

AI-Driven Security Intelligence Framework for Knowledge Protection in Cloud Ecosystems

Julius Olusegun Oyelami, Azleena Mohd Kassim*, Nor Athiyah Abdullah,
Mohd Heikal Husin, Nor Shamira Sabri

School of Computer Sciences, Universiti Sains Malaysia, 11800, Pulau Pinang, Malaysia

Abstract—Cloud-based knowledge sharing creates a need to coordinate security controls with the protection of organizational knowledge. This study proposes a Security Intelligence Framework (SIF) linking computational intelligence (CI) and intelligent agents (IA) to artificial intelligence (AI), and AI to penetration testing (PT), cloud security (CS), and the secure systems development life cycle (SSDLC). A cross-sectional questionnaire survey obtained 500 responses from professionals in five organizations, and the manuscript reports an analysis using partial least squares structural equation modelling in SmartPLS 4. The reported paths are positive, but inconsistencies between the structural coefficients, construct correlations, and explained variance require reconciliation before inferential conclusions can be finalized. The reported explained variance is low for SSDLC ($R^2 = 0.069$) and PT ($R^2 = 0.118$). The study concerns respondents' perceptions and does not establish improvements in deployed security controls, threat-detection performance, scalability, or knowledge-loss prevention. Its contribution is a knowledge-protection-oriented integration of intelligence capabilities and security practices that can guide further empirical and technical evaluation. Cloud security ontology, Zero Trust, blockchain auditability, and ethical AI governance are potential extensions rather than evaluated components.

Keywords—Artificial intelligence; computational intelligence; intelligent agents; cloud security; knowledge protection; blockchain security

I. INTRODUCTION

The significance of securing data in transit within cloud environments is undeniable [1]. As cybersecurity challenges evolve, the protection of data during transmission becomes critical to maintaining the integrity of knowledge distribution. In cloud environments, data in transit is particularly vulnerable, affecting the overall process of knowledge dissemination. Data processed into information, and subsequently analyzed to form knowledge, necessitates robust protection to enhance organizational performance and profitability. Extensive evidence underscores that knowledge is essential for the development of expert systems and knowledge-based artificial intelligence, particularly generative AI. However, current security measures for knowledge protection are insufficient, posing challenges to knowledge management infrastructures and undermining effective decision-making and organizational performance. The lack of dedicated security solutions for knowledge protection highlights the risks and potential losses from data and information breaches. Studies have thoroughly explored the key challenges and vulnerabilities in cloud security that contribute to knowledge loss and risk within cloud-based knowledge

distribution systems. The importance of data integrity emerges as a crucial aspect of securing knowledge systems.

Cloud security (CS) is a vital component of cybersecurity that demands attention, especially as more organizations adopt cloud technologies for their operations [2]. The diverse applications and growth of cloud services necessitate a deeper understanding of their impact on data, information, and business activities [3]. Previous studies have indicated that the presence of knowledge gaps hampers the effective integration of expert systems in the creation of AI-based knowledge databases. This leads to inadequate knowledge representation and under-developed knowledge ontologies, which are crucial for decision-making and complex problem-solving. Consequently, it remains unclear how knowledge artefacts can be effectively presented, secured, and protected during sharing and distribution across a wide spectrum within the cloud ecosystem [2], [3]. To address these knowledge gaps, there is a pressing need for an intelligent security framework that protects knowledge during sharing and distribution across cloud environments.

This study proposes a Security Intelligent Framework (SIF) that leverages artificial intelligence (AI), computational intelligence (CI), and intelligent agents (IA), a.k.a human intelligence, to enhance cloud security. The proposed methodology is based on the Secured Systems Development Life Cycle (SSDLC) application, penetration testing (PT) and cloud security (CS) ontology to strengthen the security of knowledge dissemination within cloud ecosystems. Empirical data collected from five organizations through questionnaires and analyzed using Smart-PLS elucidates the impact of AI, CI, and IA on SDLC, PT, and CSO within the SIF. The study concludes that the SIF offers a viable solution for secure knowledge sharing and distribution over the internet and cloud environments, thereby addressing security gaps in knowledge distribution and fostering effective knowledge management processes. This study introduces a Security Intelligence Framework (SIF) that operationalizes the integration of AI, CI, and IA within the Secure Systems Development Life Cycle (SSDLC) to enhance cloud security and knowledge protection. The framework incorporates Penetration Testing (PT) and Cloud Security Ontology (CSO).

Research has highlighted the foundational role of cloud security across various sectors [2]. A slow adoption rate of cloud computing ontology (CCO) has been cited as a significant challenge in implementing cloud computing security [3], [4]. To address these issues, [2] recommend an ontology-based security framework involving experts from different security domains. Such a framework can deploy protective software

*Corresponding author (azleena.mk@usm.my)

to maintain a consistent collaborative security framework. Visibility issues in cloud systems continue to create numerous security challenges [6]. Thus, CS emerges as a promising technology that can provide an effective security platform for data and information sharing, thereby ensuring protection within organizations [2].

Cloud computing is a contemporary technology that has recently garnered significant interest within the research community. As a successor to various computing research domains, including service-oriented architecture, distributed and grid computing, and virtualization, cloud computing inherits both their advancements and limitations [7]. To achieve a comprehensive understanding of cloud computing and to facilitate its swift adoption within the scientific community, an ontology that deconstructs the cloud into five principal layers [5], [6]. This ontology elucidates the interrelations and dependencies of these layers on preceding technologies as depicted in Fig. 1. Over the decades, various researchers have focused on identifying security issues in cloud computing through the development of cloud security ontologies [8], [9]. These ontologies, integral to artificial intelligence in computer science, serve as structured frameworks comprising specific vocabularies to describe certain realities. They have been defined in numerous ways and applied across various domains [9], [10], [11].

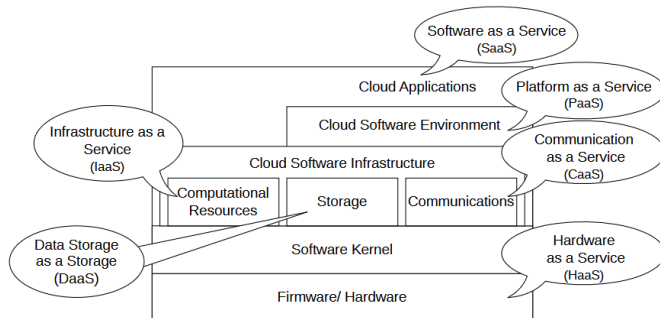


Fig. 1. The five layers of cloud computing ontology.

In a study by [7] emphasized the role of cybersecurity information exchange in generating ontologies useful for cloud security solutions. [12], [13] proposed an unsupervised ontology induction approach effective for knowledge extraction, which could extend to cybersecurity domains. Their findings suggested that Hard-Soft-Fusion (HSF) aligns heterogeneous knowledge and data semantically, providing actionable insights for secure knowledge management. Thus, security considerations are paramount in every cloud and digital project [13]. Mittal et al. in [3] introduced computational intelligence (CI) for securing data and knowledge repositories through real-time data analysis and pattern recognition. The integration of AI and machine learning algorithms for threat detection and prediction is crucial [2]. A study by [15], [17] demonstrated AI's effectiveness in enhancing cloud security, highlighting its role in securing systems and developing a two primary types of cloud environments have been identified: public clouds, which share resources among multiple users, and private clouds, which are accessible only to authorized personnel within an organization [8].

Cloud Computing Ontology (CCO) encompass services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), Data Storage as a Service (DaaS), Hardware as a Service (HaaS) and Communication as a Service (CaaS) as illustrated in 1. This platform has been considered as an asset in cloud computing security [4]. The use of IaaS, in particular, has surged in recent years [8], [11], with the number of connected devices expected to reach 20.4 billion by 2025 [9]. This increase in connectivity and IaaS usage heightens vulnerability in cloud environments, complicating the transformation of large data sets and information into knowledge. Consequently, organizations face challenges in bridging knowledge gaps, which impede their ability to solve complex problems and enhance decision-making for improved performance. The COVID-19 pandemic further exposed the susceptibility of organizational knowledge infrastructures to cyber-attacks within the cloud ecosystem [9], presenting a notable application of ontologies in the context of cloud computing security. They introduce an innovative Platform-as-a-Service (PaaS) architecture that incorporates semantic security risk management tools alongside dynamic web service policy frameworks.

Organizations depend on knowledge assets such as technical procedures, expert interpretations, design rationales, and contextualized records. Knowledge risks therefore extend beyond unauthorized access to individual files to include the loss, misuse, or deterioration of knowledge needed for organizational activities. Durst and Zieba [1] provide a knowledge-risk perspective that motivates examining how protection supports knowledge sharing and use. Cloud security research offers relevant technical approaches. Farzaan et al. [2] implement an AI-based incident detection and response pipeline and evaluate it with security datasets. Mittal et al. [3] use multiple knowledge representations to support threat-intelligence analysis. Alhammadi and Mabrouk [4] examine a multi-agent deep-learning approach to distributed denial-of-service detection. These studies address important technical or representational problems, but their evidence does not automatically establish how professionals perceive the coordination of intelligence capabilities with secure development, testing, and operational cloud security. The present study develops an integrative SIF centered on that coordination. CI and IA are conceptualized as contributors to an organizational AI capability, which is associated with PT, CS, and SSDLC practices. These practices are, in turn, related to an overall SIF evaluation. The proposed contribution is the organization of these relationships around knowledge protection. The study introduces neither a new detection algorithm nor a technically validated security architecture, and it does not claim that combining AI with agents is itself unprecedented. The objectives are to formulate a coherent conceptual model for intelligence-supported knowledge protection; examine the reported associations among its survey constructs; and identify the empirical and technical validation needed before operational use. The second objective remains conditional on resolving the measurement and statistical reporting issues identified in Section 4. Extensions involving ontologies, Zero Trust, blockchain, and AI governance are discussed as a future research agenda.

II. RELATED WORK AND CONCEPTUAL FOUNDATION

A. Knowledge Protection and Security Practices

Knowledge protection concerns the confidentiality, integrity, availability, context, and authorized use of knowledge assets. For example, protecting a design document includes controlling access to the file and preserving the meaning, provenance, and permitted use of the design rationale it contains. In this paper, the distinction between data and knowledge protection is conceptual: no separate knowledge-loss outcome or semantic-integrity measure is reported.

Secure development, technical assessment, and operational controls provide complementary points of intervention. NIST's Secure Software Development Framework identifies practices that can be integrated into a development life cycle [5], [9]. NIST's technical testing guidance describes planning, assessment, interpretation of findings, and mitigation [6], [10]. These sources support considering SSDLC and PT as complementary practices; they do not establish the survey relationships proposed here. CS denotes the broader cloud-security practices represented by the questionnaire and must be distinguished from a cloud security ontology (CSO), which would require a separately specified semantic model.

B. Focused Comparison and Originality

Table I compares the study with closely related work using the type of evidence and the scope of protection. The comparison supports an integrative research contribution rather than a claim of technical superiority. In particular, an organizational perception survey cannot be compared directly with detection accuracy measured on an attack dataset.

TABLE I. FOCUS COMPARISON WITH RELATED STUDIES

Study	Focus	Evidence	Relationship to the proposed SIF
Durst and Zieba [1]	Knowledge-risk mapping	Conceptual classification	Motivates the knowledge-risk perspective; does not validate this SIF.
Farzaan et al. [2]	AI incident detection and response	Implementation and attack datasets	Technical performance evidence; this study examines perceptions of capability and practice
Mittal et al. [3]	Threat-intelligence representation	AI pipeline with knowledge representations	Supports semantic intelligence; semantic reasoning is an untested extension here.
Alhammadi and Mabrouk [4]	Multi-agent DDoS detection	Deep-learning and dataset evaluation	Tests a specific attack task; the present model links broader organizational practices.
Present study	Knowledge-protection-oriented integration	Cross-sectional perception survey	Candidate model; measurement and structural results require reconciliation.

The model treats intelligence capabilities as potential enablers of security practices. Its theoretical rationale is that analytic capability becomes relevant to knowledge protection

when it informs development decisions, vulnerability assessment, and operational controls. This is a proposed capability-to-practice explanation, grounded in the problems addressed by the cited work. The available evidence does not establish a separate "Knowledge Protection Theory" or validate a "Cyber-Knowledge Governance Model"; those unsupported labels have been removed.

C. Construct Definitions and Model Boundaries

AI is an umbrella field, while CI methods and intelligent agents can overlap with AI. Their treatment as separate survey constructs therefore require clear item wording and evidence of discriminant validity. Table II provides conceptual definitions for interpreting the model; it does not substitute for the original questionnaire. IA means software agents with a degree of autonomous perception, decision-making, or action, and is not a synonym for human intelligence.

TABLE II. CONCEPTUAL DEFINITIONS AND MEASUREMENT BOUNDARIES

Code	Construct	Interpretation
CI	Computational intelligence	Adaptive computational approaches that support reasoning under uncertainty [13], [15]
IA	Intelligent agents	Software agents supporting autonomous observation, decisions or action [20], [21]
AI	Artificial intelligence	Perceived organizational capability to apply intelligent analysis and support decisions [3], [12], [13]
PT	Penetration testing	Perceived use of authorized vulnerability testing and assessment [22], [23], [24]
CS	Cloud security integration	Perceived security practices protecting cloud resources. Not equivalent to CSO [31], [39], [40]
SSDLC	Secure systems development life cycle	Perceived integration of security practices into development [21]
SIF	Security Intelligence Framework	Framework-level outcome in the reported paths.
MA / MS	Model acceptance / model satisfaction	Reported formative evaluation scales.

Model acceptance (MA) and model satisfaction (MS) are reported as formative scales in the original instrument description. They concern respondents' evaluation of the proposed framework. Their conceptual relevance is distinguishable from demonstrated security effectiveness. Because their connection to SIF is unspecified, they are retained as supplementary measurements and are not added to the structural diagram or treated as SIF indicators without supporting records.

D. Hypotheses and Indirect Associations

The following hypotheses make explicit the positive relationships represented in the reported path table. Their formulation in this revision does not establish that directional hypotheses were documented before the original analysis. H1 proposes a positive association between CI and AI. Adaptive computation may support analysis where security information is incomplete or uncertain. H2 proposes a positive association between IA and AI. Agents may support distributed observation and coordinated responses, as illustrated by the technical

approach in [4]. Both hypotheses concern perceived capability; construct overlap remains a measurement concern.

H3 proposes a positive association between AI and PT, because analytic support may assist the prioritization and interpretation of vulnerability tests. H4 proposes a positive association between AI and CS, because detection and analysis capabilities may inform operational controls; the incident-response application in [2] provides a technical motivation. H5 proposes a positive association between AI and SSDLC, because analytic support may inform security decisions during development. Secure development still requires process and organizational practices [5]. H6, H7, and H8 propose positive associations of PT, CS, and SSDLC, respectively, with the SIF evaluation. Their rationale is that testing, operational protection, and development practices address complementary security needs [5], [6]. These hypotheses cannot be adequately evaluated until the SIF measurement model is documented. The model also proposes indirect associations from CI and IA through AI to the security-practice constructs, and onward to SIF. This ordering expresses the proposed mechanism through which intelligence capabilities may be connected to practice. A cross-sectional survey cannot establish that this sequence occurs over time. Specific indirect effects therefore require cautious interpretation and confidence intervals. “Partial mediation” is not established where the corresponding direct relationship between the same antecedent and outcome has not been estimated. Fig. 2 proposed structural paths corresponding to H1–H8. The dashed SIF box indicates an undocumented measurement specification. Arrows represent hypothesized associations, not established causal effects. MA, MS, CSO and governance extensions are not assigned tested structural roles.

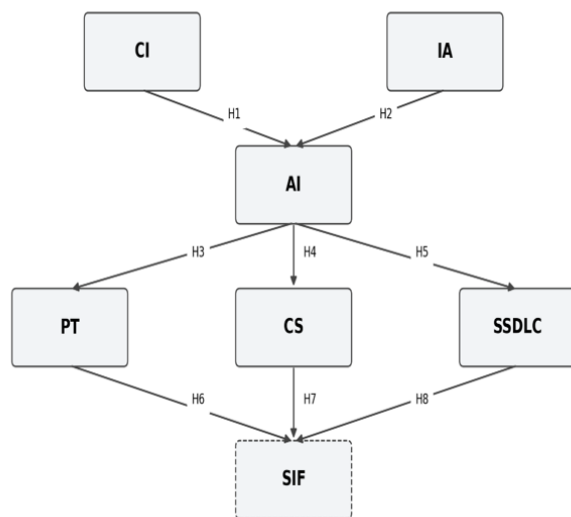


Fig. 2. Proposed structural path to H1-H8.

This study proposes a Security Intelligent Framework (SIF) to enhance risk management and cybersecurity through intelligent monitoring of human activities. Related research highlights the importance of the Secure Systems Development Life-Cycle (SSDLC) in establishing robust security controls [22], [23], which described SSDLC as a process focusing on

security throughout each phase of the system development lifecycle, ensuring security requirements are integrated into every project. Despite its benefits, SSDLC adoption has been limited due to varying organizational needs [24].

This study underscores the necessity of maintaining integrity and adequate documentation within SSDLC to prevent security breaches by ensuring security during systems development. Similarly, penetration testing practices are essential for identifying vulnerabilities in cloud applications [25]. Application of Penetration Testing (PT) reveals threats and potential exploits, underscoring the need for regular PT to protect cloud assets [26]. Understanding and application of PT is crucial for mitigating cyber-attacks [27]. This study proposes a Security Intelligent Framework (SIF) to support cloud security risk management and enhance knowledge distribution, integrating SSDLC and PT for comprehensive security monitoring. In conclusion, knowledge management involves creating, coding, sharing, distributing, and using knowledge. The process should incorporate a secure systems development life-cycle (SSDLC) and ensure cloud security (CS) and penetration testing (PT) are observed to safeguard knowledge resources. In this review study, it can be concluded that PT plays a crucial role in assessing vulnerability [28]. Hence, to enhance knowledge security by preventing knowledge loss and risk during knowledge sharing and distribution within the cloud ecosystem, performing periodic penetration testing is mandatory to assess any form of threats against knowledge sharing and distribution in the cloud.

1) Digital Ecosystem: The increasing dependency on cloud-based infrastructures for knowledge creation, storage, and dissemination has transformed the digital ecosystem into a highly interconnected but vulnerable environment. Cloud computing has enabled organizations to distribute and access data globally, supporting collaboration, scalability, and cost efficiency. However, this advancement comes with significant security risks, including data breaches, insider threats, unauthorized access and ransomware attacks. The use of AI, as identified by [16], is fundamental in artificial immune systems and soft computing, offering solutions for security challenges in digital knowledge processing. AI application in intrusion detection systems provides advanced, adaptable security measures mimicking human logic [17]. Despite its potential, limited attention to AI has impacted economic growth and organizational welfare, emphasizing the critical role of AI in data sharing [19]. [18] emphasized the role of intelligent agents (IA) in security, advocating for their use in continuous monitoring and proactive threat prevention. [20] explored AI capabilities in providing basic defenses for cloud security, including access control, authentication, and intrusion detection. Despite advancements in policies and technologies like PKI and SSL, AI remains crucial in addressing cloud security risks [21]. This study proposes a Security Intelligent Framework (SIF) to enhance risk management and cybersecurity through intelligent monitoring of human activities.

Related research highlights the importance of the Secure Systems Development Life-Cycle (SSDLC) in establishing robust security controls [22] and [23], which described SSDLC as a process focusing on security throughout each phase of the system development lifecycle, ensuring security requirements are integrated into every project. Despite its benefits, SSDLC

adoption has been limited due to varying organizational needs [24]. This study underscores the necessity of maintaining integrity and adequate documentation within SSDLC to prevent security breaches by ensuring security during systems development. Similarly, penetration testing practices are essential for identifying vulnerabilities in cloud applications [25]. Application of Penetration Testing (PT) reveals threats and potential exploits, underscoring the need for regular PT to protect cloud assets [26]. Understanding and application of PT is crucial for mitigating cyber-attacks [27]. This study proposes a Security Intelligent Framework (SIF) to support cloud security risk management and enhance knowledge distribution, integrating SSDLC and PT for comprehensive security monitoring. In conclusion, knowledge management involves creating, coding, sharing, distributing, and using knowledge. The process should incorporate a secure systems development life-cycle (SSDLC) and ensure cloud security (CS) and penetration testing (PT) are observed to safeguard knowledge resources. In this review study, it can be concluded that PT plays a crucial role in assessing vulnerability [28]. Hence, to enhance knowledge security by preventing knowledge loss and risk during knowledge sharing and distribution within the cloud ecosystem, performing periodic penetration testing is mandatory to assess any form of threats against knowledge sharing and distribution in the cloud.

The Global Cybersecurity Outlook 2025 by the World Economic Forum highlights a 62% rise in targeted attacks on cloud-based infrastructures since 2022, underscoring the urgent need for intelligent, adaptive, and proactive security frameworks [29]. In the contemporary digital ecosystem, knowledge is a strategic asset, an intangible capital that drives innovation, competitiveness, and decision-making. Knowledge distribution across cloud environments depends on secure and reliable infrastructure; yet traditional cybersecurity mechanisms often fail to protect knowledge in transit or during collaborative exchanges. The complexity of knowledge representation and sharing in distributed environments has intensified the need for intelligent, context-aware, and self-learning security models [30]. Despite advances in encryption, access control, and identity management, many existing frameworks focus primarily on protecting data rather than knowledge, leaving significant vulnerabilities in systems that integrate artificial intelligence and knowledge management [31]. Recent trends in Artificial Intelligence (AI) and Computational Intelligence (CI) offer promising directions for strengthening cloud security. AI-driven approaches such as deep learning-based intrusion detection, autonomous penetration testing, and predictive analytics allow systems to detect, learn, and respond to threats dynamically [32]. Similarly, Intelligent Agents (IA) can simulate human-like reasoning to autonomously monitor, prevent, and mitigate risks within cloud environments [33]. There remains a critical knowledge gap between traditional cybersecurity measures and intelligent knowledge protection mechanisms. Most security frameworks are reactive and data-centric, lacking semantic awareness of knowledge structures and ontologies that govern information sharing in cloud ecosystems. As organizations integrate Generative AI and Large Language Models (LLMs) into their operations, the boundaries between data, information, and knowledge are increasingly blurred, posing new challenges to privacy, intellectual property, and governance [9]. This calls for a multi-layered, intelligent security framework capable of

learning from dynamic threats while ensuring the integrity and confidentiality of shared knowledge assets.

2) Overview of Cloud Security and Knowledge Protection: Cloud computing has become a cornerstone of digital transformation, providing scalable infrastructure for data management, analytics, and knowledge dissemination. However, as organizations increasingly rely on distributed and virtualized infrastructures, the exposure to cyber threats and knowledge leakage has grown exponentially [34], [35]. Unlike traditional IT environments, cloud ecosystems are characterized by multi-tenancy, virtual networking, and dynamic provisioning, which complicate the enforcement of consistent security policies. These complexities create vulnerabilities during data transmission, storage, and access, particularly when dealing with knowledge risk that arises from digital platforms [35].

Recent research emphasizes the necessity of knowledge-centric security rather than merely data-centric protection [36]. Knowledge security involves safeguarding the processes of creation, transfer, and application of knowledge within cloud-based systems. This paradigm recognizes that data, once contextualized and interpreted, transforms into organizational knowledge, making it a high-value target for adversaries and competitors [37], [38], [39]. Therefore, effective cloud security must integrate both technical intelligence (AI, CI, IA) and organizational intelligence (policies, standards, and ethics) to ensure resilient knowledge distribution.

3) Ontology-Based Cloud Security Models: Ontologies play a pivotal role in structuring and semantically linking data to facilitate secure knowledge representation and exchange. The Cloud Computing Ontology (CCO), introduced by [5], remains foundational in understanding the layered architecture of cloud ecosystems comprising Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Recent works have expanded this model to include Data-as-a-Service (DaaS) and Security-as-a-Service (SECaaS), emphasizing the need for layered protection across interconnected systems [38], [40]. Emerging research applies ontology-based reasoning to detect and mitigate vulnerabilities in cloud ecosystems [38], [42]. For example, ontology-driven intrusion detection systems (O-IDS) leverage semantic patterns to identify abnormal behavior in distributed environments. These systems can model complex relationships between entities such as users, data types, and applications to enhance visibility and traceability. Integrating ontological security with AI-based reasoning mechanisms has also enabled real-time risk assessments, ensuring that knowledge distribution and leverage adhere to compliance and trust standards [39], [40]. Despite these advancements, gaps remain in integrating cloud ontologies with intelligent, self-learning security models. Many existing systems lack adaptive feedback mechanisms and semantic interoperability, which are crucial for managing heterogeneous data sources and complex knowledge flows. This limitation highlights the need for a unified, intelligent framework that combines ontological reasoning with adaptive AI capabilities.

4) The Convergence of AI, CI, and IA in Security: The synergy between Artificial Intelligence (AI), Computational Intelligence (CI), and Intelligent Agents (IA) forms the foundation for next-generation cloud security systems. AI techniques such as machine learning (ML), deep learning (DL), and neural networks have proven effective in anomaly detection,

malware analysis, and threat prediction [40], [41], [42]. Computational Intelligence complements these approaches through fuzzy logic, evolutionary algorithms, and swarm optimization, enabling systems to adapt to uncertainty and incomplete data [41], [45]. Intelligent Agents, modelled on cognitive and behavioral theories, provide autonomy, adaptability, and reasoning, key attributes for continuous security monitoring. IA-based system can perform autonomous scanning, real-time alerting, and even self-healing actions in response to detected anomalies [50]. The fusion of AI–CI–IA within cloud security leads to a paradigm known as Security Intelligence (SI), where systems evolve dynamically to counter sophisticated attacks. However, the challenge lies in synchronizing these components within a unified architectural framework. Many existing studies isolate AI models from human-in-the-loop mechanisms or overlook the semantic dimensions of knowledge protection. Therefore, a more integrated model, as proposed in this study's Security Intelligence Framework (SIF), to leverage knowledge security across a broad spectrum.

5) *Emerging Paradigms: Zero Trust, Blockchain, and Generative AI:* The emergence of Zero Trust Architecture (ZTA) has redefined cybersecurity from a perimeter-based to an identity-based approach. ZTA operates under the principle of “never trust, always verify,” applying strict authentication and continuous validation for every user and device [42], [47]. Integrating SIF within Zero Trust environments enhances its intelligence by enabling contextual access control and adaptive verification based on AI-driven trust scoring [43]. Similarly, Blockchain technology contributes to immutable auditability and decentralized trust. Studies demonstrate its potential for secure knowledge provenance, ensuring that every modification to knowledge assets is transparently recorded [44], [49]. The integration of blockchain with AI strengthens data traceability, while smart contracts automate security enforcement and access control. This convergence offers a resilient infrastructure for knowledge lifecycle management in distributed cloud systems. Furthermore, Generative AI (GenAI) is rapidly transforming knowledge creation and distribution. While GenAI tools (e.g., ChatGPT, Claude, Gemini) enhance productivity, they also introduce novel security risks such as prompt injection, data poisoning, and unauthorized knowledge synthesis [45]. Researchers now emphasize AI governance frameworks and ethical auditing models to balance innovation with privacy and intellectual property protection [46], [47]. Integrating GenAI risk mitigation into SIF ensures alignment with modern AI safety standards.

6) *Gaps in Existing Studies:* Despite the vast body of research on cloud security, three major gaps persist:

- 1) **Fragmented Integration:** existing models rarely combine AI, CI, and IA within a single, empirically validated framework.
- 2) **Neglect of Knowledge Semantics:** current security mechanisms focus on data protection rather than safeguarding the knowledge lifecycle creation, sharing, and utilization.
- 3) **Limited Empirical Validation:** few studies test integrated frameworks across organizational contexts to assess reliability and scalability

This study addresses these gaps by proposing a Security Intelligence Framework (SIF) that unites AI, CI, IA, SSDLC,

PT, and CS into a cohesive system. Unlike prior models, the SIF is designed for continuous learning, semantic awareness, and proactive adaptation, thereby redefining how organizations protect and distribute knowledge in the cloud. Fig. 3 illustrates how SIF can address the gap. The conceptual framework (illustrated in Fig. 2) integrates Computational Intelligence (CI) and Intelligent Agents (IA) as core enablers of Artificial Intelligence (AI) within the Secure Systems Development Life Cycle (SSDLC). Penetration Testing (PT) and Cloud Security (CS) serve as operational mechanisms validating security robustness. The Security Intelligence Framework (SIF) represents the culmination of these interrelated components, driving secure knowledge sharing and distribution within cloud ecosystems. The visually mapped AI, CI, and IA relationships with SSDLC, PT, and CS layers, demonstrating feedback loops for adaptive learning and security reinforcement. Fig. 3 illustrates the conceptual framework for the Security Intelligence Framework (SIF) with adaptive learning and security reinforcement feedback.

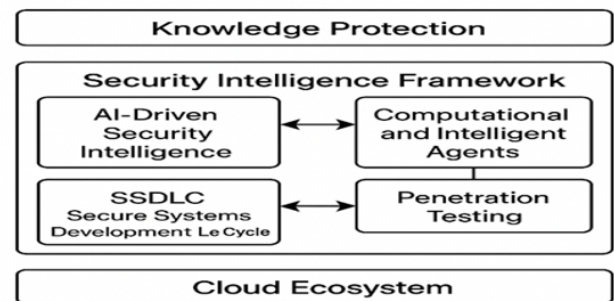


Fig. 3. Security Intelligence Framework (SIF).

III. METHODOLOGY

This study targeted three public organizations and two private organizations, collecting data through quantitative-based questionnaires. Each organization provided 100 responses, resulting in a total sample size of 500 respondents, all of whom are knowledge management and cybersecurity professionals.

A. Design and Sampling

The study used a cross-sectional, descriptive explanatory questionnaire design. The reported sample comprises 500 professionals from five organizations in Malaysia: three public and two private organizations, each contributing 100 responses. The target population included information technology professionals, cybersecurity specialists, and knowledge-management officers. Purposive sampling was used to recruit participants with relevant experience, with a stated eligibility requirement of at least five years of experience in one of these areas.

These eligibility criteria do not establish that every participant had equivalent cloud-security expertise. The equal organizational counts describe the obtained sample, not a probability sample of organizations or professionals. The design is subject to selection bias and cannot support population-representative estimates. Moreover, responses are nested within organizations; shared practices may induce dependence, and

500 individual responses should not be interpreted as 500 independent organizational observations.

PLS-SEM was chosen to examine a multiconstruct model with reported reflective and formative measurements. Its use should be justified by the model's measurement assumptions and analytical aims [7]. Sample size alone does not establish adequate power, correct specification, representativeness, or measurement quality.

B. Questionnaire and Pilot Study

The structured questionnaire contained demographic and organizational questions; items relating to AI, CI, IA, CS, PT, and SSDLC; and MA and MS scales. Responses used a five-point scale from 1 (strongly disagree) to 5 (strongly agree). The manuscript reports review by five domain experts and a pilot involving 30 participants, with pilot Cronbach's alpha above 0.80. Construct-specific pilot statistics and the item revision record are needed to assess those claims.

C. Data Collection

The manuscript reports electronic distribution through survey links, voluntary participation, informed consent, anonymity, and screening in IBM SPSS Statistics 29 before analysis. It reports 500 complete responses and no missing values in the retained dataset. This does not establish the absence of incomplete submissions or exclusions before retention.

D. Measurement and Structural Assessment

For reflective constructs, the assessment should report outer loadings, Cronbach's alpha, composite reliability, and average variance extracted (AVE). Conventional guides include loadings near or above 0.708, internal consistency of approximately 0.70–0.95, and AVE of at least 0.50 [7]. Lower loadings require examination of content validity and measurement quality; indicators should not be removed solely to improve a numerical threshold. Reliability coefficients above a threshold do not establish discriminant validity. The Fornell–Larcker matrix is retained as a descriptive check. The heterotrait–monotrait ratio (HTMT) and its bootstrap intervals should be reported because reliance on the Fornell–Larcker criterion alone can fail to identify measurement problems [8]. A threshold of 0.85 is a conservative guide, while 0.90 can be considered for closely related constructs with a substantive justification. The criterion should be selected consistently and supported by the measurement design. For formative scales, content coverage, convergent validity through an appropriate redundancy analysis, indicator collinearity, and the significance and relevance of outer weights need assessment [7].

Indicator VIFs should be distinguished from the inner VIFs for structural predictors. No inner VIF conclusion can be inferred from the MA/MS table. Structural assessment should report path estimates with bootstrap standard errors, confidence intervals and p values; R^2 and adjusted R^2 for endogenous constructs; and predictor-specific f^2 . R^2 describes explained in-sample variance. Out-of-sample predictive performance requires a separate assessment, such as PLSpredict with prediction errors compared with appropriate benchmarks [9]. For an individual predictor, $f^2 = (R^2_{\text{included}} - R^2_{\text{excluded}})/(1 - R^2_{\text{included}})$; values of 0.02, 0.15 and 0.35 are conventional guides for small,

medium and large effects, subject to context [7]. For PLS predict, Q^2 predict above zero indicates improvement over a mean-based benchmark, and prediction errors should also be compared with a linear-model benchmark [9]. These criteria must not be conflated with technical security performance. The source reports 5,000 bootstrap resamples. Bootstrapping permits estimation of sampling uncertainty for paths and indirect effects [10]. However, the supplied files do not document sufficient settings to reproduce the inference. Because a priori directional testing is not established, the revised analysis should use two-sided tests and 95% bootstrap confidence intervals unless dated study documentation supports a different choice.

IV. RESULTS AND VERIFICATION STATUS

A. Reflective Measurement Results

Table III transcribes the measurement statistics reported in the source. Cronbach's alpha ranges from 0.854 to 0.908, composite reliability from 0.893 to 0.929, and AVE from 0.585 to 0.688. These ranges replace the conflicting ranges in the original narrative. The AVE and composite reliability values can be reproduced approximately from the rounded loadings using the usual standardized-indicator formulae, which supports transcription consistency but does not independently validate the data or alpha values.

TABLE III. REPORTED REFLECTIVE MEASUREMENT STATISTICS

Construct	Loading in item order 1 to 6	Alpha	CR	AVE
AI	0.867, 0.728, 0.854, 0.670, 0.624, 0.834	0.857	0.895	0.591
PT	0.827, 0.851, 0.862, 0.719, 0.842, 0.826	0.904	0.926	0.677
CS	0.859, 0.819, 0.914, 0.738, 0.751, 0.880	0.908	0.929	0.688
CI	0.826, 0.715, 0.860, 0.677, 0.626, 0.852	0.854	0.893	0.585
IA	0.882, 0.773, 0.872, 0.689, 0.557, 0.828	0.860	0.898	0.601
SSDLC	0.843, 0.855, 0.860, 0.717, 0.811, 0.830	0.903	0.925	0.674

Note: CR = composite reliability; AVE = average variance extracted. Item codes follow construct name plus item number. SIF indicators were not supplied.

The reported loadings range from 0.557 to 0.914. AI4, AI5, CI4, CI5, IA4, and IA5 are below approximately 0.708 and merit substantive review. The source does not supply item wording or loading-level bootstrap results, so claims that every loading is statistically significant have been removed. Table III omits SIF measurement indicators, preventing a complete evaluation of the outcome construct.

B. Discriminant Validity and Collinearity

Diagonal entries are reported square roots of AVE. The CS entry 0.834 is inconsistent with the reported AVE of 0.688 and requires verification. PT and CS replace the the inconsistent source labels APT and CCS.

The displayed diagonal values exceed the corresponding off-diagonal correlations for the six listed constructs. However, the CS diagonal in the source is 0.834, whereas $\sqrt{0.688}$ is approximately 0.829. Table IV retains the source value and

TABLE IV. FORNELL-LACKER MATRIX

Variable	AI	APT	CCS	CI	IA	SSDLC
AI	0.769	0.344	0.471	0.451	0.487	0.263
APT	0.344	0.823	0.196	0.294	0.339	0.768
CCS	0.471	0.196	0.834	0.506	0.436	0.167
CI	0.451	0.294	0.506	0.765	0.651	0.241
IA	0.487	0.339	0.436	0.651	0.775	0.273
SSDLC	0.263	0.768	0.167	0.241	0.273	0.821

Note: Bold diagonal values represent the square root of the Average Variance Extracted ($\sqrt{AVE}$); off-diagonal values are inter-construct correlations. Each $\sqrt{AVE}$ value exceeds the corresponding correlations with other constructs, supporting discriminant validity.

explicitly flags the discrepancy rather than silently selecting a replacement. PT and SSDLC also have a high reported correlation of 0.768, which warrants examination of their item content and HTMT result. Full HTMT results, associated intervals, and SIF correlations are absent. Discriminant validity therefore cannot be confirmed for the complete model. The formative VIFs reported for MA and MS range from 1.454 to 4.570 (Appendix, Table VIII). These values are below five, but several exceed three. The original statement that all VIFs are below three is incorrect. Formative-indicator values do not establish that the structural model is free of collinearity. Inner VIFs remain to be supplied.

C. Direct Relationships

TABLE V. DIRECT PATH

ID	Path	β	SE	t	p
H1	CI $\rightarrow$ AI	0.425	0.073	5.849	<0.001
H2	IA $\rightarrow$ AI	0.568	0.073	7.766	<0.001
H3	AI $\rightarrow$ PT	0.344	0.049	7.039	<0.001
H4	AI $\rightarrow$ CS	0.471	0.048	9.712	<0.001
H5	AI $\rightarrow$ SSDLC	0.263	0.049	5.337	<0.001
H6	PT $\rightarrow$ SIF	0.219	0.067	3.263	0.001
H7	CS $\rightarrow$ SIF	0.185	0.044	4.222	<0.001
H8	SSDLC $\rightarrow$ SIF	0.216	0.070	3.076	0.002

Note: SE = reported bootstrapped standard error. Reported $p = 0.000$ is displayed as $p < 0.001$.

Table V preserves the reported estimates for auditability, with terminology and p-value display standardized. The positive coefficients are consistent with the proposed direction of H1–H8. They are not presented as verified hypothesis decisions because the SIF measurement specification and the model-wide consistency checks remain unresolved. The reported direct-path t values are compatible with the rounding precision of the coefficients and standard errors; unrounded outputs are still needed to reproduce the inference.

The AI–CS, AI–PT, and AI–SSDLC coefficients are reported as 0.471, 0.344, and 0.263, respectively. These describe modelled associations among survey constructs. They do not quantify changes in detection accuracy, vulnerability reduction, development defects, or the incidence of knowledge loss.

D. Explained Variance and Internal Consistency

The reported SSDLC and PT values correspond to 6.9% and 11.8% explained variance and should be described as low (Table VI). The CS value corresponds to 22.1%. These

TABLE VI. VARIANCE AND INTERPRETATION

Outcome	Reported R^2	Interpretation
AI	0.865	Inconsistent with coefficients and correlations
SSDLC	0.069	Low explained variance, 6.9%.
PT	0.118	Low explained variance, 11.8%.
CS	0.221	22.1% explained variance; substantial variation remains unexplained.
SIF	0.230	23.0% reported; outcome measurement requires documentation.

Note: SE = reported bootstrapped standard error. Reported $p = 0.000$ is displayed as $p < 0.001$.

results leave considerable variation unexplained. The SIF value of 23.0% is provisional because its measurement is undocumented. No value establishes out-of-sample prediction or operational security effectiveness. The reported AI R^2 of 0.865 is incompatible with the displayed coefficients and correlations if they refer to the same standardized model in which CI and IA are the only predictors of AI. Specifically, $\beta' r = (0.425 \times 0.451) + (0.568 \times 0.487) = 0.468291$. This is a diagnostic calculation, not a corrected estimate. Using the predictor correlation of 0.651 gives $\beta' R_X \beta = 0.817552$, which also differs from 0.865 and from $\beta' r$. The same correlation matrix implies coefficients of approximately 0.232 and 0.336, rather than 0.425 and 0.568. A single numerical substitution would therefore conceal a wider inconsistency. The source reports a standardized root mean square residual (SRMR) of 0.054, but its model type and supporting export are not supplied. It is retained here only as an unverified reported value and is not used to establish model validity. The supplied manuscript contains no numerical f^2 , Q^2 , output. Statements that all Q^2 values are positive and that predictive validity has been established have therefore been removed.

E. Specific Indirect Relationships

TABLE VII. SPECIFIC INDIRECT EFFECTS

Path	β	SE	t	p
CI $\rightarrow$ AI $\rightarrow$ PT	0.146	0.032	4.594	<0.001
AI $\rightarrow$ SSDLC $\rightarrow$ SIF	0.057	0.022	2.604	0.009
IA $\rightarrow$ AI $\rightarrow$ SSDLC	0.149	0.036	4.151	<0.001
IA $\rightarrow$ AI $\rightarrow$ CS $\rightarrow$ SIF	0.049	0.015	3.404	0.001
CI $\rightarrow$ AI $\rightarrow$ PT $\rightarrow$ SIF	0.032	0.012	2.765	0.006
IA $\rightarrow$ AI $\rightarrow$ PT	0.195	0.039	4.961	<0.001
CI $\rightarrow$ AI $\rightarrow$ CS $\rightarrow$ SIF	0.037	0.012	3.104	0.002
CI $\rightarrow$ AI $\rightarrow$ SSDLC $\rightarrow$ SIF	0.024	0.010	2.403	0.004
AI $\rightarrow$ CS $\rightarrow$ SIF	0.087	0.023	3.790	<0.001
IA $\rightarrow$ AI $\rightarrow$ SSDLC $\rightarrow$ SIF	0.032	0.013	2.409	0.016
IA $\rightarrow$ AI $\rightarrow$ PT $\rightarrow$ SIF	0.043	0.016	2.681	0.008
IA $\rightarrow$ AI $\rightarrow$ CS	0.267	0.041	6.534	<0.001
AI $\rightarrow$ PT $\rightarrow$ SIF	0.075	0.025	3.042	0.002
CI $\rightarrow$ AI $\rightarrow$ SSDLC	0.112	0.028	4.037	<0.001
CI $\rightarrow$ AI $\rightarrow$ CS	0.200	0.043	4.642	<0.001

Table VII preserves the 15 reported indirect effects. The coefficient products are broadly compatible with the rounded direct paths, but this arithmetic agreement does not establish measurement validity or resolve the inconsistent AI model. In particular, the reported CI $\rightarrow$ AI $\rightarrow$ SSDLC $\rightarrow$ SIF row combines $t = 2.403$ with $p = 0.004$, which requires verification of the p -value calculation and testing convention. Confidence intervals are unavailable.

These results can be described only as reported indirect

associations pending reconciliation. The cross-sectional design does not establish temporal ordering, causal mediation, or that deploying AI would improve the downstream outcomes. The original “partial mediation” conclusion has been removed because corresponding direct paths for the same antecedent–outcome pairs are not reported.

V. DISCUSSION

A. Interpretation and Comparison

The proposed model offers a way to examine how intelligence capabilities may be associated with security practices relevant to knowledge protection. A plausible interpretation of a positive AI–CS association is that professionals who perceive stronger analytic capabilities also perceive more developed cloud-security practices. Common organizational investment, respondent optimism, overlapping items, or shared method variance could also produce this association. The present design cannot distinguish these explanations.

The technical evaluations in [2] and [4] demonstrate the kind of attack-dataset evidence needed to assess implemented detection systems. This survey addresses a different question about perceived capability and practice. The knowledge-representation approach in [3] motivates future semantic integration, but semantic reasoning was not operationalized as a survey construct or tested technically here. Consequently, the study does not show that the SIF outperforms those approaches.

The low SSDLC and PT R values are consistent with an incomplete account of those practices. Development processes, available expertise, testing scope, budgets, and governance are plausible additional influences, but their effects were not estimated. The relative sizes of the AI–CS and AI–PT coefficients should not be interpreted as evidence that one operational intervention is superior; such a claim would require a suitable comparative design.

B. Research Objectives and Implications

The first objective is addressed by the explicit definitions and the proposed path structure in Fig. 1. The second objective is addressed only provisionally: Tables V and VII present reported associations, but complete assessment of H1–H8 and the indirect pathways requires verified measurement and structural outputs. The third objective is addressed by the validation priorities in Section 6. This distinction avoids presenting unresolved analyses as completed empirical validation.

The conceptual implication is that knowledge protection may be studied through the coordination of analytic capabilities and security practices, while retaining knowledge-specific outcomes as a separate requirement. The distinction between CI, IA, and AI must be demonstrated empirically because these domains overlap. MA and MS may inform evaluation of a proposed framework, but acceptance or satisfaction cannot stand in for objective protection outcomes.

For managers, the framework can structure discussions among security teams, developers, and knowledge managers about where intelligence may support existing controls. Any implementation should specify the knowledge assets, threats,

authorized actions, human review points, and measurable outcomes. The survey does not justify removing human oversight, automating penetration testing without defined scope, or assuming that an accepted framework will improve security.

C. Proposed Extensions

A CSO could represent knowledge assets, threats, vulnerabilities, permissions, and control relationships in a future implementation. This would require an explicit ontology, competency questions, validation cases, and evidence that semantic reasoning improves a relevant outcome. CS in the current survey must not be relabeled CSO without such operationalization.

Zero Trust could inform resource access decisions in a future SIF implementation. NIST SP 800-207 describes resource-centred access principles and rejects implicit trust based only on network location or ownership [11]. Blockchain auditability is a separate design option whose benefit would need comparison with conventional tamper-evident audit logs, including cost, privacy, and governance considerations. Neither extension was evaluated in this survey.

AI governance would also require explicit evaluation criteria. The NIST AI Risk Management Framework offers a basis for considering risks and trustworthiness across the AI life cycle [12], [13], [16]. Explainability, accountability, human oversight, and privacy should be specified and assessed in future work rather than described as demonstrated features of the present SIF. Generative-AI security and knowledge authenticity are further research topics, not findings of this study.

D. Limitations and Future Research

The cross-sectional design limits causal inference and prevents evaluation of temporal adaptation. Self-reported measures are vulnerable to common-method variance, recall error, social-desirability bias, and differences in respondents’ interpretation of the constructs. Anonymity and consent do not demonstrate that these biases are absent. Purposive recruitment from five organizations restricts transferability, and the clustered data structure raises additional questions about independence and uncertainty estimation.

The most immediate limitation is incomplete and internally inconsistent statistical reporting. SIF measurement, the MA/MS relationship to the structural model, full HTMT results, inner VIFs, effect sizes, bootstrap intervals, and prediction outputs are missing. The conflicting AI results must be reconciled before the study can support final hypothesis decisions. The pilot and main-survey timeline also require documentary confirmation.

No deployed cloud environment, attack simulation, throughput test, incident-response assessment, or observed knowledge-loss outcome was evaluated. Technical effectiveness, scalability, real-time operation, and generalizability therefore remain unestablished. The framework’s proposed semantic and governance extensions also remain unevaluated.

Future work should first reproduce the survey analysis from a documented instrument and consistent dataset, address organizational clustering, and distinguish overlapping constructs.

A subsequent study could use longitudinal observations or a controlled implementation to examine changes in security practices and outcomes. Technical evaluation should compare the SIF implementation with specified baselines using measures such as detection precision and recall, false-alarm rate, response time, confirmed knowledge-exfiltration incidents, and system overhead. Tests across organizations and workloads would be needed before claims about scalability or broader applicability.

VI. CONCLUSION

This study proposes an AI-driven Security Intelligence Framework linking intelligence capabilities with development, testing, and cloud-security practices relevant to knowledge protection. The survey of 500 professionals provides reported associations for further examination, but inconsistencies in the structural results and missing measurement details prevent a definitive validation claim. In particular, the low reported explained variance for SSDLC and PT must be acknowledged, and the AI R^2 must be reconciled with the model's coefficients and correlations.

The contribution is a conceptual integration and a clearly bounded programme of empirical evaluation. The framework should be regarded as a candidate model pending statistical verification and technical testing. Claims of improved protection, predictive accuracy, scalability, or causal mediation require additional evidence. Ontology-based reasoning, Zero Trust, blockchain auditability, and AI governance remain proposed extensions.

ACKNOWLEDGMENT

Acknowledgment to the Ministry of Higher Education Malaysia for the Fundamental Research Grant Scheme with Project Code: FRGS/1/2020/ICT02/USM/02/4.

DECLARATIONS

The authors declare no conflict of interest.

REFERENCES

- [1] S. Durst and M. Zieba, "Mapping knowledge risks: towards a better understanding of knowledge management," *Knowledge Management Research & Practice*, vol. 17, no. 1, pp. 1–13, 2019, doi: 10.1080/14778238.2018.1538603.
- [2] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 3, pp. 623–643, 2025, doi: 10.1109/TMLCN.2025.3564912.
- [3] S. Mittal, A. Joshi, and T. Finin, "Cyber-All-Intel: An AI for security related threat intelligence," *arXiv preprint, arXiv:1905.02895*, 2019. [Online]. Available: <https://arxiv.org/abs/1905.02895>
- [4] N. A. M. Alhammadi and M. Mabrouk, "A multi-agent-based deep learning model for protecting cloud computing environment against distributed denial of service flooding attacks," *Journal of Soft Computing and Data Mining*, vol. 6, no. 1, pp. 406–422, 2025. [Online]. Available: <https://journal.uthm.edu.my/index.php/jscdm/article/view/22174>
- [5] M. Souppaya, K. Scarfone, and D. Dodson, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for mitigating the risk of software vulnerabilities," *National Institute of Standards and Technology*, NIST SP 800-218, 2022, doi: 10.6028/NIST.SP.800-218.
- [6] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," *National Institute of Standards and Technology*, NIST SP 800-115, 2008, doi: 10.6028/NIST.SP.800-115.
- [7] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2–24, 2019, doi: 10.1108/EBR-11-2018-0203.
- [8] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, vol. 43, pp. 115–135, 2015, doi: 10.1007/s11747-014-0403-8.
- [9] G. Shmueli, M. Sarstedt, J. F. Hair, J.-H. Cheah, H. Ting, S. Vaithilingam, and C. M. Ringle, "Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict," *European Journal of Marketing*, vol. 53, no. 11, pp. 2322–2347, 2019, doi: 10.1108/EJM-02-2019-0189.
- [10] SmartPLS, "Bootstrapping in PLS-SEM," *SmartPLS Documentation*. [Online]. Available: <https://www.smartpls.com/documentation/algorithms-and-techniques/resampling-and-inference/bootstrapping/>. [Accessed: Oct. 14, 2026].
- [11] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *National Institute of Standards and Technology*, NIST SP 800-207, 2020, doi: 10.6028/NIST.SP.800-207.
- [12] E. Tabassi, "Artificial intelligence risk management framework (AI RMF 1.0)," *National Institute of Standards and Technology*, NIST AI 100-1, 2023, doi: 10.6028/NIST.AI.100-1.
- [13] B.-h. Li, B.-c. Hou, W.-t. Yu, X.-b. Lu, and C.-w. Yang, "Applications of artificial intelligence in intelligent manufacturing: a review," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 1, pp. 86–96, 2017.
- [14] A. Kayid, "The role of Artificial Intelligence in future technology," *Department of Computer Science, The German University in Cairo*, 2020.
- [15] V. K. Pappakrishnan, R. Mythili, V. Kavitha, and N. Parthiban, "Role of Artificial Intelligence of Things (AIoT) in Covid-19 Pandemic: A Brief Survey," *IoTBDs*, pp. 229–236, 2021.
- [16] C.-H. Lu, "The impact of artificial intelligence on economic growth and welfare," *Journal of Macroeconomics*, vol. 69, p. 103342, 2021.
- [17] H. M. Said and A.-B. M. Salem, "Exploiting computational intelligence paradigms in e-technologies and activities," *Procedia Computer Science*, vol. 65, pp. 396–405, 2015.
- [18] A. Korinek, M. Schindler, and J. Stiglitz, "Technological progress, artificial intelligence, and inclusive growth," *International Monetary Fund*, 2021.
- [19] A. A. Gutierrez, "SECURETI: ADVANCED SDLC AND PROJECT MANAGEMENT TOOL FOR TI (PHILIPPINES)," *International Journal of Computer Science & Information Technology*, vol. 13, no. 6, 2021.
- [20] K. Sahu, R. Shree, and R. Kumar, "Risk management perspective in SDLC," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 3, 2014.
- [21] A. Alshamrani and A. Bahattab, "A comparison between three SDLC models waterfall model, spiral model, and Incremental/Iterative model," *International Journal of Computer Science Issues (IJCSI)*, vol. 12, no. 1, p. 106, 2015.
- [22] S. Umrao, M. Kaur, and G. K. Gupta, "Vulnerability assessment and penetration testing," *International Journal of Computer & Communication Technology*, vol. 3, no. 6-8, pp. 71–74, 2012.
- [23] S. R. Mamilla, "A Study of Penetration Testing Processes and Tools," *Master's Project, California State University, San Bernardino*, 1220, 2021.
- [24] S. Yadav and P. Singh, "Web Application and Penetration Testing," *Journal of Informatics Electrical and Electronics Engineering (JIEEE)*, vol. 1, no. 2, pp. 1–11, 2020.
- [25] G. Aileen and G. Bacudio, "An overview of penetration testing," *International Journal of Network Security Its Applications (IJNSA)*, vol. 3, no. 6, 2011.
- [26] World Economic Forum, "Global Cybersecurity Outlook 2025," *Tech. Rep., World Economic Forum, Geneva, Switzerland*, 2025.
- [27] L. H. Bayzid, T. S. Kar, M. T. Islam, M. S. Islam, D. Özkan, and A. Mishra, "Agile project management," 2025.

- [28] P. L. Mkhize, "Knowledge Management in the Digital Age: A Systematic Review of Fourth Industrial Revolution Technologies and Sustainable Transformation," *South African Journal of Information Management*, vol. 28, no. 1, p. 2083, AOSIS, 2026.
- [29] H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, "Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research," *International Journal of Multidisciplinary Sciences and Arts*, vol. 3, no. 1, pp. 242–251, IJMSA, 2024.
- [30] W. Xiang, C. Han, Z. Lin, Y. Li, Y. Sun, and X. Lin, "Inference-Subgraph Driven Multi-Agent DRL for Joint Resource Orchestration in Communication and Computing Power Network," *IEEE Transactions on Network Science and Engineering*, vol. 13, pp. 4616–4635, 2025.
- [31] B. Zhang, H. Pan, K. Li, Y. Xing, J. Wang, D. Fan, and W. Zhang, "A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing," *Electronics*, vol. 13, no. 21, p. 4260, MDPI, 2024.
- [32] M. Zieba, S. Durst, and M. Skorupko, "Knowledge Risks Arising from Digitalization," in *Proceedings of the International Forum on Knowledge Asset Dynamics (IFKAD 2023): Managing Knowledge for Sustainability*, pp. 38–47, 2023.
- [33] J. Singh, K. K. Pandey, A. Kumar, F. Naz, and S. Luthra, "Drivers, barriers and practices of net zero economy: An exploratory knowledge-based supply chain multi-stakeholder perspective framework," *Operations Management Research*, vol. 16, no. 3, pp. 1059–1090, Springer, 2023.
- [34] A. S. A. Alsaif, "SA-HEIKSP: development and empirical validation of a cloud-based adoption framework for cross-institutional knowledge sharing in Saudi higher education institutions," *Doctoral dissertation, University of Sussex*, 2026.
- [35] P. Okanda and S. Muriithi, "An Adaptive Architecture for Cybersecurity Threat Intelligence: A Case Study on Kenyan Courts," *Southern African Journal of Security*, vol. 3, pp. 1–30, Unisa Press, 2025.
- [36] J. Orjatsalo, H. Hussinki, and A. Kianto, "The Role of Knowledge-Based Resources in Leveraging Business Analytics," *Knowledge and Process Management*, vol. 33, no. 2, pp. 213–231, John Wiley & Sons, Ltd, 2026.
- [37] R. Mittal, I. Cvejić, D. Peraković, and S. P. Raja, "Proactive detection and mitigation strategies for advanced persistent threats," *Promet-Traffic & Transportation*, vol. 37, no. 3, pp. 546–569, 2025.
- [38] H. Jodlbauer and S. Tripathi, "Analytical comparison of cross impact steady state, DEMATEL, and page rank for analyzing complex systems," *Expert Systems with Applications*, vol. 225, p. 120154, Elsevier, 2023.
- [39] D. P. Möller, "NIST cybersecurity framework and MITRE cybersecurity criteria," in *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices*, pp. 231–271, Springer, 2023.
- [40] G. Freed and M. Jackson, "Zero trust architecture in AI-driven cybersecurity: a machine learning perspective," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 5, no. 2, pp. 67–82, 2022.
- [41] C. Zhang, Y. Xu, Y. Hu, J. Wu, J. Ren, and Y. Zhang, "A blockchain-based multi-cloud storage data auditing scheme to locate faults," *IEEE Transactions on Cloud Computing*, vol. 10, no. 4, pp. 2252–2263, IEEE, 2021.
- [42] P. H. B. Correia, R. W. Achjian, D. E. G. De Oliveira, Y. A. Maria, V. T. Hayashi, M. Lopes, C. C. Miers, and M. A. Simplicio Jr, "A systematic literature review on llm defenses against prompt injection and jail-breaking: Expanding NIST taxonomy," *arXiv preprint arXiv:2601.22240*, 2026.
- [43] O. T. AlJadaan, H. Zaidi, M. Y. Al Faress, and A. O. Jabas, "Ethics in AI and computation in automated decision-making," in *Enhancing automated decision-making through AI*, pp. 397–424, IGI Global Scientific Publishing, 2025.
- [44] J. F. Hair Jr, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, "Partial least squares structural equation modeling (PLS-SEM)," *European Business Review*, vol. 26, no. 2, p. 106, Emerald Group Publishing, Limited, 2014.
- [45] C. Fornell and D. F. Larcker, "Structural equation models with unobservable variables and measurement error: Algebra and statistics," *Sage publications Sage CA: Los Angeles, CA*, 1981.
- [46] P. Passaro, A. Di Vittorio, et al., "The Typicality of the Agri-Food Product Driver of the Enhancement of Destination Tourism the Apulian Case History," *European Scientific Journal*, vol. 18, no. 1, pp. 1–19, 2022.
- [47] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, and K. O. Thiele, "Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods," *Journal of the Academy of Marketing Science*, vol. 45, no. 5, pp. 616–632, Springer, 2017.
- [48] C. M. Ringle, M. Sarstedt, and D. W. Straub, "Editor's comments: a critical look at the use of PLS-SEM in MIS quarterly," *MIS Quarterly*, vol. 36, no. 1, pp. iii–xvi, 2012.
- [49] S. L. Hoffmann, "Human-Centered Cloud AI Collaboration Models for Sustainable and Secure Digital Enterprise Innovation," *International Journal of Engineering & Extended Technologies Research (IJEETR)*, vol. 7, no. 5, pp. 16062–16072, 2025.
- [50] N. A. M. Alhammadi and M. Mabrouk, "A multi-agent-based deep learning model for protecting cloud computing environment against distributed denial of service flooding attacks," *Journal of Soft Computing and Data Mining*, vol. 6, no. 1, pp. 406–422, 2025.

APPENDIX

TABLE VIII. FORMATIVE INDICATORS

Item	Weight	<i>t</i>	<i>p</i>	VIF	Tolerance
MA1	0.048	8.027	<0.001	3.197	0.313
MA2	0.029	4.334	0.002	1.454	0.688
MA3	0.056	10.310	0.003	2.463	0.406
MA4	0.055	9.780	0.004	2.875	0.348
MA5	0.102	34.045	0.005	2.587	0.387
MA6	0.100	33.936	0.001	3.110	0.322
MA7	0.102	34.796	<0.001	4.487	0.223
MA8	0.091	27.782	0.003	2.068	0.484
MA9	0.093	33.203	0.002	2.252	0.444
MA10	0.100	34.654	0.001	2.708	0.369
MS1	0.047	7.800	0.002	2.854	0.350
MS2	0.047	7.875	<0.001	3.542	0.282
MS3	0.062	11.836	0.002	4.570	0.219
MS4	0.041	7.413	<0.001	3.342	0.299
MS5	0.039	7.189	<0.001	2.125	0.471
MS6	0.062	12.123	<0.001	3.453	0.290
MS7	0.101	34.026	<0.001	2.575	0.388
MS8	0.098	33.238	0.001	3.104	0.322
MS9	0.098	34.111	<0.001	2.325	0.430
MS10	0.090	27.711	<0.001	1.487	0.672

MA = model acceptance;
MS = model satisfaction;
VIF = variance inflation factor.