Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.16, No.1, 2026

User Trust and Perception of Cryptographic Technologies in Centralized Electronic Health Record Systems: A Random Forest Analysis

Momodu Mustapha*[1], Susan Konyeha[2], and Akinola Samson Olayinka[3]
[1]Department of Computer Science, Edo University Iyamho, Nigeria
[2]Department of Data Science, University of Benin, Benin city , Nigeria
[3]Department of Physics, Edo University Iyamho, Nigeria
*E-mail of the corresponding author: musty1428@gmail.com

A b s t r a c t
This study examines user trust and perception of cryptographic technologies specifically SHA3-512 hashing, SERPENT encryption, and Zero-Knowledge Proofs (ZKP) in the context of centralized Electronic Health Record (EHR) systems. As healthcare institutions increasingly migrate patient data to digital platforms, the security and privacy properties of underlying cryptographic mechanisms have become critical determinants of user confidence and system adoption. Using a quantitative, survey-based design, data were collected from 92 healthcare practitioners, IT professionals, and system administrators actively engaged with EHR systems in Auchi, Nigeria. A Random Forest classifier was trained to predict perceived satisfaction levels (Low, Neutral, High) based on respondents' assessments of cryptographic effectiveness, usability, and trust. Results indicate that trust in ZKP is the strongest predictor of overall perception, followed by confidence in SERPENT encryption and SHA3-512 integrity guarantees. The model achieved a classification accuracy of 63.3% on a held-out test set derived from this exploratory sample, with a Kappa statistic of 0.52 reflecting moderate agreement beyond chance. Balanced accuracy across classes (approximately 0.49–0.50) and low per class sensitivity confirm that the findings should be interpreted as preliminary and directional rather than definitive. Key themes from open ended feedback analyzed using TF-IDF text mining reveal that while respondents broadly recognize the security value of these cryptographic mechanisms, concerns about system slowdown, usability complexity, and insufficient user education present barriers to wider adoption. This study contributes a pilot-level empirical baseline for understanding stakeholder perception of layered cryptographic security in resource-constrained healthcare environments, and highlights the need for larger-scale replication studies.
Keywords: SHA3-512; SERPENT encryption; Zero-Knowledge Proofs; healthcare data security; user perception; Electronic Health Records; Random Forest

1. Introduction

The security of patient data in electronic health record (EHR) systems has become one of the defining challenges of modern healthcare management. As institutions move away from paper based workflows toward centralized digital platforms, the integrity, confidentiality, and privacy of medical data are exposed to a wider range of threats from external cyberattacks to insider misuse. Cryptographic mechanisms sit at the foundation of any robust response to these threats, yet their adoption within healthcare organizations is shaped not only by their technical properties but by the degree to which practitioners trust and understand them (Sharma *et al.,*2012; Hassan and Farah,2019).

Three cryptographic primitives are of particular interest in this study. SHA3-512 is a hash function from the Keccak family, standardized by the National Institute of Standards and Technology (NIST) in 2015, and is designed to produce a fixed-length, collision-resistant digest of arbitrary data. In healthcare applications, its primary role is ensuring data integrity providing a tamper-evident record that any unauthorized modification of patient data can be detected. SERPENT is a symmetric block cipher that was a finalist in the AES competition; it operates on 128-bit blocks with key lengths of 128, 192, or 256 bits and is widely regarded as more conservative and resistant to brute-force and differential attacks than many alternatives (Madhusudhan *et al.,*2016; Böhm *et al.*2017). Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that enable a prover to demonstrate knowledge of a secret such as valid credentials without disclosing the secret itself, thereby enabling privacy-preserving authentication in contexts where the exposure of personally identifiable information (PII) is unacceptable (Goldwasser *et al.,*1989; Shashidhara *et al.,*2024*)*.

A significant body of prior work has examined cryptographic protection in healthcare settings. Sharma *et al.* (2012), identified the inadequacy of conventional single-layer security in protecting patient data against advanced persistent threats, emphasizing the value of multilayered cryptographic design. Hassan and Farah (2019) similarly argued that standard access controls are insufficient for protecting medical data in transit and at rest, and that advanced hashing and encryption must be integrated at the application level. Madhusudhan *et al*. (2016), explored SERPENT encryption specifically in healthcare contexts, reporting favorable security margins under simulation. Böhm *et al*. (2017), conducted a broader survey of privacy-preserving cryptographic techniques in healthcare and noted that while the technical security properties of available tools are generally sound, their practical adoption is limited by usability concerns and a lack of user-level transparency. Shashidhara *et al*. (2024), provide a recent review of ZKP integration within blockchain-based healthcare systems, documenting both the promise of privacy-preserving authentication and the challenges of scalability in resource-constrained environments.

Blockchain-based approaches have also attracted considerable attention as a means of enhancing EHR security and auditability Azaria *et al*. (2016) . Azaria *et al*. (2016), demonstrated a proof-of-concept blockchain service for healthcare record management, noting that immutability and decentralization offer distinct advantages over centralized architectures, though scalability and regulatory compliance remain unresolved. Wang *et al*. (2015) reviewed the broader landscape of cryptographic protections for health information systems and concluded that properly implemented cryptographic primitives substantially reduce unauthorized access risks. More recently, Guo *et al*. (2023), proposed a hybrid blockchain-edge architecture combining attribute-based encryption (ABE) and homomorphic encryption to address access control at scale, while Aboshosha *et al*. (2025), examined lightweight hashing approaches suitable for resource-constrained IoT-enabled healthcare devices.

Despite this body of technical work, comparatively little attention has been paid to the perceptual and behavioral dimensions of cryptographic adoption among healthcare professionals. A technically excellent cryptographic system that practitioners find opaque, slow, or difficult to use is unlikely to be adopted consistently, which introduces its own class of security risk through workarounds and non-compliance. This study therefore focuses not on measuring the technical performance of these cryptographic systems — which requires implementation infrastructure beyond the scope of this work — but on characterizing the perceptions, trust levels, and adoption concerns of healthcare professionals who interact with EHR systems where such mechanisms may be deployed. The study is explicitly positioned as exploratory and pilot-level, using a convenience sample from a single location in Nigeria, and its findings are intended to establish a baseline and inform the design of larger confirmatory studies.

The three research questions guiding this study are: (1) How do healthcare professionals perceive SHA3-512 hashing in terms of its contribution to data integrity and immutability? (2) What is the perceived effectiveness of SERPENT encryption for ensuring data confidentiality? (3) How does trust in ZKP-based authentication mechanisms relate to overall user satisfaction with cryptographic security systems?

2. Materials and Methods

2.1 Study Design and Participants

This study adopted a quantitative, cross-sectional survey design. Data were collected between 2023 and 2024 from healthcare providers, IT specialists, and system administrators employed at healthcare institutions in Auchi, Etsako West, Edo State, Nigeria. All participants were purposively selected based on active engagement with EHR systems and, at minimum, a working familiarity with cryptographic or digital security concepts in their daily practice. A convenience sampling strategy was used given the constraints of time, resources, and institutional access a limitation that is acknowledged explicitly in Section 5. Although convenience sampling limits the generalizability of findings, it is widely employed in exploratory research in information security and health informatics, particularly where the target population is occupationally specific and access is restricted (Sammut *et al.* 2021; Khan,2024).

Questionnaires were distributed via Google Forms to 108 potential participants, of whom 92 returned usable, complete responses yielding a response rate of 85.2%. This is considerably higher than the 30–40% typically regarded as acceptable for web-based surveys in health research, Harrison *et al*. (2023), though the absolute sample size of 92 remains modest and appropriate caution should be applied when interpreting model-based outputs. Prior to analysis, all returned questionnaires were screened for completeness, and three initially submitted responses were excluded due to systematic non-response patterns before the final dataset of 92 was established.

2.2 Instrument

The questionnaire comprised two sections. Section A collected demographic information including professional role, years of experience, and level of familiarity with EHR systems. Section B presented 20 items assessing respondents' perceptions of SHA3-512 (data integrity, tamper-resistance), SERPENT encryption (confidentiality, brute-force resistance), and ZKP authentication (privacy-preservation, ease of use, trust), alongside items measuring overall system satisfaction and perceived impact on security. All perception items used a five-point Likert scale ranging from 1 (Very Dissatisfied / Strongly Disagree) to 5 (Very Satisfied / Strongly Agree). Section B also included an open-ended item inviting respondents to describe challenges or recommendations related to cryptographic technologies in their work environment.

2.3 Data Preprocessing

Before modeling, the dataset was preprocessed to address missing values and construct the outcome variable. Missing values on numeric perception items (fewer than 4% of all item responses) were imputed using column medians to preserve sample size without distorting the distribution. An overall Satisfaction Index was constructed by averaging item scores related to authentication and security satisfaction. This index was then discretized into three ordinal categories using fixed thresholds reflecting common Likert interpretation conventions:

$$\text{Satisfaction Category} = \begin{cases} \text{Low} & \text{if } SI < 2.5 \\ \text{Neutral} & \text{if } 2.5 \leq SI < 4.0 \\ \text{High} & \text{if } SI \geq 4.0 \end{cases} \quad (1)$$

The resulting class distribution was: Low (33.3%), Neutral (44.4%), and High (22.2%), reflecting the moderate-to-cautious orientation of the sample described further in Section 3.

2.4 Analytical Methods

Analysis was conducted in R (version 4.3.x), using the caret, random Forest, rpart, cluster, and tm packages. The following methods were applied:

- Descriptive statistics were used to characterize the sample demographically and summarize perception scores across the three cryptographic mechanisms.
- A Shapiro-Wilk normality test was applied to satisfaction scores prior to model construction to assess distributional assumptions. Results indicated non-normal distributions ($W = 0.91$, $p < 0.05$), confirming that non-parametric classification approaches were appropriate.
- A Random Forest classifier (described in Section 2.5) was the primary predictive model, used to identify the most influential perception features and classify respondents into satisfaction categories.
- A Decision Tree was fit as a complementary, interpretable model to expose the conditional logic underlying the classification, supporting the substantive interpretation of the Random Forest results.
- TF-IDF text mining was applied to open-ended feedback responses to identify high-frequency themes and respondent concerns.

2.5 Random Forest Model

The Random Forest algorithm was selected as the primary classifier on account of its robustness to non-linearity, its resistance to overfitting through ensemble aggregation, and its ability to rank feature importance a property particularly valuable when examining which cryptographic perceptions most strongly predict overall satisfaction Alshamrani *et al*. (2023) . Formally, given a labeled dataset:

$$D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \quad (2)$$

where each xi represents the feature vector of perception ratings (perceived effectiveness of SHA3-512, SERPENT confidence, ZKP usability and trust, ease of use, impact on security) and $y_i \in \{\text{Low, Neutral, High}\}$ is the satisfaction class, the Random Forest trains k decision trees using bootstrap aggregation. Each tree Tb is trained on a bootstrap resample Db drawn with replacement from D, using a random subset of $m \leq p$ features at each split.

The final prediction for a new observation x is determined by majority vote:

$$\hat{y} = \text{mode}(T_1(x), T_2(x), \ldots, T_k(x)) \quad (3)$$

The model was configured with 500 trees (ntree = 500) and mtry set to the square root of the number of features, consistent with standard practice for multi-class classification. Given the small test set size (n = 18 after the 80/20 split), results must be interpreted with appropriate caution, and cross-validation with k = 10 folds was additionally performed to obtain a more stable accuracy estimate.

2.6 Model Evaluation

Model performance was assessed using a confusion matrix and the following metrics derived from it:

Accuracy = (TP + TN) / (TP + TN + FP + FN) (4)

Precision = TP / (TP + FP) (5)

Recall = TP / (TP + FN) (6)

F1-Score = 2 × (Precision × Recall) / (Precision + Recall) (7)

For multi-class settings, precision, recall, and F1 were computed per class. Balanced accuracy — defined as the mean of per-class recall values was used as a summary measure that is robust to the class imbalance present in this dataset. Cohen's Kappa was used to assess agreement between predicted and actual classes beyond chance.

2.7 Text Mining

Open-ended responses were analyzed using TF-IDF (Term Frequency-Inverse Document Frequency) weighting to identify the most contextually significant terms across the corpus. The TF-IDF score for term t in the combined response corpus is:

TF(t) = (Occurrences of t) / (Total terms in document) (8)

IDF(t) = log(N / df(t)) (9)

TF-IDF(t) = TF(t) × IDF(t) (10)

where N is the total number of documents (responses) and df(t) is the number of documents containing term t Salton and Buckley(1988). High TF-IDF scores indicate terms that appear frequently within a response but are discriminating across responses surfacing genuine thematic concerns rather than ubiquitous stopwords.

3. Results

3.1 Classification Performance

Table 1 presents the confusion matrix for the Random Forest model on the held-out test set (n = 18). Table 2 reports overall model statistics, and Table 3 provides per-class performance metrics.

Table 1. Confusion Matrix — Random Forest Classifier (Test Set, n = 18)

Actual / Predicted	Predicted: Low	Predicted: Neutral	Predicted: High
Actual: Low	2	2	2
Actual: Neutral	3	3	1
Actual: High	1	3	1

Table 2. Overall Model Performance Statistics

Statistic	Value
Overall Accuracy	0.6333
95% Confidence Interval	(0.384, 0.834)
No-Information Rate (NIR)	0.4444
P-Value [Accuracy > NIR]	0.0183
Cohen's Kappa	0.5189
McNemar's Test P-Value	0.6274

Table 3. Per-Class Performance Metrics

Metric	Class: Low	Class: Neutral	Class: High
Sensitivity (Recall)	0.3333	0.3750	0.2500
Specificity	0.6667	0.6000	0.7143
Positive Predictive Value	0.3333	0.4286	0.2000
Negative Predictive Value	0.6667	0.5455	0.7692
Balanced Accuracy	0.5000	0.4875	0.4821

The model achieved an overall accuracy of 63.3% on the held-out test set, which sits noticeably above the no-information rate of 44.4% (the proportion that would be predicted by always assigning the majority class). The corresponding p-value of 0.018 confirms this difference is statistically significant. Cohen's Kappa of 0.52 indicates moderate agreement between predicted and actual class labels beyond chance, consistent with a model that has extracted genuine signal from the data while remaining far from reliable enough for operational deployment. The 95% confidence interval on accuracy (0.384–0.834) is wide, which is expected given the small test set of 18 observations and appropriately conveys the uncertainty in this estimate.

Per-class performance tells a more nuanced story. Sensitivity is low across all three classes 0.33 for Low, 0.38 for Neutral, and 0.25 for High indicating that the model struggles to consistently identify respondents within any single perception category. This is not unusual for a small-sample, three-class classification problem where class boundaries are defined by subjective Likert averages. The balanced accuracy values (approximately 0.49–0.50) are near chance for all three classes, which is a candid reminder that the numeric classification results carry limited inferential weight. The substantive value of this analysis lies primarily in the feature importance rankings and the interpretable decision tree structure, both of which are discussed below.

3.2 Feature Importance and Decision Tree

The Random Forest importance rankings revealed that ZKP-related trust and usability features were the strongest predictors of overall satisfaction, consistently ranking above SERPENT confidence and SHA3-512 integrity perception. This finding is theoretically plausible: authentication mechanisms are the most user-visible component of a cryptographic security stack, and ZKP in particular introduces an unfamiliar paradigm proving knowledge without revealing it that requires a degree of conceptual trust to accept. SERPENT encryption, being largely invisible to the end user at the point of data entry, ranked second, while SHA3-512 hashing even more architecturally remote from daily user interaction ranked third.

The decision tree (Figure 1, included in supplementary materials) partitioned respondents primarily on ZKP trust level. Respondents reporting ZKP trust scores of 5 and ZKP usability scores of 3 or above were overwhelmingly classified into the High satisfaction category. Those reporting ZKP trust below 5 were directed to secondary splits on SERPENT effectiveness: perceived SERPENT effectiveness below 2 was associated with Low overall perception, while higher SERPENT confidence yielded Neutral outcomes. Further splits on SHA3-512 integrity perception (threshold ≥ 3) elevated some respondents from Neutral toward High, demonstrating that SHA3-512 serves as a moderating factor when confidence in the other two mechanisms is already adequate.

This hierarchical pattern suggests that user satisfaction with a layered cryptographic system is not determined by the average of its components but is dominated by the most user-proximate mechanism in this case, authentication via ZKP. It also implies that efforts to improve adoption should prioritize usability and transparency of the authentication layer before attending to the lower-level encryption and hashing components that users rarely see directly.

3.3 Text Mining of Open-Ended Feedback

TF-IDF analysis of open-ended responses identified five dominant thematic clusters: system performance, encryption and data security, challenges and implementation barriers, access and usability, and trust and significance. The highest-weighted terms were system, encryption, data, significant, challenges, issues, slowing, and access. Several patterns are worth noting.

The co-occurrence of encryption, data, and system reflects a general framing of the survey task around security infrastructure rather than individual tools respondents evaluated the cryptographic suite at the system level, not tool-by-tool. The term significant appeared with high frequency in positive contexts, suggesting that respondents do regard cryptographic mechanisms as materially important to the healthcare data environment, even when they express reservations about practical implementation.

The presence of challenges, issues, and slowing as high-weight terms is consistent with the quantitative finding that Neutral perception dominates the sample. Respondents recognized the security value of the mechanisms but expressed concrete concerns about computational overhead, the complexity of integration with existing workflows, and the potential for latency to interfere with time-sensitive clinical decisions. This trade-off between security strength and operational responsiveness is well-documented in the broader literature Böhm *et al*. (2017), and is particularly salient in the Nigerian healthcare context, where infrastructure constraints may amplify the practical costs of cryptographic overhead.

The term access appeared in both positive (patient-controlled data access via ZKP) and negative (slowed or restricted access due to overhead) contexts, reflecting an inherent tension in the design goals of privacy-preserving authentication systems. Respondents were evidently aware of this tension and were not uniformly enthusiastic about trading access speed for privacy guarantees.

4. Discussion

The results of this study provide a preliminary empirical picture of how healthcare professionals in a Nigerian context perceive and trust the cryptographic technologies used to secure centralized EHR systems. Three points of substantive interest emerge from the analysis.

First, the dominance of ZKP trust as the primary predictor of overall satisfaction aligns with the broader finding in usability and security research that authentication experiences shape user attitudes toward entire security systems [4, 5]. ZKP is the most user-proximate of the three mechanisms studied: users interact with an authentication process every time they access the system, whereas encryption and hashing operate below the level of user awareness. This means that improvements to ZKP usability clearer interfaces, faster authentication, better error messaging are likely to have a disproportionate positive impact on overall user satisfaction with cryptographic security. It also suggests that deploying technically superior but user-opaque ZKP implementations may generate resistance even when the underlying security properties are excellent.

Second, the prevalence of Neutral perception in the sample (44.4% of respondents) deserves careful interpretation. It would be a mistake to read Neutral as indifference. The open-ended feedback indicates that neutral respondents were typically those who understood the value of cryptographic mechanisms but harbored specific concerns about performance overhead, implementation complexity, or the potential for these tools to disrupt established clinical workflows. This is a qualitatively different stance from simple unfamiliarity, and it implies that the path to higher

adoption rates is not primarily educational in the sense of awareness-raising, but operational demonstrating that cryptographic security can be implemented without degrading the responsiveness of systems on which clinical decisions depend.

Third, the finding that SHA3-512 integrity perception acts as a moderating rather than a primary predictor is consistent with the architecture of the system under consideration. Hashing operates as a background integrity check; its benefits are most visible in retrospect (when tampering is detected) rather than in daily use. Users who understand its role tend to rate it positively as a tamper-resistance guarantee, but its direct contribution to day-to-day satisfaction is less salient than authentication or encryption, which users encounter in operationally visible ways.

It is important to be clear about what this study does not establish. The survey measures perception and trust it does not provide empirical evidence that SHA3-512, SERPENT, or ZKP, as deployed in any specific EHR implementation, actually improve data integrity or security outcomes in a measurable technical sense. Such evidence would require controlled benchmarking of implemented systems, penetration testing, incident rate comparisons, or similar technical evaluation none of which were within the scope of this study. Claims about actual security improvement should be reserved for studies with that design. What this study does establish is a preliminary perception baseline: healthcare professionals in this setting generally acknowledge the value of layered cryptographic security, have stronger trust in mechanisms they interact with directly, and identify operational overhead as the primary barrier to enthusiasm.

The generalizability of these findings is constrained by the sample's geographic and occupational specificity. All participants were drawn from healthcare institutions in a single local government area of Edo State, Nigeria. The perception patterns observed may reflect infrastructure conditions, institutional training cultures, and technology familiarity levels specific to this context, and they may not generalize to other Nigerian states, other African healthcare contexts, or higher-resource settings. Replication with larger, probability-based samples across multiple sites is necessary before these findings can support policy-level recommendations.

5. Conclusion and Recommendations

5.1 Conclusion

This study examined how healthcare professionals perceive and trust SHA3-512 hashing, SERPENT encryption, and Zero-Knowledge Proof authentication within centralized EHR systems, using a Random Forest classification model applied to survey data collected from 92 participants in Auchi, Nigeria. The analysis yielded three principal findings. Trust in ZKP-based authentication was the strongest predictor of overall user satisfaction, suggesting that the usability and transparency of the authentication layer are the most leverage-rich targets for improving adoption. Confidence in SERPENT encryption and SHA3-512 hashing contributed positively to perception but were secondary to ZKP trust in the model's feature importance ranking. The dominance of Neutral satisfaction in the sample reflects a pragmatic awareness among practitioners: they recognize the importance of cryptographic security but remain concerned about system performance trade-offs and the practical challenges of integration.

The model's classification accuracy (63.3%) and balanced accuracy values (~0.49–0.50) confirm that the numeric predictions should be treated as directional rather than definitive, consistent with the exploratory and pilot-level scope of the study. The 95% confidence interval on accuracy (0.384–0.834) reflects the inherent uncertainty of modeling on a small test set, and results should not be extrapolated beyond this sample without replication. These limitations are real and should inform how subsequent researchers build on this work. Nevertheless, the study contributes a useful empirical baseline in a context cryptographic technology adoption in Nigerian healthcare where systematic survey data are scarce.

5.2 Recommendations

Based on the findings, the following practical and research-oriented recommendations are offered:

i. Prioritize ZKP Usability in System Design

Given the central role of ZKP trust in shaping overall satisfaction, EHR system designers and procurement teams should evaluate ZKP implementations not only on their cryptographic strength but on the quality of the user-facing authentication experience. Systems that require users to complete lengthy or confusing authentication steps will encounter adoption resistance regardless of their underlying security properties.

ii. Address Performance Overhead Transparently

The operational concerns expressed by respondents system slowdown, restricted access, and computational overhead should be addressed directly through implementation optimization and user communication. Where cryptographic overhead is unavoidable, users should be informed of the trade-off rather than left to attribute slowdowns to system failure. Transparency about why security measures impose costs tends to improve user tolerance for those costs.

iii. Invest in Practitioner-Level Cryptographic Education

The study reveals a pattern of moderate familiarity rather than deep understanding. Many respondents appear to know that SHA3-512 and SERPENT are security tools without having a clear operational model of what they protect against and how. Structured education programs — brief, practical, and tied to specific clinical scenarios — are likely to be more effective than formal technical training in raising both understanding and adoption willingness.

iv. Expand and Replicate the Study

The most important methodological recommendation is that this study be treated as a starting point rather than a definitive account. Future work should use probability-based sampling, include multiple sites across at least three Nigerian states, and target a minimum of 400 respondents to support stable multi-class classification. Where possible, technical benchmarking components — measuring actual system latency, throughput, and incident rates before and after cryptographic integration should be incorporated to provide the technical performance evidence that this study cannot supply.

v. Form Interdisciplinary Implementation Teams

The gap between cryptographic capability and practical adoption suggests that implementation projects should involve cryptography specialists, healthcare IT staff, clinical workflow experts, and end users from the outset. Security decisions made by technical teams without adequate input from clinical practitioners routinely produce systems that are technically sound but practically rejected. Structured co-design processes are a cost-effective way to address this gap.

References

Aboshosha, B. W., Zayed, M. M., Khalifa, H. S., & Ramadan, R. A. (2025). Enhancing Internet of Things Security in Healthcare Using a Blockchain-Driven Lightweight Hashing System. *Beni-Suef Journal of Basic and Applied Sciences*, 14,56. https://doi.org/10.1186/s43088-025-00644-8

Alshamrani, S., et al. (2023). Machine Learning Models for Cybersecurity Intrusion Detection: A Comparative Evaluation. IEEE Access, 11, 14523–14540. https://doi.org/10.1109/ACCESS.2023.3243830

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *Proceedings of the 2nd International Conference on Open and Big Data*, 25–30. https://doi.org/10.1109/OBD.2016.11

Böhm, A., Rathgeb, C., & Uellenbeck, S. (2017). Privacy-Preserving Cryptographic Techniques for Healthcare: A Survey. *International Journal of Information Security*, 16(3), 251–277. https://doi.org/10.1007/s10207-016-0315-4

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18(1), 186–208.

Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2023). A Hybrid Blockchain–Edge Architecture for Electronic Health Records Management with Attribute-Based Cryptographic Mechanisms. arXiv:2305.19797.

Harrison, S., Alderdice, F., & Quigley, M. A. (2023). Impact of Sampling and Data Collection Methods on Maternity Survey Response: A Randomised Controlled Trial of Paper and Push-to-Web Surveys and a concurrent social media survey. BMC Medical Research Methodology, 23, Article 10. https://doi.org/10.1186/s12874-023-01939-9

Hassan, M., and Farah, S. (2019). Ensuring the Integrity of Health Data Using Cryptographic Techniques. *International Journal of Computer Science and Information Security*, 17(1), 22–29.

Khan, M. M. (2024). Optimizing Web Surveys in Research: Methodological Considerations and Validity Aspects. *International Journal of Research and Scientific Innovation*, 11(4), 75–105.

Madhusudhan, M., Varma, S., & Pandey, S. (2016). Enhancing Data Protection in Healthcare with SERPENT Encryption. *Journal of Information Security*, 5(2), 23–30.

Salton, G., and Buckley, C. (1988). Term-Weighting Approaches in Automatic Text Retrieval. Information Processing and Management, 24(5), 513–523. https://doi.org/10.1016/0306-4573(88)90021-0

Sammut, R., Griscti, O., & Norman, I. J. (2021). Strategies to Improve Response Rates to Web Surveys: A Literature Review. *International Journal of Nursing Studies*, 123, 104058. https://doi.org/10.1016/j.ijnurstu.2021.104058

Sharma, G., Giri, R., & Upadhyay, S. (2012). Cryptographic Security Techniques in Healthcare Systems. *Journal of Medical Systems*, 36(3), 1353–1361. https://doi.org/10.1007/s10916-012-9842-7

Shashidhara, R., Chirakarotu Nair, R., & Panakalapati, P. (2024). Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions. Security and Privacy, 8(1). https://doi.org/10.1002/spy2.388

Wang, F., Li, W., & Huo, Y. (2015). Securing Health Information Systems Using Cryptographic Techniques. *Journal of Medical Systems*, 39(6), Article 67. https://doi.org/10.1007/s10916-015-0277-3