Machine learning methods for classification and prediction information security risk assessment

Alva Hendi Muhammad[1], Asro Nasiri[2], Agung Harimurti[1,3]
[1]Department of Informatics, Postgraduate School, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
[2]Department of Informatics, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
[3]Division of Informatics Literacy, Ministry of Communication and Information Technology of the Republic of Indonesia, Makassar, Indonesia

Article Info

Article history:

Received Feb 19, 2024
Revised Oct 18, 2024
Accepted Oct 23, 2024

Keywords:

Classification
Cybersecurity
Information security
Machine learning
Risk assessment
Security analysis

ABSTRACT

Information is an essential company asset that must be protected. The value of information assets depends on the type and scale of the business and its role in delivering services. One of the primary programs that can help identify areas of improvement and guide the development of security awareness programs is risk assessment. Managing cybersecurity risks is critical to protecting enterprises from developing cyber threats and promoting resilience. This includes detecting, assessing, and mitigating risks to protect sensitive data, systems, and networks. While cybersecurity risk management is challenging, organizations may improve their security posture. This paper seeks to contribute to the field of information security risk assessment by leveraging the power of machine learning to provide quick, cost-effective, and individualized risk assessments for small and medium enterprises. Specifically, we extend the evaluation for security level classification by utilizing a support vector machine, random forest, and gradient boosting algorithms. The results demonstrate how well the model detects significant cases while reducing false positives. The model's exceptional precision ensures that its identifications are dependable, while the high recall demonstrates that it accurately detects relevant data. Precision is critical in security risk assessment because a false positive result might have profound effects.

Corresponding Author:

Alva Hendi Muhammad
Department of Informatics, Postgraduate School, Universitas Amikom Yogyakarta
St. Ring Road Utara, Condong Catur, Sleman, Yogyakarta 55283, Indonesia
Email: alva@amikom.ac.id

1. INTRODUCTION

Information security systems are essential for safeguarding digital assets in today's data-driven world. To address the expanding array of cyber threats, organizations rely on state-of-the-art technologies and recent advancements in the field [1]. When dealing with corporate information security issues, a risk-based strategy is one of the most effective methods [2]. Risk assessment is a systematic process encompassing risk analysis and evaluation aimed at a thorough understanding of the current information security risks and their potential consequences [3]. This process presents significant challenges owing to its interdependencies with various platforms, operating systems, application programs, networks, individuals, and processes [4], [5]. Incorrect information in risk assessment can pose significant and costly threats, as underestimating risks can leave the organization vulnerable to severe threats. In contrast, overestimating risks can lead to discontinuing valuable IT services and technologies. Thus, managing cybersecurity risks is essential for protecting organizations against continuously evolving cyber threats. This involves the process of identifying, assessing, and mitigating risks to protect sensitive data, systems, and networks [2].

While cybersecurity risk management does pose challenges, businesses have excellent opportunities to improve their security posture. The dynamic nature of potential threats poses a significant challenge to effectively managing cyber security threats, and organizations find it difficult to keep up with ever-evolving threats [6]. Since cybercriminals are constantly devising new strategies to attack targets, it is challenging for organizations to foresee and counter new threats. To address this issue, organizations must adopt flexible and responsive risk management approaches capable of swiftly adapting to new threats [7], [8]. According to the National Institute of Standards and Technology (NIST), risk management consist of four components, namely risk framing, risk assessment, risk response strategy, and risk monitoring [5]. Unlike other components, the risk assessment process facilitates the identification of threats, vulnerabilities, possible damage, and the probability of exploits.

An information security risk assessment (ISRA) is essential for organizations, as it critically evaluates the effectiveness of policies in protecting asset integrity, ensuring data confidentiality, and maintaining data accessibility and availability [2]. This assessment scrutinizes an organization’s capacity to protect its valuable and essential assets. While the field of cybersecurity assessment lacks a single, globally accepted theoretical framework, there are several established methodologies guiding the process, including the ISO 2700 Series, the NIST SP 800 Series, and control objectives for information and related technology (COBIT) [5], [9], [10]. These frameworks offer guidance for research and practical application, especially in examining the assessment process and its influence on information security in organizations. While there is some overlap in general security principles among these frameworks, the choice of a specific framework hinges on various factors. This includes the industry in which the organization operates, regulatory requirements, and the organization’s unique concerns [8], [11], [12]. The scope of the ISRA depends entirely on the specific needs and circumstances of the involved organization [12].

The necessity for thorough and effective risk assessment in the field of information security is growing as cyber threats become more sophisticated. The cornerstone of many economies, small and medium-sized enterprises (SMEs), are not immune from these security concerns. Despite their nimbleness and ingenuity, SMEs face particular cybersecurity challenges. SMEs frequently have particular difficulties, such as uneven support from upper management [13], issue-specific policies and procedures that workers have to follow constantly but disregard strategic direction [14], and also limited funding but rapidly evolving threat environments [15]. Even with sufficient funds, they struggle to prioritize effective security programs, both technically and non-technically [16]. The continuously changing cybersecurity threat landscape and best practices might make them even more vulnerable [4], [11]. The increased propensity of cybercriminals to target SMEs emphasizes the essential need for effective security procedures [2]. Therefore, organizational readiness to deal with such scenarios is essential for effective risk management of security threats.

Studies have shown that a significant number of SMEs have experienced cyberattacks, highlighting the need for effective risk assessment [7], [8], [17]. However, only a small percentage of SMEs actively engage in information and communication technology (ICT) risk assessments [8]. Since the challenges posed by information security in SMEs are complex and multifaceted, this indicates a gap in cybersecurity awareness and preparedness among SMEs. To address this gap, SMEs need a tailored metric or model that not only acknowledges their unique constraints but also equips them to address the ever-evolving cyber threats effectively [7], [17], [18]. The model should consider factors such as security importance, implementation challenges, and external influences on SME executives’ perceptions of security [19]. Additionally, an ISRA program can help identify areas of improvement and guide the development of security awareness programs [20], [21].

Within the domain of information technology and computer security, ISRA involves scrutinizing and evaluating an organization’s security controls, policies, and procedures [21]. This practice is indispensable for ensuring the effectiveness and compliance of security measures with relevant laws and standards. Essentially, ISRA acts as a sentinel, identifying vulnerabilities, assessing risks, and verifying compliance, thus fortifying an organization’s defenses against cyberattacks [2]. Research conducted in the field of ISRA has generated invaluable insights into the effectiveness of auditing practices within organizations, with a particular focus on SMEs [8]. These insights serve as a basis for improving assessment procedures. Existing studies have shed light on the challenges that SMEs face in maintaining their cybersecurity, including limited resources and expertise [18], [22]. Simultaneously, these studies have highlighted the potential advantages of conducting effective security assessments. Nevertheless, a significant gap persists in the current body of research, specifically concerning the application of security assessments and audits in SMEs, given their unique circumstances and constraints [18], [23]. This necessitates the development of an ISRA program that is purpose-built for SMEs. Such a program should be automated to optimize its operational capabilities and, most importantly, capable of providing a security level that empowers SMEs to enhance their information security posture.

In this paper, we investigate ISRA data derived from information security or *keamanan informasi* (KAMI) index [24], a framework developed by the Indonesian agency for security from ISO 27000. Artificial intelligence (AI) and machine learning are pivotal in this approach. These technologies enable the development of intelligent systems that can adapt to evolving threats. This paper aims to make substantial contributions to the field of ISRA that harnesses the power of machine learning to offer timely, cost-effective, and personalized risk assessments on SMEs. By addressing the existing research gap, this study seeks to provide SMEs with a comprehensive understanding of the benefits, challenges, and best practices related to security assessment tailored to their unique context. This, in turn, will empower these enterprises to enhance their cybersecurity defenses against the ever-evolving landscape of cyber threats.

2. METHOD

This study employed a data science approach with a machine learning perspective, as demonstrated by [25], [26]. The research framework integrates statistics, computer science, programming, and domain expertise to collect, process, and analyze data to gain insights or address specific issues. The study utilizes machine learning algorithms and analytical tools for data processing and comprehension. The absence of a unified theory regarding dynamics cybersecurity introduces both challenges and opportunities for machine learning-driven and data-centric methodologies aimed at comprehending intricate systems [27]. These models are required to represent real-world systems accurately, deduce system attributes, and adapt based on expert insights and observations to yield practical advantages.

2.1. Research context

In the context of this study, we have directed our attention towards the challenges of utilizing information security programs, particularly in the SMEs of Indonesia [16]. Integrating AI into ISRA for SMEs is becoming increasingly important due to its potential to enhance efficiency in non-financial auditing contexts like cybersecurity [22]. AI's ability to analyze unstructured, text-based evidence is particularly relevant in these contexts. The need to explore AI's utilization in non-financial auditing, particularly through text analysis, has gained recognition [28]. Further research is needed to identify security assessment tasks that can be automated through AI and explore the efficiency implications of assessing text-based evidence using AI.

This research aims to investigate the utilization of various machine learning algorithms to enhance the efficiency of information security assessments, specifically for SMEs. The complexity and significance of the assessment process make it an ideal subject for exploring the application of AI. This study focuses on exploring the potential use of the ISRA based on KAMI, which holds a crucial role in organizational innovation and necessitates internal security assessment. The KAMI's index is a straightforward assessment tool developed by the National Cyber and Crypto Agency or Badan Siber dan Sandi Negara (BSSN) of Indonesia [24]. Despite its simplicity, KAMI can assess and measure the completeness and maturity of information security based on ISO/IEC 27001 standards [29]. Thus, this study uses KAMI's index from BSSN as the central point for designing an AI-augmented assessment, addressing the need for further exploration in this field.

As illustrates in Figure 1, KAMI encompasses five dimensions: governance, risk management, security framework, asset management, and security technology [10]. While it does not evaluate the effectiveness of existing security measures, it offers a quick overview of an organization's readiness and preparedness in terms of information security. The assessment results, aligned with COBIT or CMMI maturity levels as a reference (https://www.isaca.org), can be used to map and rate an organization's information security [30], [31].

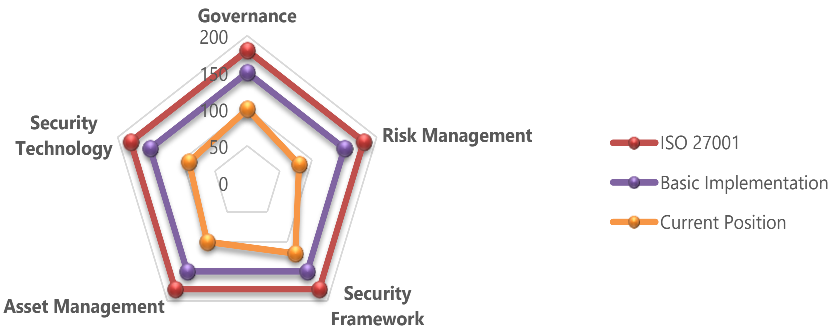

Figure 1. Scopes of KAMI's dimensions [16]

It is crucial to recognize that although KAMI is based on current standards and best practices for businesses, each sector should adopt its implementation to align with its unique circumstances and requirements. Given that organizations face specific risks, threats, and vulnerabilities, the success of implementing KAMI practices may vary. Therefore, KAMI should not be considered a one-size-fits-all strategy for all enterprises, especially those managing critical infrastructure. Consequently, this research has focused on exploring information security attributes derived from KAMI to assist SMEs in better managing their cybersecurity risks.

2.2. Research framework

The research framework was rigorously built to meet a specific research question: developing a machine learning classification model and subsequent assessment of its efficiency and effectiveness compared to manual assessments. This evaluation is carried out during the comparative phase. To determine the model's effectiveness, the results of its assessments are evaluated to those of a human auditor. This approach aligns with the conventional AI assessment method by comparing its outcomes with human performance on identical tasks. The research framework is divided into three distinct phases, as shown in Figure 2.

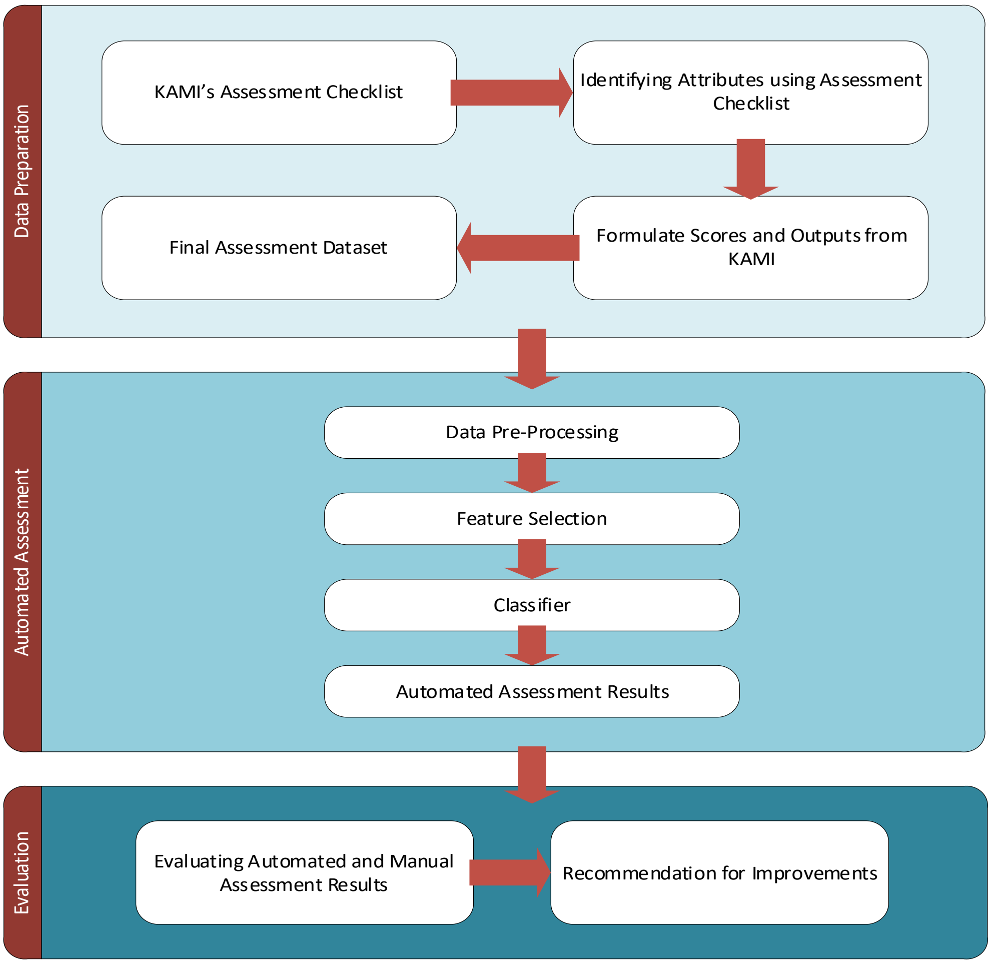
Data Preparation
KAMI's Assessment Checklist
Identifying Attributes using Assessment Checklist
Formulate Scores and Outputs from KAMI
Final Assessment Dataset
Automated Assessment
Data Pre-Processing
Feature Selection
Classifier
Automated Assessment Results
Evaluation
Evaluating Automated and Manual Assessment Results
Recommendation for Improvements

Figure 2. Research framework

2.2.1. Phase 1: Data preparation

This initial phase encompasses several crucial steps. Firstly, it involves the identification of the representations of KAMI within the established framework. Subsequently, the questions originating from KAMI are aligned with these representations. This alignment serves the purpose of pinpointing essential attributes within the assessment checklist. Following the identification of these significant attributes, an assessment checklist is meticulously crafted. This checklist is constructed based on the attributes' relevance and pertinence to the assessment process. An additional aspect of this phase is the assignment of scores to each question in the assessment checklist. These scores serve as quantitative indicators, signifying the level of compliance with KAMI for each specific question. After completing the aforementioned processes, the resulting dataset is painstakingly recorded. This dataset serves as the foundation for the succeeding phases of the research.

2.2.2. Phase 2: Automated assessment

The second phase of our research consists of two independents but connected tasks: automated and manual assessment. These tasks collectively evaluate respondents' compliance with the established criteria. The first task, which is an automated assessment, requires the use of machine learning algorithms. This automated mechanism is responsible for assigning compliance scores to respondents based on their responses and data patterns. This research utilizes various machine learning algorithms to facilitate this evaluation, providing an objective assessment of compliance. Concurrently, the second task involves assessment by human auditors. These auditors use a Likert-type scale to measure respondents' compliance. Compliance scores are awarded to each respondent based on human judgment and knowledge. This parallel manual assessment process offers a complementary perspective on compliance, considering the nuanced aspects that may not be captured by automated assessment alone.

2.2.3. Phase 3: Evaluation

The third and final phase of our study is dedicated to critically evaluating the assessment process. This phase consists of two primary components. The first aspect involves a comprehensive examination of the results obtained through both automated and manual assessments. The outcomes from the manual evaluation, carried out by human auditors, are meticulously compared with those generated through the automated evaluation. This comparative analysis serves as a pivotal step in assessing the overall effectiveness of the assessment approach. It sheds light on the alignment and disparities between human and automated assessment results, providing valuable insights into the performance of the AI-based evaluation. Also, the last phase encompasses a discussion focused on potential recommendations for enhancing the assessment process. These recommendations aim to refine and optimize the assessment methodology, taking into account the findings and lessons learned from the comparative evaluation of the automated assessments.

2.3. Dataset description

This research uses a synthetic dataset from assessment responses using a checklist obtained from KAMI's framework. The comprehensive dataset is organized into three distinct components:

- Scale of electronic systems. This section describes the importance of electronic systems owned by the organization, categorized into three labels: low, high, and strategic.
- Assessment score results. This section incorporates scores from the assessment responses across five dimensions of KAMI. The scores for each component exhibit a wide range, contingent on the complexity of the questions, falling within the intervals of [0,1,2,3], [0,2,4,6], or [0,3,6,9].
- Final assessment outcomes. The main focus of this section is the classification of assessment results into three distinct classes: good, good enough, and provides basic framework.

This classification is predicated on the comprehensive assessment results, which are subdivided into the three categories mentioned above to facilitate understanding. It is worth mentioning that the gathered dataset is exceptionally balanced, comprising 510 data points, with 170 data points allocated equitably to each class. It is crucial to highlight this equilibrium since it provides a strong foundation for future investigations and interpretations.

2.4. Machine learning models

This study aimed to achieve maximum accuracy by utilizing three supervised learning algorithms: support vector machine, random forest, and gradient boosting. The SVM method operates by constructing hyperplanes in a multidimensional space, effectively segregating instances with different class labels. This classification approach maximizes the margin between support vectors through the utilization of radial basis function (RBF) kernels. The SVM is configured with the following parameters: cost=1, regression loss epsilon=0.1, numerical tolerance =0.001, and 10,000 iterations.

Random forest integrates the predictions of various decision tree algorithms to generate a final prediction. DT is a machine learning algorithm employed for regression or classification. Classification will be the sole focus of this paper, as it is the primary objective of the security level assessment. Furthermore, we fine-tuned the random forest model by employing 100 trees.

Conclusively, our study incorporates gradient boosting, a technique that assembles an ensemble of shallow trees sequentially, with each subsequent tree enhancing the performance of its predecessor. For this purpose, an optimized distributed gradient boosting library called extreme gradient boosting (XGBoost) was chosen. The model employs 100 trees with a learning rate of 0.3. We adjusted the regularization parameters to optimize the model by setting lambda =1. Simultaneously, initial values for tuning tree-based parameters include a max depth of an individual tree =5, a subsample fraction for training instances =1, and a tree, level, and split value of 1 each. This all-encompassing approach enables a rigorous examination and application of these methods, establishing the groundwork for accurate and successful results.

3. RESULTS AND DISCUSSION

3.1. Performance evaluation

The investigations focus mainly on the ISRA category to evaluate the applicability of the proposed model in different situations. Meanwhile, the model's accuracy is evaluated using an approach called 5-fold cross-validation to eliminate the possibility of data partitioning. The dataset is initially partitioned into five groups before using the 5-fold cross-validation technique. The initial four groups are designated for training, while the last group is allocated for testing. During the cross-validation procedure, five separate training and test sets are employed to validate the entirety of the data. This task is performed as part of the approach. During the assessment phase, the efficacy of the model is assessed by considering its accuracy (Acc), recall (Re), precision (Pr), and F-measure (F1) values in order to gain a comprehensive understanding. The method for determining a definition for them is as follows:

$$Acc = \frac{TP+TN}{TP+FP+TN+FN} \times 100\% \tag{1}$$

$$Re = \frac{TP}{TP+FN} \times 100 \tag{2}$$

$$Pr = \frac{TP}{TP+FP} \times 100\% \tag{3}$$

$$F1 = 2 \times \frac{TP}{2\times TP+FN+FP} \times 100\% \tag{4}$$

The machine learning classifier comparison among support vector machine, random forest, and gradient boosting produced insightful results, shedding light on the nuanced performance of each algorithm. As shown in Table 1 and Figure 3, SVM emerges as the frontrunner, boasting the highest accuracy at 94.3%, a recall of 94.4%, and a precision of 94.3%. This outcome underscores SVM's proficiency in effectively classifying instances across diverse class labels, striking a balance between precision and recall, as evidenced by its F-measure of 94.2%. The trademark of SVM lies in its capacity to maximize the margin between support vectors through RBF kernels, enabling robust separation of different class labels.

Table 1. Performance comparison of different models

Model	Accuracy (%)	Recall (%)	Precision (%)	F1-score (%)
SVM	94.3	94.4	94.3	94.2
Random forest	90.6	90.7	90.6	90.4
Gradient boosting	91.8	91.7	91.8	91.7

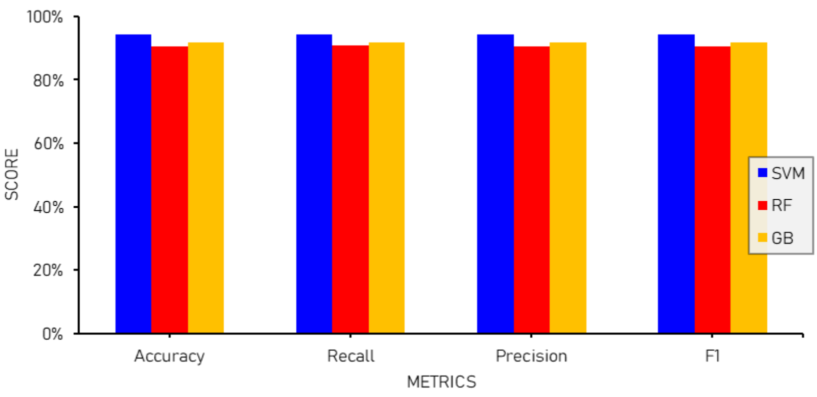

Figure 3. Performance comparison of the models

In contrast, the random forest algorithm, which utilizes the collective predictions of 100 decision trees, shows a notable level of accuracy, achieving a notable rate of 90.6%. While its recall of 90.7% suggests a notable capability to identify positive cases accurately, the precision of 90.6% highlights its prowess in recognizing negative cases. However, the F-measure of 90.4% indicates a slight compromise in achieving a balanced precision and recall, distinguishing it from the SVM's more cohesive combination.

The utilization of gradient boosting, specifically through the implementation of extreme gradient boosting with a total of 100 trees and a learning rate of 0.3, results in an accuracy rate of 91.8%. This outcome effectively demonstrates the ability of gradient boosting to enhance predictive performance sequentially. The efficiency of gradient boosting in attaining a balanced equilibrium between accuracy and recall is reinforced by the balanced precision, recall, and F-measure, all of which are at a level of 91.7%. The distinctive characteristic of gradient boosting is its iterative ensemble methodology, in which each successive tree capitalizes on its predecessor's qualities, enhancing the overall predictive capability of the model.

3.2. Main findings and contributions

In this experiment, the SVM model yielded an astounding accuracy rate of 94.3%. This score illustrates how well the model predicts the future and shows how machine learning has the ability to transform information security assessment. This high accuracy rate is a positive indication of the model's capability in a world where safeguarding sensitive data is essential. The remarkable recall and precision rates of the SVM of 94.4% and 94.3%, respectively, are highlighted in the paper. The results show how well the model can detect significant cases while lowering false positives. The outstanding precision ensures that the identifications made by the model are reliable, and the high recall shows that it accurately detects pertinent facts. In ISRA, accuracy is essential because even one false positive result can have grave consequences.

The findings also have important implications where it opens up new avenues for research in the area of ISRA and provide confidence in the machine learning model's practical use. The model's ability to maintain high accuracy while improving memory and precision provides compelling evidence in favor of its widespread adoption. More robust security measures and increased operational efficiencies could come from this.

Utilizing the KAMI framework for evaluation allows us to match our research with an internationally accepted benchmark. Based on the ISO 27001 standard, KAMI has significant implications for ISRA, affecting the more extensive information security landscape. This study 's validation of KAMI's assessment checklist underscores its significance as a noteworthy addition. The analysis also emphasizes the need for increased effectiveness as KAMI's reach expands. It is thought that applying machine learning technology is a workable strategy, specifically when dealing with unstructured evidence, a common problem in the information security industry. This study also provides a significant step forward in improving ISRA's efficiency without sacrificing the process's fundamental efficacy.

Machine learning-based assessment systems provide efficiency benefits to internal organizations by streamlining procedures and enabling comprehensive evaluations that strengthen decision-making. Information security managers, security auditors, and practitioners in charge of safeguarding critical data and systems should pay particular attention to this paper. Machine learning integration strengthens ISRA's capabilities by giving them a solid tool for evaluating big datasets and identifying potential threats and weaknesses. By highlighting the crucial components of information security and demonstrating the flexibility of machine learning in auditing, the study sets a standard and piques interest in more investigation. The potential for combining machine learning with cybersecurity is enormous since professionals in the field are prepared to use AI and machine learning to strengthen their defenses against vital assets.

4. CONCLUSION

This research evaluates the best machine learning models to classify and predict ISRA data collection. The dataset was derived from a framework designed by the Indonesian security agency based on ISO 27000, named KAMI's index. The strategy relies heavily on machine learning to enable the creation of intelligent systems that can respond to changing threats. This work seeks to make significant contributions to the field of ISRA by leveraging the power of machine learning to provide quick, cost-effective, and tailored risk assessments for SMEs. Our experiment showed that the SVM model obtained an astonishing 94.3% accuracy, proving its potential to change information security evaluation. The model's strong recall and precision rates show that it can discover noteworthy cases while minimizing false positives. This is critical in ISRA, where accuracy is paramount. The study's implementation of the KAMI framework is consistent with the ISO 27001 standard, which emphasizes its importance in the information security landscape. The report also emphasizes the need for greater effectiveness as KAMI's reach grows. Machine learning-based assessment systems can increase ISRA efficiency by reducing procedures and allowing for comprehensive evaluations.

ACKNOWLEDGEMENTS

This research has been supported by the Internal of Excellence Research Grant, Research Department of Universitas Amikom Yogyakarta Indonesia, with a contract number: 8271/KONTRAK-LPPM/AMIKOM/X/2022 (August, 29th 2023).

REFERENCES

[1] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, 2019, doi: 10.3390/info10040122.

[2] F. A. Shaikh and M. Siponen, "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity," *Computers and Security*, vol. 124, 2023, doi: 10.1016/j.cose.2022.102974.

[3] P. Cheimonidis and K. Rantos, "Dynamic risk assessment in cybersecurity: a systematic literature review," *Future Internet*, vol. 15, no. 10, 2023, doi: 10.3390/fi15100324.

[4] N. Kaloudi and L. I. Jingyue, "The AI-based cyber threat landscape: A survey," *ACM Computing Surveys*, vol. 53, no. 1, 2020, doi: 10.1145/3372823.

[5] K. AL-Dosari and N. Fetais, "Risk-management framework and information-security systems for small and medium enterprises (SMEs): a meta-analysis approach," *Electronics*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173629.

[6] H. Salin and M. Lundgren, "Towards agile cybersecurity risk management for autonomous software engineering teams," *Journal of Cybersecurity and Privacy*, vol. 2, no. 2, pp. 276–291, 2022, doi: 10.3390/jcp2020015.

[7] M. Calvo and M. Beltrán, "A model for risk-based adaptive security controls," *Computers and Security*, vol. 115, 2022, doi: 10.1016/j.cose.2022.102612.

[8] A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, "Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors," *Risk Analysis*, vol. 43, no. 10, pp. 2082–2098, 2023, doi: 10.1111/risa.14092.

[9] A. Edegbeme-Beláz and A. Kerti, "A new approach to information security auditing in public administration," *Hadmérnök*, vol. 17, no. 3, pp. 109–131, 2022, doi: 10.32567/hm.2022.3.8.

[10] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, 2022, doi: 10.1016/j.eij.2022.03.001.

[11] D. M. Magesa and J. A. Mshana, "Assessing challenges facing implementation of information security critical success factors: a case of national examination council, Tanzania," *European Journal of Theoretical and Applied Sciences*, vol. 1, no. 5, pp. 883–897, 2023, doi: 10.59324/ejtas.2023.1(5).74.

[12] A. Kő, G. Tarján, and A. Mitev, "Information security awareness maturity: conceptual and practical aspects in Hungarian organizations," *Information Technology and People*, vol. 36, no. 8, pp. 174–195, 2023, doi: 10.1108/ITP-11-2021-0849.

[13] T. Singh, A. C. Johnston, J. D'Arcy, and P. D. Harms, "Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 3, no. 2, pp. 100–126, 2023, doi: 10.1108/ocj-06-2022-0012.

[14] E. Rostami, F. Karlsson, and E. Kolkowska, "The hunt for computerized support in information security policy management: A literature review," *Information and Computer Security*, vol. 28, no. 2, pp. 215–259, 2020, doi: 10.1108/ICS-07-2019-0079.

[15] M. Dart and M. Ahmed, "Operational shock: A method for estimating cyber security incident costs for large Australian healthcare providers," *Journal of Cyber Security Technology*, pp. 1–26, 2023, doi: 10.1080/23742917.2023.2291914.

[16] A. H. Muhammad, J. D. Santoso, and A. F. I. Akbar, "Information security investment prioritization using best-worst method for small and medium enterprises," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 1, pp. 271–280, 2023, doi: 10.11591/ijeecs.v31.i1.pp271-280.

[17] J. N. Al-Karaki, A. Gawanmeh, and S. El-Yassami, "GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3079–3095, 2022, doi: 10.1016/j.jksuci.2020.09.011.

[18] M. Van Haastrecht, B. Y. Ozkan, M. Brinkhuis, and M. Spruit, "Respite for smes: A systematic review of socio-technical cybersecurity metrics," *Applied Sciences*, vol. 11, no. 15, 2021, doi: 10.3390/app11156909.

[19] K. A. Saban, S. Rau, and C. A. Wood, "SME executives' perceptions and the information security preparedness model," *Information and Computer Security*, vol. 29, no. 2, pp. 263–282, 2021, doi: 10.1108/ICS-01-2020-0014.

[20] A. D. Veiga, "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture," *Information and Computer Security*, vol. 26, no. 5, pp. 584–612, 2018, doi: 10.1108/ICS-08-2017-0056.

[21] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers and Security*, vol. 57, pp. 14–30, 2016, doi: 10.1016/j.cose.2015.11.001.

[22] B. Y. Ozkan, M. Spruit, R. Wondolleck, and V. B. Coll, "Modelling adaptive information security for SMEs in a cluster," *Journal of Intellectual Capital*, vol. 21, no. 2, pp. 235–256, 2020, doi: 10.1108/JIC-05-2019-0128.

[23] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," *Decision Support Systems*, vol. 147, 2021, doi: 10.1016/j.dss.2021.113580.

[24] BSSN, "Indeks KAMI," *Badan Siber dan Sandi Negara*, 2019. Accessed: Mar. 19, 2024. [Online]. Available: https://bssn.go.id/indeks-kami/

[25] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

[26] F. A. Vadhil, M. L. Salihi, and M. F. Nanne, "Machine learning-based intrusion detection system for detecting web attacks," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 1, pp. 711–721, 2024, doi: 10.11591/ijai.v13.i1.pp711-721.

[27] T. W. Edgar and D. O. Manz, "Machine learning," *Research Methods for Cyber Security*, pp. 153–173, 2017, doi: 10.1016/b978-0-12-805349-2.00006-6.

[28] D. P. Alagarswamy *et al.*, "Towards audit requirements for AI-based systems in mobility applications," *International Conference on Information Systems Security and Privacy*, pp. 339–348, 2023, doi: 10.5220/0011619500003405.

[29] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," *International Journal on Informatics Visualization*, vol. 4, no. 4, pp. 225–230, 2020, doi: 10.30630/joiv.4.4.482.

[30] R. Ehrensperger, C. Sauerwein, and R. Breu, "A maturity model for digital business ecosystems from an IT perspective," *Journal*

of Universal Computer Science, vol. 29, no. 1, pp. 34–72, 2023, doi: 10.3897/jucs.79494.

[31] J. Iden, T. R. Eikebrokk, and M. Marrone, “Process reference frameworks as institutional arrangements for digital service innovation,” *International Journal of Information Management*, vol. 54, 2020, doi: 10.1016/j.ijinfomgt.2020.102150.

BIOGRAPHIES OF AUTHORS

Alva Hendi Muhammad received his Ph.D. in Information Technology from the University of Technology Sydney in Australia. He currently works as an assistant professor in the Department of Informatics of the Postgraduate Program at Universitas Amikom Yogyakarta in Indonesia. He has over 10 years of experience teaching at both the undergraduate and postgraduate levels in an educational institution. Some of his research has been published in academic journals and presented at conferences. His research interests include modeling decision and expert systems, incorporating artificial intelligence with engineering and educational technology, and also information security. He can be contacted at email: alva@amikom.ac.id.

Asro Nasiri is currently pursuing a doctoral degree in Informatics. Previously, he has a solid 13-year career in the aircraft sector as an avionic engineer. He has spent more than ten years instructing and promoting innovation at Universitas Amikom Yogyakarta. He was the head of the Innovation Center at Universitas Amikom Yogyakarta, where he encouraged creativity and entrepreneurship among students and professors. He also worked as Director at Amikom Business Park, where he promoted collaboration and economic progress. His enthusiasm for technology governance drove him to create IT master plans and undertake IT governance audits. He has also served as a commissaris at an IT training institution and as the Co-Founder and Chief Operating Officer of FROGS Indonesia. His professional background displays a dedication to generating innovation, encouraging collaboration, and leveraging technology to move enterprises forward. He can be contacted at email: asro.nasiri@amikom.ac.id.

Agung Harimurti holds a Master of Computer Science and Ph.D. in Information Management from Gadjah Mada University, besides several short studies at Oxford Internet Institute, Cornell University (USA), Tsing Hua University (China), and Griffith University, Australia. He is currently lecturing with the Master of Informatics at Universitas Amikom Yogyakarta, Indonesia. He has become a reviewer of several international journals, such as the Asian Journal of Economics, Business, and Accounting, the Asian Journal of Advances in Research, and the Journal of Global Economics, Management, and Business Research. He is also a member of the Indonesian Computer, Electronics, and Instrumentation Support Society (IndoCEISS) and the Association of Indonesian Informatics Experts (IAII). His research areas of interest include cyber security, information management, financial technology, and e-services. He can be contacted at email: harimurti@amikom.ac.id.