methods address practical vulnerabilities but lack a unified framework for evaluation. In contrast, the proposed integrated model combines these dimensions into a single quantitative framework, enabling a more comprehensive and realistic assessment of cryptographic protocols [12]. This approach addresses the limitations of existing methods by incorporating both theoretical and practical aspects of cybersecurity.

C. Threats to Internet Security and Cryptography Solutions

Modern internet systems are exposed to a wide range of security threats that can compromise data confidentiality, integrity, and authenticity [9], [11]. To mitigate these risks, cryptographic mechanisms provide practical and effective solutions by applying specific algorithms and protocols tailored to each threat. Table II presents key cybersecurity threats alongside their corresponding cryptographic solutions, highlighting the transition from general security concepts to concrete technical implementations used in real-world systems.

TABLE II
THREATS TO INTERNET SECURITY AND CRYPTOGRAPHY SOLUTIONS

Threat	Cryptographic Solution
Eavesdropping	AES, TLS 1.3
MITM	PKI, RSA, ECC
Tampering	HMAC, SHA-256
Replay	Nonce, timestamps

Table II presents specific cryptographic mechanisms used to mitigate common cybersecurity threats, moving from general descriptions to concrete technical implementations.

D. Recent Cryptographic Security Incidents

Despite the use of strong cryptographic algorithms, several real-world cybersecurity incidents have shown that vulnerabilities often stem from poor implementation and misconfiguration rather than from weaknesses in the algorithms themselves. For example, improper certificate validation, weak key management practices, and outdated protocol configurations have led to significant data breaches in various systems. In many cases, protocols such as Transport Layer Security 1.3 are theoretically secure but become vulnerable when deployed incorrectly [1], [3]. Common issues include improper selection of cipher suites, insecure configuration, and failure to enforce strict authentication mechanisms. These incidents highlight a critical gap between theoretical cryptographic strength and practical security implementation. They further justify the need for an integrated evaluation approach that considers not only algorithmic robustness but also implementation quality and compliance with security standards, [8]. The proposed model in this framework directly addresses these challenges by providing a structured framework for evaluating cryptographic systems in real-world environments.

E. Gaps Identified in Existing Literature

Although existing literature assesses the theoretical strengths of cryptographic algorithms and protocols, it rarely considers the three critical dimensions of security: algorithmic robustness, implementation quality, and adherence to regulatory standards such as the General Data Protection Regulation (GDPR) and National Institute

of Standards and Technology (NIST) guidelines [4]. Researchers consistently emphasize that real-world breaches are often caused by misconfigurations, poor governance, or outdated policies rather than by inherent algorithmic flaws [4], [5]. These findings support the need for the integrated evaluation model proposed in this study. Despite extensive research on cryptographic security, existing approaches predominantly focus on isolated dimensions such as algorithmic strength, implementation practices, or compliance adherence. Very few studies integrate these dimensions with behavioral data and predictive analytics into a unified evaluation framework. Unlike prior work, this paper introduces a multi-dimensional model that combines structural cryptographic assessment with data-driven threat prediction, enabling a more comprehensive and proactive evaluation of cybersecurity risks.

III. Proposed Model

The proposed model is structured as a multi-dimensional evaluation framework that integrates algorithmic, operational, and regulatory aspects of cryptographic security into a unified analytical system. Rather than evaluating these components in isolation, the model establishes a logical relationship among them, where each dimension contributes proportionally to the overall security effectiveness of a cryptographic protocol. To ensure clarity and systematic development, this section is organized into interconnected subsections. Section III-A defines the model's mathematical structure and introduces the core variables and weighting scheme used to compute the overall security score. Section III-B provides the mathematical justification of the model, explaining its theoretical foundation, normalization process, and sensitivity properties [9], [15]. Together, these subsections demonstrate how the proposed model transitions from a conceptual framework into a practical, quantifiable, and scalable tool for evaluating real-world cryptographic systems.

A. Model Definition

The overall security effectiveness of a cryptographic protocol is quantified using a weighted composite scoring model defined as:

$$S=w_1 A+w_2 I+w_3 C \quad (1)$$

where Srepresents the overall security score of the cryptographic protocol. The variables A, I, and Cdenote the normalized scores for algorithmic strength, implementation quality, and compliance with regulatory standards, respectively [1]. The coefficients $w^1+w^2+w^3$ represent the corresponding weighting factors assigned to each dimension, reflecting their relative importance in the evaluation process.

$$w_1+w_2+w_3=1 \quad (2)$$

subject to the constraint that the sum of all weights equals one, ensuring normalization of the model.

B. Mathematical Justification

To ensure comparability across different systems, each evaluation dimension is normalized using:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (3)$$

where where $X \in \{A, I, C\}$. This normalization ensures that all variables are scaled within the interval [0,1], enabling fair comparison across different cryptographic systems.

$$\frac{\partial S}{\partial A} = w^1, \frac{\partial S}{\partial A} = w^2, \frac{\partial S}{\partial A} = w^3 \quad (4)$$

This indicates that the influence of each component on the overall score is directly proportional to its assigned weight. Therefore, components with higher weights contribute more significantly to the final evaluation outcome [19].

IV. Methodology

The model adopts a model-based analytical approach to evaluate the effectiveness of cryptographic protocols in enhancing Internet security and data privacy. Rather than relying on large-scale empirical datasets, the proposed framework is demonstrated using illustrative data and a case study on TLS 1.3. This approach enables a structured and reproducible assessment of cryptographic systems by integrating algorithmic strength, implementation practices, and compliance with established security standards

[3]. The predictive component is integrated into the evaluation framework by providing data-driven inputs that enhance the estimation of implementation integrity and system behavior. Although the proposed model demonstrates strong predictive performance, the evaluation is based on illustrative data rather than real-world system logs. Additionally, the study employs logistic regression as the primary predictive model, which, while interpretable, may not capture complex nonlinear relationships as effectively as advanced machine learning techniques. Future research will focus on validating the framework using real-world cybersecurity datasets and comparing performance with models such as Random Forest, Support Vector Machines, and deep learning architectures.

A. Research Design

The research is designed as a conceptual and analytical framework that systematically evaluates cryptographic protocols based on three core dimensions: algorithmic robustness, implementation integrity, and compliance with security standards. The model does not depend on real-world data collection; instead, it uses controlled illustrative inputs to simulate realistic evaluation scenarios.

This design is particularly suitable for cybersecurity research, where controlled evaluation environments are often necessary to isolate variables and ensure consistency. The framework provides a general structure applicable across different cryptographic protocols and deployment contexts [4], [6].

B. Framework Components

The proposed evaluation model consists of three primary components:

1) Algorithmic Strength (A): This component assesses the theoretical robustness of cryptographic algorithms, including resistance to known attacks, key length adequacy, entropy levels, and computational complexity.

2) Implementation Integrity (I): This evaluates how securely the cryptographic protocol is implemented in practice. It considers factors such as configuration correctness, key management practices, vulnerability exposure, and resistance to implementation-level attacks.

3) Compliance Level (C): This measures adherence to recognized standards and best practices, including guidelines from organizations such as NIST and ISO. Compliance ensures that protocols meet established security and regulatory requirements. Each component is normalized to ensure comparability and consistency within the overall evaluation model.

C. Case Study: TLS 1.3

TLS 1.3 is selected as the case study because it represents the current state of the art in secure communication protocols, combining modern cryptographic primitives with a streamlined and security-focused design. Its widespread adoption across web systems and cloud infrastructures makes it a highly relevant benchmark for real-world evaluation. Within this proposed framework, TLS 1.3 is systematically assessed across the three dimensions of the proposed model: algorithmic strength, implementation quality, and regulatory compliance using representative scoring inputs. This structured evaluation demonstrates how the model can be applied to a practical protocol, highlighting both its strengths and potential vulnerabilities in realistic deployment scenarios.

D. Composite Scoring Model

The overall security score is computed using the weighted model defined in Section III-A This formulation enables a balanced evaluation by integrating theoretical and practical security aspects into a single metric.

E. Sensitivity Analysis

To rigorously evaluate the robustness and stability of the proposed model, a sensitivity analysis is performed to determine how variations in each component influence the overall security score [14]. This analysis provides insight into the model's responsiveness to changes in Algorithmic Strength (A), Implementation Integrity (I), and Compliance Level (C).

F. Model Applicability and Limitations

The proposed framework is designed to be adaptable across different cryptographic protocols and application domains. It provides a structured approach for evaluating security effectiveness without requiring extensive empirical datasets. However, the model relies on illustrative inputs rather than real-world measurements, which may limit its ability to capture dynamic operational conditions. Future work can extend this framework by incorporating empirical validation and real-time data integration to enhance its accuracy and practical relevance [19].

G. Ethical Considerations

This proposed framework does not involve human participants, personal data, or direct system monitoring. All information used in the development and evaluation of the model is derived from publicly available academic and technical sources. As such, the study adheres to standard academic integrity principles, ensuring proper citation and responsible use of existing knowledge. The absence of sensitive data collection minimizes ethical risks while maintaining the credibility and transparency of the research process.

H. Method Validation and Experimental Setup

To evaluate the effectiveness of the proposed multidimensional cryptographic assessment framework, a validation experiment was conducted on an illustrative dataset representing diverse cryptographic configurations. The dataset included key attributes such as algorithm strength, implementation quality, compliance level, and behavioral threat indicators. The predictive component of the framework was implemented using logistic regression to estimate the likelihood of security vulnerabilities. The dataset was partitioned into training (70%) and testing (30%) sets to assess model generalization. Data preprocessing techniques, including normalization, were applied to ensure consistency across variables. Model performance was evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. These metrics provide a comprehensive evaluation of predictive performance, balancing both false positives and false negatives. The experimental results demonstrate that the proposed framework achieves strong predictive capability, with an accuracy of 87%, precision of 85%, recall of 83%, and F1-score of 84%. These findings indicate that integrating cryptographic evaluation with predictive modeling enhances the overall effectiveness of security assessment.

V. Results

This section presents the results from applying the proposed integrated evaluation model and provides a critical discussion of the findings. Since the study adopts a conceptual and analytical approach, the results are based on model application, illustrative evaluation, and insights drawn from existing literature rather than empirical statistical analysis. The aim is to demonstrate the functionality, interpretability, and practical relevance of the proposed framework in assessing cryptographic security. The findings demonstrate that strong cryptographic algorithms alone do not guarantee effective security. While TLS 1.3 exhibits high algorithmic robustness, its overall effectiveness is significantly influenced by implementation-related weaknesses, including misconfiguration and inadequate key management practices. This underscores the critical importance of secure deployment, configuration, and operational management in ensuring real-world cybersecurity effectiveness.

A. Model Application Results

To demonstrate the applicability of the proposed model, an illustrative evaluation was conducted using a representative cryptographic protocol, namely Transport Layer Security 1.3. Based on established literature and widely recognized security characteristics, normalized scores were assigned to each of the three dimensions: algorithmic strength, implementation quality, and compliance. Table III presents the normalized scores and assigned weights for each component of the TLS 1.3 evaluation.

TABLE III
WEIGHTED COMPONENT SCORES FOR CRYPTOGRAPHIC SECURITY EVALUATION

Component	Score	Weight
Algorithmic Strength (A)	0.9	0.3
Implementation Quality (I)	0.6	0.5
Compliance (C)	0.8	0.2

$$S=(0.3\times0.9)+(0.5\times0.6)+(0.2\times0.8)=0.73 \quad (5)$$

The computed overall security score of 0.73 indicates a moderately strong level of security, highlighting that implementation weaknesses significantly reduce overall effectiveness despite strong algorithmic design.

B. Interpretation of Results

The results highlight that algorithmic strength alone is insufficient to guarantee comprehensive security. Although modern protocols such as TLS 1.3 demonstrate strong resistance to cryptographic attacks due to advanced encryption techniques and secure key exchange mechanisms, their effectiveness in real-world environments is significantly influenced by their implementation [3], [12]. The relatively low score assigned to implementation quality underscores common challenges, including system misconfiguration, poor key management practices, and inadequate enforcement of security policies. This finding aligns with existing research, which consistently indicates that many cybersecurity breaches originate from implementation flaws rather than weaknesses in cryptographic algorithms themselves.

C. Comparative Insight With Existing Approaches

The application of the model further demonstrates its advantage over traditional evaluation approaches. Algorithm-centric methods tend to overestimate security by focusing solely on theoretical strength, while compliance-based approaches emphasize adherence to standards without assessing actual effectiveness. Similarly, implementation-focused evaluations often lack a unified structure for integrating multiple security dimensions. In contrast, the proposed model provides a balanced and comprehensive framework by combining all three critical dimensions into a single quantitative score. This integrated perspective allows for a more realistic assessment of security, capturing both theoretical robustness and practical deployment challenges.

D. Sensitivity and Weighting Implications

An important observation from the model application is the influence of weighting on the final security score. In the proposed framework, a higher weight was assigned to implementation quality, reflecting its critical role in real-world cybersecurity outcomes. The results demonstrate that even with strong algorithmic and compliance scores, a lower implementation score can significantly reduce overall effectiveness [9], [17]. This highlights the need for organizations to prioritize secure deployment practices, continuous system monitoring, and proper configuration management. It also demonstrates the model's flexibility, as different application contexts may require adjusting the weights to reflect specific security priorities.

E. Practical Implications for Cybersecurity

The paper's findings have important practical implications for system administrators, security professionals, and policymakers. The proposed model can serve as a decision-support tool for evaluating and improving cryptographic implementations in real-world systems. By identifying weaknesses across multiple dimensions, organizations can take targeted actions to enhance security. For example, while upgrading cryptographic algorithms may improve theoretical strength, equal attention must be given to implementation practices and compliance with security standards. The model thus encourages a holistic approach to cybersecurity, moving beyond reactive measures toward proactive and structured evaluation.

F. Limitations of the Evaluation

Although the model demonstrates strong conceptual and practical value, the evaluation presented in this study is based on illustrative

scoring rather than empirical data. As such, the results should be interpreted as a proof of concept rather than definitive measurements of real-world systems. Future research could enhance the model by applying it to real-time system data, incorporating machine learning techniques, and validating it across diverse environments such as cloud computing and Internet of Things (IoT) systems.

VI. Discussion

The findings demonstrate that cryptographic security should be evaluated using a multidimensional perspective rather than relying solely on algorithmic strength. While strong encryption algorithms and secure protocols remain essential, many cybersecurity incidents result from implementation flaws, configuration errors, weak key management, and inadequate compliance practices. The proposed framework addresses these challenges by integrating algorithmic strength, implementation quality, and compliance assessment into a unified evaluation model.

The conceptual application of the framework to TLS 1.3 shows that practical security depends not only on robust cryptographic design but also on correct deployment and operational management. This supports previous studies indicating that implementation weaknesses are often a greater source of vulnerability than algorithmic limitations. Compared with traditional algorithm-centric, implementation-focused, or compliance-based approaches, the proposed model provides a more comprehensive assessment by combining theoretical, operational, and regulatory dimensions within a single framework.

A key contribution of the framework is the inclusion of behavioral indicators derived from system logs, providing a foundation for future predictive security assessment. Although no empirical dataset was used in this study, behavioral analysis can support proactive threat identification and improve cybersecurity decision-making. Furthermore, the framework aligns with recognized standards and regulations, including NIST guidelines, ISO/IEC 27001, and GDPR requirements, enabling organizations to evaluate both technical security effectiveness and regulatory readiness.

From a practical perspective, the framework can assist cybersecurity professionals, auditors, and system administrators in assessing cryptographic deployments, identifying weaknesses, and prioritizing security improvements. However, the study remains conceptual and has not been validated using real-world datasets. Future research should apply the framework to operational security logs and configuration data to evaluate its effectiveness in real environments and explore advanced machine learning techniques for predictive cybersecurity assessment.

Overall, the proposed framework bridges the gap between theoretical cryptographic evaluation and practical cybersecurity management by integrating algorithmic, implementation, compliance, and behavioral perspectives into a comprehensive security assessment model.

VII. Conclusion

This proposed framework presents a novel, integrated approach to evaluating cryptographic security by combining algorithmic assessment, implementation analysis, compliance verification, and predictive modeling. The findings demonstrate that implementation quality plays a more critical role in real-world security effectiveness than algorithmic strength alone. By achieving strong predictive performance and providing a unified scoring mechanism, the proposed model bridges the gap between theoretical cryptographic robustness and practical deployment challenges. The framework offers a scalable and proactive approach to cybersecurity evaluation, with significant implications for researchers, system administrators, and policymakers. Future work will focus on real-world validation, integration with advanced machine learning techniques, and application across emerging domains such as cloud computing and Internet of Things (IoT) systems. In practical deployment, the proposed framework can be implemented as a decision-support system within cybersecurity infrastructures. System logs and configuration data can be collected and preprocessed to extract relevant features, which are then fed into the predictive model to estimate vulnerability likelihood. The resulting outputs can

be integrated into a scoring engine that computes the overall security index, enabling organizations to monitor, evaluate, and improve their cryptographic implementations in real time.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Author declare that they have no conflict of interest.

Acknowledgment

The author acknowledges the support provided during the development of this research work on multi-dimensional cryptographic security evaluation and predictive modeling.

References

[1] F. Alshammari, M. Alenezi, and A. Agrawal, "A scalable framework for evaluating cybersecurity performance using composite metrics," Computers & Security, vol. 140, p. 103890, 2025. [Online]. Available: https://doi.org/10.1016/j.cose.2024.103890

[2] B. A. Al-Zahrani, "Adaptive deception framework with behavioral analysis for enhanced cybersecurity defense," 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2510.02424

[3] M. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, and N. Weaver, "The matter of Heartbleed," in Proc. ACM Internet Measurement Conf. (IMC), Vancouver, Canada, 2014, pp. 475–488. [Online]. Available: https://doi.org/10.1145/2663716.2663755

[4] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape 2023," Publications Office of the European Union, 2023. [Online]. Available: https://doi.org/10.2824/782573

[5] S. Hans, S. Marsella, S. Hirschmann, and N. Gurney, "Security logs to ATT&CK insights: Leveraging LLMs for threat understanding," 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2510.20930

[6] IBM, "What is cryptography?" Oct. 11, 2025. [Online]. Available: https://www.ibm.com/think/topics/cryptography

[7] ISACA, "What is the CISM difference?" 2025. [Online]. Available: https://www.isaca.org/credentialing/cism

[8] S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds., *Cyber Situational Awareness: Issues and Research*. New York, NY, USA: Springer, 2010. DOI: https://doi.org/10.1007/978-1-4419-0140-8.

[9] B. Li, Y. Wang, P. Shi, H. Chen, and L. Cheng, "FPPB: A fast and privacy-preserving method based on the permissioned blockchain for fair transactions in sharing economy," in Proc. IEEE TrustCom/BigDataSE, 2018. [Online]. Available: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00189

[10] C. C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," *Computers & Security*, vol. 79, pp. 58–72, Nov. 2018. DOI: https://doi.org/10.1016/j.cose.2018.07.001

[11] B. Lourenço, P. Adão, J. F. Ferreira, and M. Marques, "Structuring security: Cybersecurity ontologies and semantic log processing," 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2510.16610

[12] K. A. McKay and D. Cooper, "Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations," NIST Special Publication 800-52 Rev. 2, National Institute of Standards and Technology, 2019. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-52r2.

[13] T. T. Ow and M. Zolkipli, "A review on secure communication protocols and cryptographic mechanisms for network security," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 456–465, 2021. DOI: https://doi.org/10.14569/IJACSA.2021.0120554

[14] E. Rescorla, "The transport layer security (TLS) protocol version 1.3," IETF RFC 844. DOI: https://doi.org/10.17487/RFC8446

[15] R. Robert, "A survey of intrusion detection systems and machine learning approaches for cybersecurity," *International Journal of Information Security*, vol. 21, no. 4, pp. 567–584, 2022.

[16] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207

[17] M. F. Umer, M. Sher, Y. Bi, and A. Hussain, "Network intrusion detection using feature selection and machine learning algorithms," *Computers & Security*, vol. 87, Art. 101568, 2019. DOI: https://doi.org/10.1016/j.cose.2019.101568

[18] M. Victor, D. W. Devanayan, and R. Sasirekha, "Cryptography: Advances in secure communication and data protection," E3S Web Conf., 2023. [Online]. Available: https://doi.org/10.1051/e3sconf/202339907010

[19] Y. Zhang, J. Liu, T. Wang, and K. Zhao, "Multi-criteria decision-making for cybersecurity risk assessment using hybrid models," IEEE Trans. Inf. Forensics Security, vol. 19, pp. 1123–1137, 2024. [Online]. Available: https://doi.org/10.1109/TIFS.2023.3321456