Designing a Fuzzy Inference System for Evaluating Information Security Policy Management in Organizations

Ameneh Khadivar*[1], Khatere Ghorbani Moghadam[2], Hanieh Siahsarani[3], Marzieh Shaverdi[4]

Abstract

In recent years, the rapid growth of cyber threats and the increasing dependence of organizations on information technology have highlighted the importance of information security policy management. However, traditional approaches to evaluating information security policies rely largely on deterministic methods, which may be less effective in addressing uncertainty and the complexity of contemporary organizational environments. This study aimed to design a fuzzy inference system for evaluating information security policy management. After reviewing recognized information security standards and frameworks, the SANS Institute policy documents were selected as the primary source for extracting evaluation indicators. Subsequently, key factors affecting information security policy management were identified, and fuzzy if–then rules were developed based on the documents and expert judgments. A total of 218 policy statements across 10 domains were identified and evaluated by 15 experts. The content validity of the instrument was confirmed with a CVR of 0.73, while its reliability was supported by an overall Cronbach's alpha of 0.803. A Mamdani-based fuzzy inference system was then implemented in MATLAB using the Fuzzy Logic Toolbox. The final model consisted of 10 fuzzy inference subsystems and one comprehensive system, incorporating more than 400 fuzzy rules and evaluating organizational information security policy management at three levels: weak, medium, and strong. The results indicate that the proposed framework can transform qualitative evaluations and expert judgments into a quantitative and interpretable structure and can serve as a decision-

[1] Associate Professor, Department of Management, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran. (Corresponding Author). Email: a.khadivar@alzahra.ac.ir

[2] Assistant Professor, Mosaheb Institute of Mathematics, Kharazmi University, Tehran, Iran.

[3] M.Sc. Graduate in Technology Management, Faculty of Social Sciences and Economics, Alzahra University, Tehran, Iran.

[4] Faculty Member, Department of Financing and Economics of Science, Technology and Innovation, National Research Institute for Science Policy (NRISP), Tehran, Iran. Email: shaverdi@nrisp.ac.ir

support tool for identifying areas requiring improvement in information security policy management.
Keywords: Information Security, Information Security Policy, Fuzzy Logic, Fuzzy Inference System, Information Security Management

1. Introduction

Information security is a fundamental requirement for organizational continuity as organizations increasingly depend on digital systems and information assets. Security incidents may result from cyberattacks, unauthorized access, information disclosure, human error, and inadequate compliance with security requirements. Information security policies provide formal rules for the use, protection, access, and management of information assets; however, the existence of a policy document alone does not guarantee effective security. Policy effectiveness depends on how policies are implemented, monitored, reviewed, updated, and followed by employees. Many related factors, including employee awareness, implementation quality, management support, compliance, and organizational readiness, are qualitative and uncertain. Deterministic evaluation approaches may not adequately represent linguistic judgments such as “weak awareness,” “moderate compliance,” or “strong implementation.” Fuzzy logic can represent such ambiguity through graded membership and approximate reasoning. Accordingly, this study aimed to design a fuzzy inference system for evaluating information security policy management in organizations. The framework converts expert judgments and operational policy statements into an interpretable computational structure that classifies the overall status of policy management as weak, medium, or strong and supports the identification of areas requiring improvement.

2. Materials and Methods

The study was applied in terms of its purpose and developmental in nature. The research process consisted of two main stages: identifying evaluation components and indicators, and extracting expert knowledge for designing the fuzzy inference system. First, documentary and library studies were conducted using scientific articles, books, information security standards, recognized security frameworks, and specialized policy documents. The information security policy documents of the SANS Institute were selected as the primary operational source for extracting policy statements because they contain implementable requirements that can be translated into linguistic conditions and if–then rules. SANS was not treated as a formal information security management standard. The extracted domains were conceptually mapped to ISO/IEC 27001/27002 and the NIST

Cybersecurity Framework, with additional consideration of COBIT 2019. This mapping did not constitute a formal compliance audit. Second, a questionnaire was developed based on the identified components and policy statements. The statistical population consisted of experts, specialists, and managers in information technology and information security with relevant knowledge and experience in policy management. A non-probability snowball sampling method was used, and 15 experts participated. Their judgments were expressed using three linguistic levels: weak, medium, and strong. Content validity was assessed using Lawshe's Content Validity Ratio (CVR). Thirteen of the 15 experts considered the questionnaire items appropriate and useful, producing a CVR of 0.73, above the minimum acceptable value of 0.49 for 15 evaluators. Reliability was assessed using Cronbach's alpha, which was 0.803. A separate inter-rater agreement statistic was not calculated; therefore, the reported CVR reflects content validity rather than expert agreement. A Mamdani fuzzy inference system was selected because of its rule-based structure and interpretability. The model was implemented in MATLAB using the Fuzzy Logic Toolbox. The inference process included fuzzification, rule activation and aggregation, and centroid defuzzification. The outputs of the subsystems and the comprehensive system were represented by weak, medium, and strong. In MATLAB, the output domain was defined over [0,1] and triangular membership functions were used. The architecture consisted of 10 fuzzy subsystems whose outputs were entered into a comprehensive fuzzy system.

3. Results and discussion

The review of SANS policy documents identified 218 policy statements across 10 information security domains: artificial intelligence use, digital signature, business email, Internet use, mobile employees, passwords, remote access, routers and switches, servers, and wireless communications. After content review and expert evaluation, 82 statements were classified as weak, 72 as medium, and 64 as strong. Each statement was converted into an evaluable condition and then into a linguistic if–then rule within the corresponding subsystem. At the second level, the output of each of the 10 subsystems became an input to the comprehensive fuzzy system. The implemented comprehensive system contained 421 rule rows representing 404 unique antecedent combinations. The final output represented the overall status of information security policy management at one of the three linguistic levels. For example, when five subsystem outputs were weak, three were medium, and two were strong, the comprehensive model classified the final status as weak. MATLAB decision-surface analysis showed continuous changes in the

overall output as subsystem values changed, demonstrating that the fuzzy approach can represent intermediate states rather than forcing conditions into rigid boundaries.

Table 1. Summary of key model development results

Indicator	Result
Expert participants	15
Initial policy statements	218
Information security domains	10
Weak / Medium / Strong statements	64 / 72 / 82
CVR	0.73
Cronbach's alpha	0.803
Fuzzy architecture	10 subsystems + 1 comprehensive system
Comprehensive rule base	421 rule rows; 404 unique antecedent combinations
Final output levels	Weak, Medium, Strong
Implementation	MATLAB Fuzzy Logic Toolbox
Defuzzification	Centroid

The findings indicate that the fuzzy inference approach can integrate multiple qualitative security-policy dimensions within a unified and interpretable framework. Its main practical value is to help managers identify weak or medium policy areas and prioritize corrective or control actions. The conceptual alignment with ISO/IEC 27001/27002, NIST CSF, and COBIT 2019 may facilitate organizational interpretation of the model results, although it should not be considered a formal compliance assessment.

4. Conclusion

This study developed a Mamdani fuzzy inference system for evaluating information security policy management by combining security-policy documents, expert knowledge, linguistic variables, membership functions, and if–then rules. The model transforms qualitative judgments into an interpretable decision-support structure and provides an overall assessment of policy management as weak, medium, or strong. The findings suggest that fuzzy inference is suitable for this problem because many relevant factors are linguistic and uncertain. The model has several limitations. Its rule base was developed from the judgments of 15 experts, SANS was the primary operational source of policy statements, and no independent operational data from a real organization were used for field validation. Future studies should validate the model in different organizations and industries, involve larger and more diverse expert groups, perform more

detailed mappings to security standards, compare Mamdani and Sugeno systems and other decision-making methods, investigate type-2 fuzzy logic, and explore machine-learning approaches for updating the rule base. Overall, integrating expert knowledge, information security documents, and Mamdani fuzzy inference provides a flexible and interpretable framework for evaluating information security policy management and supporting organizational decision-making.

in Press

طراحی سیستم استنتاج فازی جهت ارزیابی مدیریت خط‌مشی امنیت اطلاعات در سازمان‌ها

آمنه خدیور *[۱]، خاطره قربانی‌مقدم[۲]، حانیه سیاه‌سرانی[۳]، مرضیه شاوردی[٤]

چکیده

در سال‌های اخیر، رشد سریع تهدیدهای سایبری و افزایش وابستگی سازمان‌ها به فناوری اطلاعات، اهمیت مدیریت خط‌مشی امنیت اطلاعات را بیش از پیش نمایان ساخته است. بااین‌حال، روش‌های سنتی ارزیابی خط‌مشی‌های امنیت اطلاعات عمدتاً مبتنی بر رویکردهای قطعی بوده و در مواجهه با عدم قطعیت و پیچیدگی‌های محیط‌های نوین، کارایی محدودی دارند. در پژوهش حاضر که با هدف طراحی سیستم استنتاج فازی برای ارزیابی مدیریت خط‌مشی امنیت اطلاعات انجام شده، پس از بررسی استانداردها و چارچوب‌های معتبر امنیت اطلاعات، اسناد خط‌مشی مؤسسه SANS به‌عنوان منبع اصلی استخراج شاخص‌ها انتخاب شد. در مرحله بعد با شناسایی عوامل کلیدی مؤثر بر مدیریت خط‌مشی امنیت اطلاعات و طراحی قواعد فازی (اگر–آنگاه) بر اساس اسناد و نظرات خبرگان، ۲۱۸ در ۱۰ حوزه شناسایی و با استفاده از نظر ۱۵ خبره ارزیابی شد. روایی محتوایی ابزار با مقدار CVR برابر ۰.۷۳ و پایایی آن با آلفای کرونباخ کل برابر ۰.۸۰۳ تأیید شد. در ادامه، سیستم استنتاج فازی مبتنی بر مدل ممدانی با استفاده از جعبه‌ابزار منطق فازی در محیط MATLAB پیاده‌سازی شد. مدل نهایی از ۱۰ زیرسیستم استنتاج فازی و یک سیستم جامع تشکیل شد و بیش از ۴۰۰ قاعده فازی در پایگاه قواعد آن به‌کار گرفته شد که وضعیت مدیریت خط‌مشی امنیت اطلاعات سازمان را در سه سطح ضعیف، متوسط و قوی ارائه می‌کند. نتایج نشان می‌دهد چارچوب پیشنهادی با فراهم‌سازی امکان تبدیل ارزیابی‌های کیفی و قضاوت‌های خبرگان به ساختاری کمّی و قابل تفسیر، می‌تواند به‌عنوان ابزار پشتیبان تصمیم‌گیری برای شناسایی حوزه‌های نیازمند بهبود در مدیریت خط‌مشی امنیت اطلاعات مورد استفاده قرار گیرد.

واژه‌های کلیدی: *امنیت اطلاعات، خط‌مشی امنیت اطلاعات، منطق فازی، سیستم استنتاج فازی، مدیریت امنیت اطلاعات*

۱. دانشیار گروه مدیریت، دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران. a.khadivar@alzahra.ac.ir (نویسنده مسئول).

۲. استادیار موسسه تحقیقات ریاضی دکتر مصاحب، دانشگاه خوارزمی، تهران، ایران. k.ghorbani@khu.ac.ir .

۳. فارغ‌التحصیل کارشناسی ارشد مدیریت فناوری دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، تهران، ایران.

۳. عضو هیئت علمی گروه تأمین مالی و اقتصاد علم، فناوری و نوآوری، مؤسسه تحقیقات سیاست علمی کشور، تهران. shaverdi@nrisp.ac.ir.

٤. عضو هیئت علمی گروه تأمین مالی و اقتصاد علم، فناوری و نوآوری، مؤسسه تحقیقات سیاست علمی کشور، تهران. shaverdi@nrisp.ac.ir.

طبقه‌بندی موضوعی: Security Policy, Security Governance, Security and Privacy، Artificial Intelligence، Fuzzy Logic.

مقدمه

در سال‌های اخیر، گسترش فناوری اطلاعات و افزایش وابستگی سازمان‌ها به سامانه‌های دیجیتال، امنیت اطلاعات را به یکی از مؤلفه‌های اساسی تداوم فعالیت سازمان‌ها تبدیل کرده است. دارایی‌های اطلاعاتی در معرض تهدیدهایی مانند حملات سایبری، دسترسی غیرمجاز، افشای اطلاعات و خطاهای انسانی قرار دارند که می‌توانند پیامدهای مالی، عملیاتی، اعتباری و حقوقی به همراه داشته باشند. ازاین‌رو، تدوین، اجرا و ارزیابی مناسب خط‌مشی‌های امنیت اطلاعات از الزامات مهم حفاظت از دارایی‌های سازمانی است (بلگورجو، کاووس‌اوغلو و بنباسات[1]، ۲۰۱۰).

صرف تدوین خط‌مشی امنیتی، تضمین‌کننده امنیت سازمان نیست و اثربخشی آن به نحوه اجرا، پایش، به‌روزرسانی و میزان پایبندی کارکنان وابسته است. عدم رعایت خط‌مشی‌های امنیت اطلاعات از عوامل مهم رخدادهای امنیتی محسوب می‌شود (سیپونن و ونس[2]، ۲۰۱۰) و خطاهای انسانی، ضعف آگاهی و شناخت ناکافی کارکنان نیز می‌تواند آسیب‌پذیری سازمان را افزایش دهد (پاهنیلا، سیپونن و محمود[3]، ۲۰۰۷). مطالعات پیشین نیز بر اهمیت این موضوع تأکید کرده‌اند؛ کاسولا، پرزیوسی، راک و تروپانو[4] (۲۰۰۵: ۱۷۲) با استفاده از مدل تجمیع فازی، چارچوبی برای تحلیل، مقایسه و طبقه‌بندی خط‌مشی‌ها برحسب سطوح امنیتی ارائه کردند. سهرابی‌صفا، ون‌سولمز و فرنل[5] (۲۰۱۶: ۷۵) نشان دادند اشتراک دانش امنیت اطلاعات، همکاری، مداخله و تجربه بر نگرش نسبت به رعایت خط‌مشی امنیت اطلاعات اثر معنادار دارند و تعهد و هنجارهای شخصی نیز بر این نگرش اثرگذارند. همچنین، العُتیبی، فرنل و کلارک[6] (۲۰۱۶: ۳۵۴–۳۵۵) بر اهمیت آگاهی، آموزش و عوامل فرهنگی در رفتار مرتبط با رعایت خط‌مشی امنیت اطلاعات تأکید کردند.

با وجود این، ارزیابی مدیریت خط‌مشی امنیت اطلاعات همچنان با چالش مواجه است؛ زیرا بسیاری از عوامل مؤثر بر آن، مانند آگاهی کارکنان، کیفیت اجرای خط‌مشی، میزان انطباق و آمادگی سازمان، ماهیتی کیفی و زبانی دارند. روش‌های مبتنی بر مقادیر قطعی، انعطاف کافی برای نمایش

---

[1] Bulgurcu, Cavusoglu, & Benbasat
[2] Siponen & Vance
[3] Pahnila, Siponen, & Mahmood
[4] Casola, Preziosi, Rak, & Troiano
[5] Sohrabi Safa, Von Solms, & Furnell
[6] Alotaibi, Furnell, & Clarke

مفاهیمی مانند «آگاهی بالا»، «انطباق متوسط» یا «اثربخشی پایین» ندارند. منطق فازی با امکان نمایش درجات مختلف عضویت و استدلال تقریبی، ابزار مناسبی برای مدل‌سازی این نوع عدم قطعیت و قضاوت‌های انسانی فراهم می‌کند (زاده[1]، ۱۹۷۸: ۳).

بر این اساس، هدف پژوهش حاضر طراحی یک سیستم استنتاج فازی برای ارزیابی مدیریت خط‌مشی امنیت اطلاعات در سازمان‌ها است. در این پژوهش، پس از بررسی منابع، استانداردها و چارچوب‌های مرتبط، اسناد خط‌مشی مؤسسه سنس[2] به‌عنوان یکی از منابع شناسایی مؤلفه‌های مورد ارزیابی استفاده شده و با بهره‌گیری از دانش خبرگان و قواعد زبانی «اگر–آنگاه»، یک سیستم استنتاج فازی مبتنی بر مدل ممدانی طراحی و در محیط MATLAB پیاده‌سازی شده است. این رویکرد امکان تبدیل قضاوت‌های کیفی خبرگان به ساختاری قابل محاسبه و تفسیر را فراهم کرده و می‌تواند به‌عنوان ابزار پشتیبان تصمیم‌گیری برای شناسایی حوزه‌های نیازمند بهبود و اولویت‌بندی اقدامات اصلاحی مورد استفاده قرار گیرد.

در این پژوهش، امنیت اطلاعات به حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات و سایر ویژگی‌های مرتبط با آن اطلاق می‌شود (ایزو/آی ای سی[3]، ۲۰۲۶) و خط‌مشی بیان رسمی جهت‌گیری سازمان در حوزه موردنظر است. همچنین، الزامات مربوط به استقرار و مدیریت سیستم مدیریت امنیت اطلاعات براساس ISO/IEC 27001:2022 و راهنمای کنترل‌های امنیت اطلاعات براساس ISO/IEC 27002:2022 مورد توجه قرار گرفته‌اند (ISO/IEC 27001, 2022; ISO/IEC 27002, 2022). خط‌مشی امنیت اطلاعات نیز مجموعه‌ای از قواعد و الزامات رسمی برای نحوه دسترسی، استفاده و حفاظت از دارایی‌های اطلاعاتی سازمان است (العتیبی و همکاران، ۲۰۱۶: ۳۵۲). منطق فازی چارچوبی برای نمایش مفاهیم مبهم با درجات مختلف عضویت است (زاده، ۱۹۷۸: ۳) و سیستم استنتاج فازی با استفاده از متغیرهای زبانی، توابع عضویت و قواعد «اگر–آنگاه»، روابط میان ورودی‌ها و خروجی‌ها را از طریق فازی‌سازی، استنتاج و فازی‌زدایی مدل می‌کند (لوگاناثان، راماکریشنان، ساتیامورتی و آزاماتولا[4]، ۲۰۲۴: ۴). در پژوهش حاضر، سیستم ممدانی به دلیل ساختار قاعده‌محور، تفسیرپذیری و تناسب آن با دانش زبانی خبرگان انتخاب شده است.

---

[1] Zadeh
[2] SANS Institute
[3] ISO/IEC
[4] Loganathan, Ramakrishnan, Sathiyamoorthy, & Azamathulla

in Press

مبانی نظری و توسعه فرضیه‌ها

امنیت اطلاعات و خط‌مشی امنیت اطلاعات

امنیت اطلاعات به حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات و سایر ویژگی‌های مرتبط با آن اطلاق می‌شود (ایزو/آی ای سی، ۲۰۲۶) و خط‌مشی بیان رسمی جهت‌گیری سازمان در حوزه موردنظر است. همچنین، الزامات مربوط به استقرار و مدیریت سیستم مدیریت امنیت اطلاعات براساس ISO/IEC 27001:2022 و راهنمای کنترل‌های امنیت اطلاعات براساس ISO/IEC 27002:2022 مورد توجه قرار گرفته‌اند (ISO/IEC 27001, 2022; ISO/IEC 27002, 2022). محرمانگی به جلوگیری از دسترسی افراد غیرمجاز به اطلاعات، یکپارچگی به حفظ صحت و کامل بودن اطلاعات و دسترس‌پذیری به امکان استفاده افراد مجاز از اطلاعات و منابع در زمان مورد نیاز اشاره دارد.

یکی از ابزارهای مهم سازمان‌ها برای تحقق اهداف امنیت اطلاعات، تدوین و اجرای خط‌مشی‌های مناسب است. خط‌مشی به‌طور کلی بیانگر نیت و جهت‌گیری رسمی مدیریت سازمان در خصوص یک موضوع مشخص است (ایزو/آی ای سی، ۲۰۲۶). بر این اساس، خط‌مشی امنیت اطلاعات مجموعه‌ای از قواعد، الزامات، دستورالعمل‌ها و رویه‌های رسمی است که نحوه استفاده، حفاظت، دسترسی و مدیریت دارایی‌های اطلاعاتی سازمان را مشخص می‌کند. این خط‌مشی‌ها تعیین می‌کنند که چه رفتارهایی در ارتباط با دارایی‌های اطلاعاتی قابل قبول و چه رفتارهایی غیرقابل قبول هستند و کارکنان و کاربران سازمان موظف‌اند در چارچوب آن‌ها عمل کنند. براساس اسناد مؤسسه سنس، خط‌مشی امنیتی معمولاً سندی رسمی است که الزامات و قواعد مشخصی را در یک حوزه خاص از امنیت اطلاعات یا امنیت شبکه تعیین می‌کند. چنین خط‌مشی‌هایی یکی از ابزارهای رسمی کنترل امنیت اطلاعات محسوب می‌شوند و نقش مهمی در مشخص‌کردن مسئولیت‌ها، حدود دسترسی و رفتار مورد انتظار کاربران ایفا می‌کنند العتیبی و همکاران (۲۰۱۶). بنابراین؛ اثربخشی امنیت اطلاعات در یک سازمان تنها به وجود ابزارها و فناوری‌های امنیتی وابسته نیست، بلکه نحوه تدوین، اجرا، نظارت و به‌روزرسانی خط‌مشی‌های امنیتی نیز در این زمینه اهمیت اساسی دارد.

مدیریت خط‌مشی امنیت اطلاعات

مدیریت خط‌مشی امنیت اطلاعات فرایندی فراتر از تدوین یک سند امنیتی است و مجموعه فعالیت‌های مرتبط با طراحی، تصویب، ابلاغ، اجرا، پایش، بازنگری و به‌روزرسانی خط‌مشی‌های

امنیتی را شامل می‌شود. هدف از این فرایند آن است که الزامات امنیت اطلاعات در تمام سطوح سازمان به‌صورت منسجم اجرا شده و رفتار کارکنان با اهداف امنیتی سازمان همسو شود.

اثربخشی خط‌مشی‌های امنیت اطلاعات تحت تأثیر عوامل متعددی قرار دارد. میزان آگاهی کارکنان، آموزش‌های امنیتی، حمایت مدیریت ارشد، فرهنگ امنیتی سازمان، میزان مشارکت کارکنان و سازوکارهای نظارتی از جمله عواملی هستند که می‌توانند بر میزان پذیرش و اجرای خط‌مشی‌های امنیتی اثرگذار باشند. ازاین‌رو؛ ارزیابی مدیریت خط‌مشی امنیت اطلاعات باید علاوه بر جنبه‌های فنی، مؤلفه‌های انسانی و سازمانی را نیز دربرگیرد.

یکی از چالش‌های اصلی در ارزیابی این حوزه آن است که بسیاری از عوامل مؤثر بر مدیریت خط‌مشی امنیت اطلاعات ماهیتی کیفی دارند. مفاهیمی مانند «آگاهی مناسب کارکنان»، «حمایت کافی مدیریت»، «انطباق متوسط با خط‌مشی» یا «اثربخشی بالای آموزش‌های امنیتی» را نمی‌توان همواره با مقادیر قطعی و مرزهای دقیق عددی بیان کرد. ازاین‌رو؛ استفاده از روش‌هایی که قابلیت پردازش اطلاعات زبانی، ابهام و عدم قطعیت را داشته باشند، می‌تواند به ارزیابی واقع‌بینانه‌تر وضعیت مدیریت خط‌مشی امنیت اطلاعات کمک کند.

سیستم‌های خبره

سیستم خبره نوعی سامانه رایانه‌ای مبتنی بر دانش است که برای انجام وظایفی طراحی می‌شود که در حالت معمول نیازمند دانش و تجربه یک متخصص انسانی هستند. این سیستم‌ها با استفاده از مجموعه‌ای از حقایق، دانش تخصصی و قواعد استنتاج، قادر به تحلیل یک مسئله و ارائه نتیجه یا پیشنهاد هستند.

در مسائلی که دانش متخصصان دارای ابهام و عدم قطعیت است، استفاده از قواعد کلاسیک و قطعی ممکن است انعطاف‌پذیری لازم را نداشته باشد. در چنین شرایطی، تلفیق ساختار سیستم‌های خبره با منطق فازی می‌تواند امکان بازنمایی مناسب‌تر دانش انسانی را فراهم آورد.

منطق فازی

منطق فازی توسط لطفی‌زاده به‌عنوان رویکردی برای مدل‌سازی مفاهیم مبهم و استدلال تقریبی ارائه شد. برخلاف منطق کلاسیک که در آن عضویت یک عنصر در یک مجموعه تنها می‌تواند صفر یا یک باشد، در منطق فازی هر عنصر می‌تواند با درجه‌ای از عضویت به یک مجموعه تعلق داشته باشد (زاده، ۱۹۷۸: ۳). این ویژگی امکان نمایش مفاهیمی را فراهم می‌کند که دارای مرزهای دقیق و قطعی نیستند.

in Press

برای مثال؛ در یک سیستم ارزیابی امنیت اطلاعات ممکن است سطح آگاهی کارکنان با واژه‌هایی مانند «کم»، «متوسط» و «زیاد» بیان شود. در رویکرد کلاسیک، تعیین یک مرز عددی دقیق میان این سطوح می‌تواند دشوار و تا حدودی قراردادی باشد، در حالی که در منطق فازی یک مقدار مشخص می‌تواند به‌طور هم‌زمان و با درجات متفاوت به چند مجموعه فازی تعلق داشته باشد. مجموعه‌های فازی با استفاده از توابع عضویت تعریف می‌شوند. تابع عضویت، درجه تعلق هر مقدار به یک مجموعه فازی را تعیین می‌کند. توابع عضویت می‌توانند اشکال مختلفی داشته باشند که توابع مثلثی، ذوزنقه‌ای و گاوسی از متداول‌ترین انواع آن‌ها هستند. انتخاب نوع و پارامترهای تابع عضویت می‌تواند براساس دانش خبرگان، ویژگی‌های داده‌ها و ماهیت مسئله صورت گیرد. توانایی منطق فازی در ترکیب اطلاعات کمی و کیفی، استفاده از متغیرهای زبانی و بازنمایی دانش متخصصان، موجب شده است که این رویکرد در بسیاری از مسائل تصمیم‌گیری و ارزیابی که با عدم قطعیت و ابهام همراه‌اند مورد استفاده قرار گیرد. همچنین، مدل‌سازی فازی می‌تواند چارچوبی مناسب برای نمایش روابط غیرخطی پیچیده فراهم کرده و در عین حال ساختار استدلالی نسبتاً شفافی داشته باشد (وانگاس‌آیالا، بارون‌ولاندیا و لئال‌لارا[1]، ۲۰۲۲).

سیستم استنتاج فازی

سیستم استنتاج فازی با استفاده از متغیرهای زبانی، توابع عضویت و قواعد «اگر–آنگاه»، روابط میان ورودی‌ها و خروجی‌ها را از طریق فازی‌سازی، استنتاج و فازی‌زدایی مدل می‌کند (لوگاناثان و همکاران[2]، ۲۰۲۴: ۴). هدف اصلی این سیستم تبدیل دانش زبانی و قضاوت‌های انسانی به یک سازوکار منظم و قابل محاسبه برای تصمیم‌گیری است.

فرایند استنتاج فازی به‌طور کلی شامل سه مرحله اصلی فازی‌سازی، استنتاج فازی و فازی‌زدایی است (لوگاناثان و همکاران، ۲۰۲۴: ۴). در مرحله فازی‌سازی، مقادیر قطعی ورودی با استفاده از توابع عضویت به درجات عضویت در مجموعه‌های فازی تبدیل می‌شوند. در مرحله استنتاج، قواعد اگر–آنگاه بر ورودی‌های فازی اعمال شده و خروجی فازی سیستم محاسبه می‌شود. در مرحله

[1]Vanegas-Ayala, Barón-Velandia, & Leal-Lara

نهایی، یعنی فازی‌زدایی، خروجی فازی به یک مقدار قطعی تبدیل می‌شود تا امکان تفسیر و استفاده عملی از نتیجه فراهم شود.

هر سیستم استنتاج فازی از چهار جزء اصلی شامل ماژول فازی‌سازی، پایگاه دانش، موتور استنتاج و ماژول فازی‌زدایی تشکیل می‌شود (نیک‌منش، فیلی و سروشین[1]، ۲۰۲۳: ۴):

الف) ماژول فازی‌سازی: این بخش مقادیر قطعی ورودی را با استفاده از توابع عضویت به مقادیر یا مجموعه‌های فازی تبدیل می‌کند.

ب) پایگاه دانش: پایگاه دانش شامل توابع عضویت، متغیرهای زبانی و مجموعه قواعد اگر–آنگاه است که براساس دانش متخصصان و اطلاعات موجود درباره مسئله طراحی می‌شوند.

ج) موتور استنتاج: موتور استنتاج قواعد موجود در پایگاه دانش را بر ورودی‌های فازی اعمال کرده و نتیجه فازی را استخراج می‌کند. این مرحله در واقع نحوه استدلال متخصص انسانی را به‌صورت محاسباتی شبیه‌سازی می‌کند.

د) ماژول فازی‌زدایی: در این مرحله، خروجی حاصل از فرایند استنتاج از یک مقدار یا مجموعه فازی به یک مقدار قطعی قابل تفسیر تبدیل می‌شود.

در طراحی سیستم‌های فازی، داده‌های ذهنی و قضاوت‌های خبرگان می‌توانند از طریق متغیرهای زبانی و مقیاس‌های رتبه‌بندی فازی در مدل وارد شوند (المادی، المملوک، المرهبی، الله، جمال و باندارا[2]، ۲۰۲۲: ۶). این ویژگی موجب می‌شود سیستم استنتاج فازی برای مسائلی که بخشی از اطلاعات آن‌ها براساس تجربه، ادراک و قضاوت انسانی شکل می‌گیرد، ابزار مناسبی باشد.

سیستم‌های استنتاج فازی ممدانی و سوگنو

و ساختار پرکاربرد در سیستم‌های استنتاج فازی، مدل ممدانی و مدل تاکاگی–سوگنو هستند. در مدل ممدانی، بخش نتیجه قواعد بر پایه مجموعه‌های فازی تعریف می‌شود، در حالی که در مدل سوگنو، نتیجه قواعد می‌تواند به‌صورت تابعی از متغیرهای ورودی بیان شود (گونی و ساریکایا[3]، ۲۰۰۹: ۸۵، ۸۹–۹۰). همچنین، سوگنو از نظر کارایی محاسباتی مزیت دارد، در حالی که ممدانی قابلیت بیشتری برای بازنمایی ورودی انسانی دارد (المادی و همکاران، ۲۰۲۲: ۴).

با توجه به اینکه در مسئله ارزیابی مدیریت خط‌مشی امنیت اطلاعات، بخش قابل‌توجهی از دانش مورد نیاز براساس قضاوت متخصصان و مفاهیم زبانی نظیر «کم»، «متوسط» و «زیاد» بیان می‌شود،

[1] Nikmanesh, Feili, & Sorooshian
[2] Almadi, Al Mamlook, Almarhabi, Ullah, Jamal, & Bandara
[3] Guney & Sarikaya

استفاده از سیستم استنتاج فازی ممدانی می‌تواند مناسب‌تر باشد. این سیستم امکان تعریف قواعدی با ساختار قابل فهم مانند «اگر سطح آگاهی کارکنان زیاد و میزان اجرای خط‌مشی بالا باشد، آنگاه وضعیت مدیریت خط‌مشی امنیت اطلاعات مطلوب است» را فراهم می‌کند. چنین ساختاری علاوه بر تسهیل استخراج دانش خبرگان، قابلیت تفسیر نتایج مدل را نیز افزایش می‌دهد.

توسعه چارچوب پژوهش

با توجه به مبانی نظری بیان‌شده، ارزیابی مدیریت خط‌مشی امنیت اطلاعات را می‌توان مسئله‌ای چندبعدی دانست که در آن تعدادی از معیارها و مؤلفه‌های اثرگذار ماهیتی کیفی، زبانی و غیرقطعی دارند. استفاده صرف از روش‌های قطعی ممکن است موجب از دست رفتن بخشی از اطلاعات موجود در قضاوت متخصصان شود؛ زیرا در محیط واقعی نمی‌توان همواره میان وضعیت‌های مختلف امنیتی مرزهای عددی مشخص و دقیقی تعیین کرد.

از سوی دیگر، سیستم استنتاج فازی امکان ترکیب دانش متخصصان، متغیرهای زبانی، قواعد تصمیم‌گیری و اطلاعات عددی را در یک چارچوب واحد فراهم می‌سازد. به همین دلیل، در پژوهش حاضر از سیستم استنتاج فازی ممدانی به‌عنوان ابزار اصلی ارزیابی مدیریت خط‌مشی امنیت اطلاعات استفاده می‌شود. مؤلفه‌ها و شاخص‌های مورد نیاز مدل با بررسی استانداردها، اسناد و چارچوب‌های معتبر امنیت اطلاعات و با تأکید بر اسناد خط‌مشی مؤسسه سنس شناسایی می‌شوند. سپس برای هر متغیر، مجموعه‌های فازی و توابع عضویت تعریف شده و قواعد اگر–آنگاه براساس دانش و نظر خبرگان تدوین می‌شوند.

در چارچوب پیشنهادی، مقادیر مربوط به شاخص‌های ارزیابی به‌عنوان ورودی سیستم در نظر گرفته شده و پس از انجام مراحل فازی‌سازی، استنتاج براساس قواعد و فازی‌زدایی، وضعیت کلی مدیریت خط‌مشی امنیت اطلاعات به‌عنوان خروجی مدل تعیین می‌شود. این خروجی می‌تواند مبنایی برای شناسایی نقاط ضعف، مقایسه وضعیت بخش‌های مختلف و تعیین اولویت اقدامات اصلاحی در سازمان قرار گیرد.

بنابراین؛ منطق توسعه مدل پژوهش بر این فرض استوار است که به‌کارگیری سیستم استنتاج فازی ممدانی، به دلیل قابلیت مدیریت ابهام و عدم قطعیت و نیز امکان استفاده از دانش زبانی خبرگان، می‌تواند چارچوبی مناسب برای ارزیابی مدیریت خط‌مشی امنیت اطلاعات فراهم آورد .بر همین اساس، در بخش بعدی نحوه استخراج مؤلفه‌ها، طراحی متغیرهای ورودی و خروجی، توابع عضویت، قواعد استنتاج و پیاده‌سازی مدل پیشنهادی تشریح خواهد شد.

روش‌شناسی پژوهشی

پژوهش حاضر از نظر هدف، کاربردی و از نظر ماهیت و فرایند اجرا، دارای رویکرد توسعه‌ای است؛ زیرا هدف اصلی آن طراحی و توسعه یک سیستم استنتاج فازی برای ارزیابی مدیریت خط‌مشی امنیت اطلاعات در سازمان‌ها است. در این پژوهش نیز تلاش شده است با استفاده از قابلیت‌های منطق فازی در مدیریت ابهام و عدم قطعیت، چارچوبی هوشمند و انعطاف‌پذیر برای ارزیابی وضعیت مدیریت خط‌مشی امنیت اطلاعات ارائه شود.

فرایند انجام پژوهش در دو مرحله اصلی شامل شناسایی مؤلفه‌ها و شاخص‌های ارزیابی و استخراج دانش خبرگان و طراحی سیستم استنتاج فازی انجام شده است.

در مرحله نخست، به‌منظور شناسایی مفاهیم، عوامل و متغیرهای مؤثر بر مدیریت خط‌مشی امنیت اطلاعات، مطالعات اسنادی و کتابخانه‌ای انجام شد. بدین منظور، مقالات علمی، کتاب‌ها، استانداردهای مرتبط با امنیت اطلاعات، چارچوب‌های معتبر امنیتی و اسناد تخصصی مرتبط با خط‌مشی‌های امنیت اطلاعات مورد بررسی قرار گرفتند. در این مرحله، رویکرد پژوهش ماهیتی اکتشافی داشت و هدف اصلی، شناسایی مؤلفه‌ها و شاخص‌هایی بود که می‌توانند در ارزیابی وضعیت مدیریت خط‌مشی امنیت اطلاعات مورد استفاده قرار گیرند.

پس از بررسی منابع و چارچوب‌های موجود، اسناد خط‌مشی امنیت اطلاعات ارائه‌شده توسط مؤسسه سنس به‌عنوان یکی از منابع مرجع برای تدوین ساختار ارزیابی انتخاب شدند. خط‌مشی‌ها و الزامات مرتبط با مدیریت امنیت اطلاعات از این اسناد استخراج و پس از بررسی و طبقه‌بندی، به‌عنوان مبنایی برای تعیین متغیرهای مورد استفاده در سیستم استنتاج فازی در نظر گرفته شدند.

در مرحله دوم، به‌منظور بهره‌گیری از دانش و تجربه متخصصان، پرسشنامه‌ای مبتنی بر مؤلفه‌ها و شاخص‌های شناسایی‌شده تهیه و در اختیار خبرگان حوزه امنیت اطلاعات قرار گرفت. هدف از این مرحله، دریافت قضاوت خبرگان درباره وضعیت و اهمیت متغیرهای مورد بررسی و همچنین استخراج دانش لازم برای تدوین قواعد استنتاج فازی بود. در این مرحله، گردآوری داده‌ها به شیوه پیمایشی انجام گرفت و نظرات متخصصان به‌عنوان مبنایی برای تعیین روابط میان متغیرهای ورودی و خروجی و تدوین قواعد زبانی «اگر–آنگاه» مورد استفاده قرار گرفت.

پس از گردآوری و تحلیل نظرات خبرگان، متغیرهای ورودی و خروجی سیستم مشخص و برای هر یک، متغیرهای زبانی و توابع عضویت مناسب تعریف شدند. سپس، پایگاه قواعد فازی با استفاده از

دانش استخراج‌شده از خبرگان تشکیل شد. قواعد تدوین‌شده روابط میان وضعیت متغیرهای ورودی و سطح ارزیابی مدیریت خط‌مشی امنیت اطلاعات را بیان می‌کنند.

در ادامه، با توجه به ماهیت زبانی متغیرهای مورد بررسی و اهمیت تفسیرپذیری قواعد، از سیستم استنتاج فازی ممدانی استفاده شد. فرایند استنتاج شامل سه مرحله اصلی فازی‌سازی داده‌های ورودی، اعمال قواعد فازی و فازی‌زدایی خروجی است. در مرحله فازی‌سازی، مقادیر قطعی ورودی به درجات عضویت در مجموعه‌های فازی تبدیل شده و سپس قواعد موجود در پایگاه دانش توسط موتور استنتاج پردازش می‌شوند. در نهایت، خروجی فازی حاصل با استفاده از روش فازی‌زدایی به یک مقدار قطعی تبدیل می‌شود که بیانگر وضعیت ارزیابی مدیریت خط‌مشی امنیت اطلاعات است. سیستم استنتاج فازی پیشنهادی با استفاده از جعبه‌ابزار منطق فازی نرم‌افزار MATLAB طراحی و پیاده‌سازی شد. پس از تعریف متغیرهای ورودی و خروجی، توابع عضویت و قواعد استنتاج، رفتار سیستم از طریق اجرای قواعد فازی و بررسی خروجی حاصل از ترکیب سطوح مختلف متغیرهای ورودی در محیط MATLAB بررسی شد. داده‌های مورد استفاده در طراحی مدل از اسناد خط‌مشی امنیت اطلاعات مؤسسه سنس و نظرات ۱۵ خبره حوزه فناوری اطلاعات و امنیت اطلاعات استخراج شده است و در پژوهش حاضر از داده‌های عملیاتی یک سازمان واقعی برای اعتبارسنجی مستقل مدل استفاده نشده است. خروجی نهایی سیستم، وضعیت مدیریت خط‌مشی امنیت اطلاعات را در سه سطح ضعیف، متوسط و قوی ارائه می‌کند.

به‌طور کلی، مراحل اجرای پژوهش شامل مطالعه منابع و اسناد، شناسایی و استخراج مؤلفه‌های ارزیابی، انتخاب اسناد مرجع سنس، طراحی ابزار گردآوری نظرات خبرگان، استخراج دانش خبرگان، تعریف متغیرها و توابع عضویت، تدوین قواعد اگر–آنگاه، طراحی سیستم استنتاج فازی ممدانی، پیاده‌سازی در محیط MATLAB و ارزیابی خروجی سیستم است.

جامعه آماری، نمونه و ابزار گردآوری داده‌ها

جامعه آماری پژوهش حاضر شامل خبرگان، متخصصان و مدیران حوزه فناوری اطلاعات و امنیت اطلاعات است که دارای دانش و تجربه مرتبط با مدیریت خط‌مشی‌های امنیت اطلاعات هستند. با توجه به تخصصی بودن موضوع پژوهش و ضرورت استفاده از افرادی که از دانش و تجربه کافی در این حوزه برخوردار باشند، انتخاب نمونه‌ها به روش غیراحتمالی و گلوله‌برفی انجام شد. در این روش، ابتدا تعدادی از متخصصان واجد شرایط شناسایی شدند و سپس با معرفی آنان، سایر خبرگان مرتبط با موضوع پژوهش مورد شناسایی و بررسی قرار گرفتند. در نهایت، ۱۵ نفر از خبرگان حوزه

امنیت اطلاعات در پژوهش مشارکت کردند. هدف از مشارکت این افراد، بهره‌گیری از دانش تخصصی آنان در ارزیابی مؤلفه‌های مورد مطالعه، استخراج قواعد تصمیم‌گیری و اعتبارسنجی دانش مورد استفاده در سیستم استنتاج فازی بود.

گردآوری اطلاعات مورد نیاز پژوهش در دو بخش مطالعات اسنادی و کتابخانه‌ای و گردآوری نظرات خبرگان انجام شد. در بخش نخست، منابع علمی مرتبط با امنیت اطلاعات، مدیریت خط‌مشی امنیت اطلاعات، سیستم‌های خبره و منطق فازی مورد بررسی قرار گرفتند. این منابع شامل مقالات علمی، کتاب‌ها، استانداردها، چارچوب‌های معتبر امنیت اطلاعات و اسناد تخصصی بودند. برای دسترسی به مطالعات پیشین، از منابع و پایگاه‌های علمی معتبر داخلی و خارجی از جمله IEEE ، ScienceDirect، Springer، Scopus، Emerald، SIDو نورمگز استفاده شد.

علاوه بر منابع علمی، اسناد و خط‌مشی‌های امنیت اطلاعات ارائه‌شده توسط مؤسسه سنس نیز مورد بررسی قرار گرفتند. پس از مطالعه، استخراج و طبقه‌بندی این اسناد، مجموعه‌ای از متغیرها و مؤلفه‌های مرتبط با مدیریت امنیت اطلاعات در ۱۰ حوزه اصلی شناسایی شد. این حوزه‌ها مبنای اولیه طراحی ابزار گردآوری داده‌ها و ساختار سیستم استنتاج فازی را تشکیل دادند.

در پژوهش حاضر، از اسناد خط‌مشی مؤسسه سنس به‌عنوان منبع عملیاتی اولیه برای استخراج گزاره‌های خط‌مشی و طراحی متغیرهای سیستم استنتاج فازی استفاده شد. انتخاب سنس به دلیل ارائه خط‌مشی‌های اجرایی و قابل تبدیل به گزاره‌های زبانی و قواعد اگر–آنگاه انجام شد. بااین‌حال، سنس یک استاندارد رسمی سیستم مدیریت امنیت اطلاعات محسوب نمی‌شود و استفاده از آن به‌تنهایی نمی‌تواند جایگزین استانداردها و چارچوب‌های بین‌المللی نظیر ISO/IEC 27001، ISO/IEC 27002و چارچوب امنیت سایبری اِن‌آی‌اِس‌تی[1] باشد. ازاین‌رو، در پژوهش حاضر سنس به‌عنوان منبع استخراج الزامات عملیاتی در نظر گرفته شده و برای بررسی پوشش مفهومی مدل، حوزه‌های استخراج‌شده با مؤلفه‌های متناظر در ISO/IEC 27001/27002 و چارچوب اِن‌آی‌اِس‌تی تطبیق مفهومی داده شدند. این تطبیق با هدف بررسی هم‌راستایی مفهومی انجام شده و به معنای انجام ممیزی یا ارزیابی رسمی انطباق با این استانداردها نیست.

محور مدل پیشنهادی			
COBIT 2019			

[1] NIST Cybersecurity Framework (NIST CSF)

	NIST CSF 2.0	ISO/IEC 27001/27002	
حاکمیت و مدیریت خط‌مشی	Govern	ISMS / Organizational controls	EDM03 / APO13
مدیریت ریسک	Govern / Identify	Risk-based ISMS	APO12
کنترل دسترسی و گذرواژه	Protect	Access controls	DSS05
شبکه و ارتباطات	Protect / Detect	Technological controls	DSS05
تداوم و بازیابی	Respond / Recover	Continuity-related controls	DSS04
انطباق	Govern	Compliance requirements	MEA03

جدول (۱). تطبیق مفهومی حوزه‌های مدل با استانداردها و چارچوب‌های مرجع امنیت اطلاعات

تطبیق فوق در سطح مفهومی انجام شده است و نباید به‌عنوان ارزیابی کامل انطباق یا پوشش تمام کنترل‌های استانداردهای مذکور تفسیر شود. به‌منظور تقویت قابلیت کاربرد و جاری‌سازی مدل پیشنهادی در محیط سازمانی، علاوه بر استانداردهای ISO/IEC 27001:2022 و ISO/IEC 27002:2022 و چارچوب اِن‌آی‌اِس‌تی ۲.۰، ارتباط مفهومی مدل با کوبیت ۲۰۱۹[1] نیز در نظر گرفته شد. چارچوبی برای حاکمیت و مدیریت اطلاعات و فناوری در سطح سازمان است و اهداف مرتبطی نظیر بهینه‌سازی ریسک(EDM03) ، مدیریت ریسک (APO12)، مدیریت امنیت (APO13)، مدیریت تداوم فعالیت (DSS04)، مدیریت خدمات امنیتی (DSS05) و مدیریت انطباق با الزامات خارجی(MEA03) می‌توانند به‌عنوان لایه حاکمیتی مکمل برای استفاده عملی از خروجی سیستم استنتاج فازی به‌کار گرفته شوند. در این چارچوب، خروجی مدل فازی می‌تواند به شناسایی حوزه‌های دارای وضعیت ضعیف یا متوسط کمک کرده و این نتایج به تعیین اولویت اقدامات مدیریتی و کنترلی در چارچوب کوبیت منجر شود. همچنین، در سازمان‌های فعال در بخش بانکی و مالی، نتایج مدل قابلیت تطبیق با الزامات و رهنمودهای کمیته بازل در زمینه مدیریت ریسک عملیاتی و تاب‌آوری عملیاتی را دارند. الزامات مرتبط با حاکمیت ریسک، مدیریت ریسک فناوری اطلاعات و ارتباطات، امنیت سایبری، تداوم کسب‌وکار و مدیریت رخدادها از جمله حوزه‌هایی

[1] COBIT ۲۰۱۹

هستند که می‌توانند در پیاده‌سازی بخشی مدل[1] در مؤسسات مالی مورد توجه قرار گیرند. بااین‌حال، از آنجا که دامنه پژوهش حاضر به صنعت بانکداری محدود نشده و متغیرها و قواعد مدل مستقیماً از الزامات کمیته بازل استخراج نشده‌اند، این ارتباط به‌عنوان یک قابلیت تطبیق و توسعه بخشی در نظر گرفته می‌شود و به معنای تأیید انطباق رسمی مدل با الزامات بازل نیست.

در مرحله بعد، براساس مؤلفه‌ها و خط‌مشی‌های استخراج‌شده، پرسشنامه‌ای برای دریافت و استخراج دانش خبرگان طراحی شد. پرسشنامه از دو بخش اصلی تشکیل شده بود. بخش نخست شامل اطلاعات جمعیت‌شناختی و حرفه‌ای پاسخ‌دهندگان و بخش دوم شامل ارزیابی خط‌مشی‌ها و مؤلفه‌های امنیت اطلاعات بود. به‌منظور تبدیل قضاوت خبرگان به متغیرهای قابل استفاده در مدل فازی، ارزیابی‌ها در سه سطح زبانی ضعیف، متوسط و قوی انجام گرفت.

براساس بررسی اسناد خط‌مشی امنیت اطلاعات مؤسسه سنس، در مرحله اولیه ۲۱۸ گزاره خط‌مشی در ۱۰ حوزه امنیت اطلاعات استخراج شد. منظور از این گزاره‌ها، شرایط و الزامات مطرح‌شده در اسناد خط‌مشی است و این اعداد بیانگر تعداد پاسخ‌های خبرگان یا تعداد قواعد فازی نهایی نیستند. پس از بررسی محتوای هر گزاره و ارزیابی آن توسط خبرگان، گزاره‌ها در سه سطح زبانی «ضعیف»، «متوسط» و «قوی» طبقه‌بندی شدند. در مجموع، ۸۲ گزاره در سطح ضعیف، ۷۲ گزاره در سطح متوسط و ۶۴ گزاره در سطح قوی قرار گرفتند. توزیع این گزاره‌ها در حوزه‌های مختلف در جدول (۲) ارائه شده است.

جدول ۲. خط‌مشی‌های شناسایی شده در حوزه امنیت اطلاعات

ردیف	عنوان خط‌مشی	تعداد خط‌مشی شناسایی شده در هر عنوان			
		ضعیف	متوسط	قوی	جمع کل
۱	استفاده از هوش مصنوعی	۱۱	۲	۲	۱۵
۲	امضای دیجیتال	۲	۱	۵	۸
۳	ایمیل تجاری	۶	۶	۶	۱۸
۴	اینترنت	۱۸	۲۱	۱۳	۵۲
۵	کارمندان سیار	۳	۳	۴	۱۰
۶	گذرواژه	۱۱	۲	۸	۲۱

[1]Basel Committee on Banking Supervision

۷	دسترسی از راه دور	۶	۶	۳	۱۵
۸	روتر و سوئیچ	۸	۱۵	۷	۳۰
۹	سرورها	۷	۸	۷	۲۲
۱۰	ارتباطات بی‌سیم	۱۰	۸	۹	۲۷
	جمع کل	۸۲	۷۲	۶۴	۲۱۸

تبدیل گزاره‌های خط‌مشی به قواعد فازی

برای تشکیل پایگاه دانش سیستم، گزاره‌های استخراج‌شده در هر حوزه به‌عنوان شرایط ورودی مورد استفاده قرار گرفتند و سطح زبانی تعیین‌شده برای هر گزاره، مبنای تعیین بخش نتیجه در قواعد اگر–آنگاه قرار گرفت. به بیان دیگر، محتوای هر گزاره ابتدا به یک شرط قابل ارزیابی تبدیل و سپس براساس سطح تعیین‌شده برای آن، یک قاعده زبانی در زیرسیستم مربوطه تدوین شد. ساختار کلی قواعد به‌صورت «اگر [شرط مرتبط با خط‌مشی] برقرار باشد، آنگاه سطح خط‌مشی مربوطه [ضعیف/متوسط/قوی] است» تعریف گردید. قواعد اولیه با استفاده از محتوای اسناد سنس استخراج و در مرحله بعد با استفاده از نظر خبرگان مورد بازنگری محتوایی قرار گرفتند.

در سطح دوم مدل، خروجی هر یک از ۱۰ زیرسیستم به‌عنوان ورودی سیستم جامع در نظر گرفته شد. بنابراین؛ در قواعد سیستم جامع، مقدم قاعده از ترکیب سطوح خروجی زیرسیستم‌ها و تالی قاعده از سطح کلی مدیریت خط‌مشی امنیت اطلاعات تشکیل می‌شود. برای نمونه، یکی از قواعد سیستم جامع بیان می‌کند که اگر سطوح زیرسیستم‌های هوش مصنوعی، ایمیل، امضای دیجیتال، اینترنت، کارمندان سیار، گذرواژه، دسترسی از راه دور، روتر و سوئیچ، سرور و ارتباط بی‌سیم به ترتیب در سطوح مشخصی قرار گیرند، آنگاه سطح نهایی مدیریت خط‌مشی امنیت اطلاعات «متوسط» خواهد بود.

سطح	نوع تابع	پارامترها
ضعیف	مثلثی	$[0.416667, 0, -0.416667]$
متوسط	مثلثی	$[0.916667, 0.5, 0.083333]$
قوی	مثلثی	$[1.41667, 1, 0.583333]$

جدول ۳. پارامترهای توابع عضویت مثلثی متغیر خروجی سیستم استنتاج فازی

ساختار اجرایی و نتایج سیستم استنتاج فازی

- **متغیرها و توابع عضویت:** خروجی زیرسیستم‌ها و سیستم جامع دارای سه برچسب «ضعیف»، «متوسط» و «قوی» است و از توابع عضویت مثلثی استفاده شده است. همچنین نسخه پیاده‌سازی‌شده MATLAB دامنه خروجی [0,1] دارد و پارامترهای دقیق توابع عضویت از کد قابل استخراج هستند. دامنه خروجی سیستم در محیط MATLAB برابر [0,1] تعریف شد و قسمت‌های توابع عضویت که خارج از این دامنه قرار می‌گیرند در زمان ارزیابی به‌طور طبیعی بریده می‌شوند. برای فازی‌زدایی نیز از روش مرکز ثقل[1] استفاده شد.
- **نمونه قواعد واقعی اگر–آنگاه**

حوزه	شرط	نتیجه
هوش مصنوعی	اگر کاربرد هوش مصنوعی برای فعالیت لابی‌گری سیاسی باشد	سطح خط‌مشی ضعیف است
گذرواژه	اگر طول گذرواژه بین ۸ تا ۱۶ کاراکتر باشد	سطح خط‌مشی متوسط است

جدول ٤. نمونه‌ای از قواعد واقعی اگر–آنگاه در سیستم استنتاج فازی پیشنهادی

به دلیل تعداد زیاد قواعد، ارائه کل پایگاه قواعد در مقاله امکان‌پذیر نیست؛ ازاین‌رو، نمونه‌ای از قواعد واقعی در جدول (۴) ارائه شده است. سیستم جامع در نسخه پیاده‌سازی‌شده شامل ۴۲۱ ردیف قاعده است که ۴۰۴ ترکیب مقدم یکتا را تشکیل می‌دهند.

روایی، پایایی و نحوه بررسی نظرات خبرگان

به‌منظور بررسی روایی محتوایی ابزار گردآوری نظرات خبرگان، از نسبت روایی محتوا (CVR) براساس روش لاوشه استفاده شد. در این مرحله، از ۱۵ خبره خواسته شد مناسب‌بودن گویه‌های پرسشنامه را ارزیابی کنند. از میان آنان، ۱۳ نفر گویه‌ها را از نظر هدف پژوهش مناسب و سودمند ارزیابی کردند و مقدار CVR برابر با ۰.۷۳ به‌دست آمد. با توجه به اینکه حداقل مقدار قابل قبول CVRبرای ۱۵ ارزیاب برابر با ۰.۴۹ است، روایی محتوایی ابزار مورد تأیید قرار گرفت. همچنین، پایایی پرسشنامه با استفاده از آلفای کرونباخ بررسی شد و مقدار آلفای کل برابر با ۰.۸۰۳ به‌دست آمد. در فرایند بازنگری ابزار، اصلاحات و تغییرات پیشنهادی خبرگان پس از بحث و بررسی در

[1] Centroid

نسخه نهایی پرسشنامه اعمال شد. پاسخ‌های خبرگان در قالب سه سطح زبانی «ضعیف»، «متوسط» و «قوی» برای تعیین سطوح خطمشی‌ها و تدوین دانش مورد استفاده در سیستم استنتاج فازی به‌کار گرفته شد. با این حال، در پژوهش اولیه شاخص مستقلی برای سنجش توافق بین ارزیابان، نظیر ضریب کاپای فلیس[۱]، محاسبه نشده و آستانه آماری مستقلی نیز برای اجماع خبرگان در پذیرش هر قاعده تعریف نشده است. بنابراین؛ مقدار CVR گزارش‌شده صرفاً بیانگر روایی محتوایی ابزار است و نباید به‌عنوان شاخص توافق بین خبرگان تفسیر شود. این موضوع یکی از محدودیت‌های روش‌شناختی پژوهش حاضر محسوب می‌شود. برای پذیرش محتوایی گویه‌های پرسشنامه، معیار CVRلاوشه و حداقل مقدار ۰.۴۹ برای ۱۵ خبره در نظر گرفته شد.

یافته‌های پژوهش و طراحی سیستم استنتاج فازی

در این بخش، نتایج حاصل از مراحل طراحی، پیاده‌سازی و تحلیل سیستم استنتاج فازی پیشنهادی برای ارزیابی مدیریت خطمشی امنیت اطلاعات در سازمان‌ها ارائه می‌شود. هدف از طراحی این سیستم، فراهم‌کردن چارچوبی مبتنی بر دانش خبرگان برای تحلیل هم‌زمان عوامل مؤثر بر مدیریت خطمشی امنیت اطلاعات و پشتیبانی از تصمیم‌گیری در شرایط همراه با ابهام و عدم قطعیت است.

براساس مطالعات انجام‌شده، بررسی منابع علمی و تحلیل اسناد و خطمشی‌های امنیت اطلاعات، متغیرهای مورد نیاز سیستم شناسایی شدند. سپس، برای هر یک از متغیرهای ورودی و خروجی، مجموعه‌های فازی و توابع عضویت تعریف و قواعد زبانی «اگر–آنگاه» براساس نظرات خبرگان تدوین شد. در ادامه، سیستم استنتاج فازی ممدانی در محیط MATLAB و با استفاده از جعبه‌ابزار منطق فازی[۲] پیاده‌سازی گردید.

فرایند پردازش در سیستم پیشنهادی شامل فازی‌سازی مقادیر ورودی، اعمال قواعد فازی، تجمیع نتایج حاصل از قواعد و در نهایت فازی‌زدایی خروجی است. برای تبدیل خروجی فازی به مقدار قطعی از روش مرکز ثقل استفاده شد. خروجی نهایی سیستم بیانگر سطح ارزیابی مدیریت خطمشی امنیت اطلاعات است و می‌تواند در شناسایی حوزه‌های نیازمند بهبود و پشتیبانی از تصمیم‌گیری مدیران مورد استفاده قرار گیرد.

---

[۱] Fleiss’ κ

[2] Fuzzy Logic Toolbox

تحلیل توصیفی خبرگان

به‌منظور استخراج دانش تخصصی و طراحی و اعتبارسنجی قواعد سیستم استنتاج فازی، از نظرات ۱۵ نفر از خبرگان حوزه فناوری اطلاعات و امنیت اطلاعات استفاده شد. بررسی ویژگی‌های تحصیلی پاسخ‌دهندگان نشان داد که ۶۰ درصد از خبرگان دارای مدرک کارشناسی ارشد و ۴۰ درصد دارای مدرک کارشناسی بودند.

بررسی سابقه کاری پاسخ‌دهندگان نیز نشان داد که بخش قابل‌توجهی از خبرگان از تجربه حرفه‌ای نسبتاً بالایی در حوزه فناوری اطلاعات و امنیت اطلاعات برخوردار بوده‌اند. براساس اطلاعات جمع‌آوری‌شده، حدود ۷/۶۶ درصد از افراد دارای سابقه کاری بین ۱۰ تا ۱۵ سال و ۷/۲۶ درصد دارای سابقه بین ۱۵ تا ۲۰ سال بوده‌اند. وضعیت سایر پاسخ‌دهندگان نیز براساس طبقات سابقه کاری تعریف‌شده در پرسشنامه گزارش می‌شود.

از نظر میزان آشنایی با فناوری اطلاعات، ۳/۷۳ درصد از پاسخ‌دهندگان سطح آشنایی خود را «زیاد» و ۷/۲۶ درصد «متوسط» ارزیابی کردند. همچنین، در زمینه امنیت اطلاعات، ۷/۶۶ درصد از پاسخ‌دهندگان دارای سطح آشنایی زیاد و ۳/۳۳ درصد دارای سطح آشنایی متوسط بودند.

این نتایج نشان می‌دهد که افراد شرکت‌کننده در پژوهش از سابقه و دانش مرتبط با حوزه مورد مطالعه برخوردار بوده‌اند؛ ازاین‌رو، نظرات آنان می‌تواند به‌عنوان یکی از منابع دانش تخصصی برای تدوین و ارزیابی قواعد سیستم استنتاج فازی مورد استفاده قرار گیرد.

تعیین متغیرهای سیستم استنتاج فازی

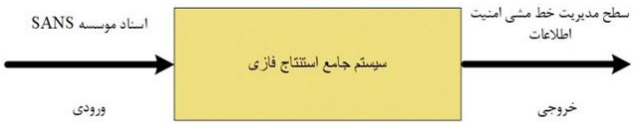
نخستین مرحله در طراحی سیستم استنتاج فازی، تعیین متغیرهای ورودی و خروجی مدل بود. این مرحله با بررسی ادبیات پژوهش، اسناد و استانداردهای امنیت اطلاعات و به‌ویژه اسناد خط‌مشی امنیتی مؤسسه سنس انجام شد. بر این اساس، مؤلفه‌ها و شاخص‌های مرتبط با مدیریت خط‌مشی امنیت اطلاعات استخراج و در قالب حوزه‌های اصلی طبقه‌بندی شدند.

متغیرهای ورودی سیستم، شاخص‌های مرتبط با حوزه‌های مختلف امنیت اطلاعات را دربرمی‌گیرند که از جمله آن‌ها می‌توان به آگاهی کارکنان، کنترل دسترسی، مدیریت ریسک، امنیت گذرواژه، امنیت ارتباطات بی‌سیم، دسترسی از راه دور و سایر مؤلفه‌های مرتبط با مدیریت خط‌مشی امنیت اطلاعات اشاره کرد.

متغیر خروجی سیستم با عنوان سطح مدیریت خط‌مشی امنیت اطلاعات تعریف شد و هدف آن ارائه ارزیابی کلی از وضعیت مدیریت خط‌مشی‌های امنیتی سازمان است.

پس از تعیین متغیرهای ورودی و خروجی، برای هر متغیر مجموعه‌های فازی متناظر تعریف شد. در این پژوهش، وضعیت متغیرها با استفاده از سه سطح زبانی ضعیف، متوسط و قوی مدل‌سازی گردید. استفاده از این متغیرهای زبانی امکان تبدیل قضاوت‌های کیفی خبرگان به مقادیر قابل پردازش در سیستم استنتاج فازی را فراهم می‌کند.

ساختار کلی متغیرهای ورودی و خروجی سیستم استنتاج فازی پیشنهادی در شکل (۱) ارائه شده است.



شکل ۱. ساختار کلی سیستم استنتاج فازی پیشنهادی

طراحی و پیاده‌سازی سیستم استنتاج فازی

پس از تعیین متغیرهای ورودی و خروجی، سیستم استنتاج فازی بر پایه مدل ممدانی طراحی شد. در این مدل، دانش خبرگان با استفاده از مجموعه‌ای از قواعد زبانی «اگر–آنگاه» در پایگاه قواعد سیستم نمایش داده می‌شود. به‌عنوان نمونه، یک قاعده می‌تواند بیان کند که اگر وضعیت دو یا چند مؤلفه امنیتی در سطوح مشخصی قرار داشته باشد، سطح ارزیابی مدیریت خط‌مشی امنیت اطلاعات نیز در یک سطح زبانی مشخص قرار خواهد گرفت.

فرایند استنتاج در سیستم پیشنهادی ماهیتی داده‌محور دارد؛ به این معنا که پردازش از مقادیر ورودی آغاز شده و پس از بررسی و فعال‌شدن قواعد مرتبط، نتیجه نهایی سیستم حاصل می‌شود. این ساختار با مفهوم استنتاج پیشرو سازگار است؛ در استنتاج پیشرو، ابتدا داده‌ها و واقعیت‌های موجود در اختیار سیستم قرار می‌گیرند و سپس قواعد متناسب با آن‌ها فعال شده و سیستم به سمت نتیجه نهایی حرکت می‌کند (سیلر و باکلی[1]، ۲۰۰۵: ۲۴). می‌کند.

در مقابل، در استنتاج پسرو، فرایند تحلیل از یک هدف یا نتیجه مشخص آغاز شده و سیستم در پی شناسایی شرایط و داده‌های لازم برای اثبات یا دستیابی به آن نتیجه است (سیلر و باکلی، ۲۰۰۵: ۲۴). با توجه به اینکه در پژوهش حاضر مقادیر متغیرهای امنیت اطلاعات به‌عنوان ورودی سیستم دریافت شده و خروجی براساس ترکیب این ورودی‌ها و قواعد تعریف‌شده محاسبه می‌شود، ساختار مورد استفاده با رویکرد استنتاج پیشرو انطباق دارد.

[1] Siler & Buckley

در سیستم ممدانی پیشنهادی، ابتدا داده‌های ورودی با استفاده از توابع عضویت تعریف‌شده فازی‌سازی می‌شوند. سپس، موتور استنتاج قواعد مرتبط را فعال کرده و نتایج قواعد را با یکدیگر ترکیب می‌کند. در مرحله نهایی، خروجی فازی حاصل به کمک فرایند فازی‌زدایی به یک مقدار قطعی تبدیل می‌شود. در پژوهش حاضر برای فازی‌زدایی از روش مرکز ثقل[1] استفاده شده است.

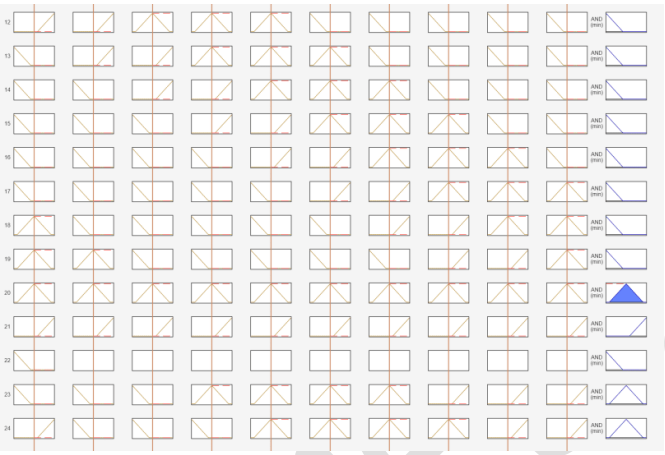
طراحی و پیاده‌سازی سیستم در محیط MATLAB و با استفاده از جعبه‌ابزار منطق فازی انجام شد. پس از تعریف متغیرهای ورودی و خروجی، توابع عضویت و پایگاه قواعد، سیستم برای مقادیر مختلف ورودی اجرا شده و رفتار آن مورد بررسی قرار گرفت. نتایج حاصل از اجرای مدل در بخش‌های بعدی براساس خروجی زیرسیستم‌ها، قواعد فعال‌شده و مقادیر نهایی سیستم تحلیل می‌شود.

اجرای مدل و نمونه خروجی سیستم

به‌منظور بررسی نحوه رفتار سیستم استنتاج فازی طراحی‌شده، مدل در محیط MATLAB برای ترکیب‌های مختلف مقادیر ورودی اجرا شد. خروجی زیرسیستم‌های فازی به‌عنوان ورودی سیستم جامع در نظر گرفته شده و براساس قواعد تعریف‌شده، سطح نهایی مدیریت خط‌مشی امنیت اطلاعات در یکی از سه سطح «ضعیف»، «متوسط» و «قوی» تعیین می‌شود.

به‌عنوان نمونه، براساس ساختار تعریف‌شده برای سیستم جامع، چنانچه از میان ۱۰ زیرسیستم مورد بررسی، پنج خروجی در سطح ضعیف، سه خروجی در سطح متوسط و دو خروجی در سطح قوی قرار گیرند، وضعیت نهایی مدیریت خط‌مشی امنیت اطلاعات در سطح «ضعیف» طبقه‌بندی می‌شود. این ساختار نشان می‌دهد که خروجی سیستم جامع حاصل تجمیع نتایج زیرسیستم‌ها و اعمال قواعد فازی تعریف‌شده است.

[1] Centroid



شکل ۲. نمایش سطح تصمیم سیستم استنتاج فازی جامع براساس خروجی

شکل (۲) نمونه‌ای از سطح تصمیم ایجادشده توسط سیستم استنتاج فازی را نشان می‌دهد. محورهای ورودی بیانگر خروجی زیرسیستم‌های هوش مصنوعی و اینترنت بوده و سطح حاصل، تغییرات خروجی سیستم جامع را در اثر تغییر مقادیر این دو زیرسیستم نمایش می‌دهد. تغییر پیوسته سطح خروجی نشان می‌دهد که مدل برخلاف طبقه‌بندی قطعی، امکان لحاظ‌کردن درجات میانی میان سطوح ضعیف، متوسط و قوی را فراهم می‌کند.

بحث و نتیجه‌گیری

پژوهش حاضر با هدف طراحی یک سیستم استنتاج فازی برای ارزیابی مدیریت خط‌مشی امنیت اطلاعات در سازمان‌ها انجام شد. از آنجا که بسیاری از مؤلفه‌های این حوزه، مانند آگاهی کارکنان، میزان رعایت الزامات امنیتی، کیفیت کنترل‌ها و سطح انطباق با خط‌مشی‌ها، ماهیتی کیفی و همراه با عدم قطعیت دارند، استفاده از روش‌های صرفاً قطعی نمی‌تواند همواره واقعیت این ارزیابی‌ها را به‌خوبی منعکس کند. بر این اساس، با استفاده از منابع علمی، چارچوب‌های امنیت اطلاعات، اسناد سنس و نظرات ۱۵ خبره، مؤلفه‌ها و قواعد زبانی «اگر–آنگاه» استخراج و یک سیستم استنتاج فازی ممدانی در محیط MATLAB طراحی و پیاده‌سازی شد. نتایج نشان داد که مدل پیشنهادی می‌تواند مؤلفه‌های مختلف امنیت اطلاعات را در یک ساختار یکپارچه پردازش و براساس ترکیب ورودی‌ها و دانش خبرگان، سطح مدیریت خط‌مشی را در سه سطح «ضعیف»، «متوسط» و «قوی» تعیین کند.

استفاده از متغیرهای زبانی امکان درنظرگرفتن درجات مختلف وضعیت امنیتی را فراهم کرده و ساختار قاعده‌محور مدل نیز موجب شده است منطق تصمیم‌گیری آن برای مدیران و کارشناسان قابل تفسیر باشد. ازاین‌رو، سیستم پیشنهادی می‌تواند به‌عنوان یک ابزار پشتیبان تصمیم‌گیری برای شناسایی حوزه‌های نیازمند بهبود و اولویت‌بندی اقدامات اصلاحی مورد استفاده قرار گیرد. این یافته‌ها با نتایج کاسولا و همکاران (۲۰۰۵: ۱۷۲) درباره کاربرد روش‌های فازی در تحلیل و طبقه‌بندی سطوح امنیتی همسو است. همچنین، نتایج با مطالعات سهرابی‌صفا و همکاران (۲۰۱۶: ۷۵، ۷۷–۷۸) و العتیبی و همکاران (۲۰۱۶: ۳۵۴–۳۵۵) از نظر اهمیت عوامل انسانی و سازمانی مانند آموزش، آگاهی و مشارکت کارکنان در اثربخشی خط‌مشی‌های امنیت اطلاعات سازگار است. تفاوت اصلی پژوهش حاضر در آن است که این عوامل را در قالب یک پایگاه قواعد فازی و یک ابزار پشتیبان تصمیم‌گیری قابل اجرا سازمان‌دهی کرده است. در تعمیم نتایج باید احتیاط شود؛ زیرا ساختار سازمان، سطح بلوغ امنیت اطلاعات، زیرساخت‌های فناوری، الزامات قانونی و فرهنگ امنیتی می‌تواند بر اهمیت متغیرها و قواعد تصمیم‌گیری اثر بگذارد. بنابراین؛ پیش از استفاده از مدل در یک سازمان مشخص، قواعد و پارامترهای آن باید متناسب با شرایط همان سازمان بازبینی شوند.

پژوهش حاضر دارای چند محدودیت است. نخست، دانش مورد استفاده در تدوین قواعد بر نظرات ۱۵ خبره استوار بوده است. دوم، منبع عملیاتی اولیه استخراج گزاره‌ها، اسناد سنس بوده است. برای کاهش این محدودیت، حوزه‌های مدل در نسخه حاضر به‌صورت مفهومی با ISO/IEC 27001/27002 و NIST CSF تطبیق داده شدند؛ بااین‌حال، این تطبیق به معنای ارزیابی کامل انطباق با کنترل‌های این استانداردها نیست. سوم، مدل در قالب سیستم استنتاج فازی ممدانی توسعه یافته و داده‌های تجربی مستقل از سازمان‌های واقعی برای اعتبارسنجی میدانی آن در دسترس نبوده است. بر این اساس، پیشنهاد می‌شود در مطالعات آینده مدل در سازمان‌ها و صنایع مختلف اجرا و با ارزیابی مستقل متخصصان مقایسه شود. همچنین، استفاده از تعداد و تنوع بیشتر خبرگان، نگاشت تفصیلی با استانداردهای امنیتی، مقایسه مدل ممدانی با سیستم سوگنو و سایر روش‌های تصمیم‌گیری، بررسی منطق فازی نوع دوم و استفاده از روش‌های یادگیری ماشین برای به‌روزرسانی قواعد می‌تواند به توسعه مدل کمک کند. در مجموع، پژوهش حاضر نشان می‌دهد که ترکیب دانش خبرگان، اسناد امنیت اطلاعات و سیستم استنتاج فازی ممدانی می‌تواند چارچوبی منعطف و قابل تفسیر برای ارزیابی مدیریت خط‌مشی امنیت اطلاعات فراهم سازد و زمینه توسعه ابزارهای هوشمند پشتیبان تصمیم‌گیری در این حوزه را ایجاد کند.

تقدیر و تشکر

نویسندگان از دانشکده علوم اجتماعی و اقتصادی، دانشگاه الزهرا، موسسه تحقیقات ریاضی دکتر غلامحسین مصاحب دانشگاه خوارزمی و مؤسسه تحقیقات سیاست علمی کشور به خاطر حمایت از این کار تشکر و قدردانی می کنند.

منابع

منابع فارسی

دانایی‌فرد، ح.، الوانی، س. م.، و آذر، ع. (1383). *روش‌شناسی پژوهش کمی در مدیریت: رویکردی جامع*. تهران: انتشارات صفار و اشراقی.

منابع انگلیسی

Almadi, A. I. M., Al Mamlook, R. E., Almarhabi, Y., Ullah, I., Jamal, A., & Bandara, N. (2022). A fuzzy-logic approach based on driver decision-making behavior modeling and simulation. *Sustainability, 14*(14), 8874. https://doi.org/10.3390/su14148874

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 352–358). IEEE. https://doi.org/10.1109/ICITST.2016.7856729

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690

Casola, V., Preziosi, R., Rak, M., & Troiano, L. (2005). A reference model for security level evaluation: Policy and fuzzy techniques. *Journal of Universal Computer Science, 11*(1), 150–174. https://doi.org/10.3217/jucs-011-01-0150

Danaeifard, H., Alvani, S. M., & Azar, A. (2004). *Quantitative research methodology in management: A comprehensive approach*. Saffar & Eshraghi Publications. (in Persian).

Guney, K., & Sarikaya, N. (2009). Comparison of Mamdani and Sugeno fuzzy inference system models for resonant frequency calculation of rectangular microstrip antennas. *Progress In Electromagnetics Research B, 12*, 81–104. https://doi.org/10.2528/PIERB08121302

International Organization for Standardization, & International Electrotechnical Commission. (2026). *Information security, cybersecurity and privacy protection—Information security management systems—Overview (ISO/IEC 27000:2026)*. ISO.

International Organization for Standardization, & International Electrotechnical Commission. (2022a). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022)*. ISO.

International Organization for Standardization, & International Electrotechnical Commission. (2022b). *Information security, cybersecurity and privacy protection—Information security controls (ISO/IEC 27002:2022)*. ISO.

Loganathan, S., Ramakrishnan, D., Sathiyamoorthy, M., & Azamathulla, H. M. (2024). Assessment of irrigational suitability of groundwater in Thanjavur district,

Southern India using Mamdani fuzzy inference system. *Results in Engineering, 21*, 101789. https://doi.org/10.1016/j.rineng.2024.101789

Nikmanesh, M., Feili, A., & Sorooshian, S. (2023). Employee productivity assessment using fuzzy inference system. *Information*, *14*(7), 423. https://doi.org/10.3390/info14070423

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS 2007)* (p. 156b). IEEE. https://doi.org/10.1109/HICSS.2007.206

SANS Institute. (n.d.). *Cybersecurity / information security policies and standards*. Retrieved August 20, 2026. SANS Cybersecurity / Information Security Policies and Standards

Siler, W., & Buckley, J. J. (2005). *Fuzzy expert systems and fuzzy reasoning*. John Wiley & Sons. https://doi.org/10.1002/0471698504

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Vanegas-Ayala, S.-C., Barón-Velandia, J., & Leal-Lara, D.-D. (2022). A systematic review of greenhouse humidity prediction and control models using fuzzy inference systems. *Advances in Human-Computer Interaction, 2022*, Article 8483003. https://doi.org/10.1155/2022/8483003

Zadeh, L. A. (1978). Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, *1*(1), 3–28. https://doi.org/10.1016/0165-0114(78)90029-5