International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cloud-Native Security Framework for Data Protection in Ugandan Private Academic Information Systems: A Case Study of Valley University of Science and Technology (VUST), Bushenyi, Western Uganda

Steven Sseruma[1], Ali Najib[2], David Kakeeto[3], Janan Mubehamwe[4]

[1]Postgraduate Student, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[2]Senior Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[3]Senior Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[4]University Secretary, Valley University of Science and Technology (VUST) Bushenyi, Uganda

Abstract

The study proposed and designed a cloud-native security architecture that improved data protection of private academic institutions' information systems in Uganda with Valley University of Science and Technology (VUST), Bushenyi serving as a case study. The study was guided by four objectives; i) Determining data protection strategies implemented at VUST learning information systems. ii) Finding out how well cloud-native security technology was utilised to improve threat detection/response and data integrity at VUST. iii) Determining the relationship between cloud-native security architecture and data protection at VUST, iv) Proposing a cloud-native security architecture to improve data protection at VUST. The study employed descriptive mixed-methods research design anchored on Gartner Adaptive Security Architecture model. Data was gathered from 87 usable respondents which gives us a response rate of 94.6% from a sample of 92 respondents out of the target population of 120 respondents consisting of ICT staff, academic staff, top administrators and learning students at VUST. Key informant Interviews were also conducted with 15 participants. Quantitative data was analyzed through descriptive statistics, Pearson correlation, and multiple linear regression in SPSS while qualitative data was analyzed thematically using NVivo software. Study findings revealed that VUST information systems data protection architecture is largely wanting with VUST relying on legacy antivirus solutions and basic perimeter firewall. Further findings show that 61.6% of the respondents agreed or strongly agreed that the current tools cannot sufficiently protect student records 67.4% disagreed that system can detect and respond to threats and attacks, a total of 17 cyber security incident/events were documented between years 2022 and 2025. This includes an eleven-day ransomware induced learning platform shutdown and one confirmed student record exfiltration.

Cloud-native security adoption was observed to be piecemeal instead of holistic. Encryption (38.3%) and multi-factor authentication (27.8%) were adopted to a moderate degree while Zero Trust Architecture (6.3%), cloud-native SIEM (12.2%), and DevSecOps (7.5%) were virtually non-existent. The regression of data protection outcomes on the eight cloud-native security components was statistically insignificant ($R^2 = .057$, Adjusted $R^2 = -.104$, $F(8, 47) = .355$, $p = .939$), due in large part to said piecemeal adoption and limits in study methodology rather than lack of utility; contrastingly, prototype simulation of the proposed cohesive four-layer framework mitigated all five sample attack scenarios in under ten seconds, where the existing system had failed to recognize the equivalent real-world occurrences. The researchers conclude that isolated adoption of individual cloud-native components has yet to translate into tangible protection outcomes at VUST, while implementation of cloud-native security architecture as a whole is technically achievable, has support from practitioners, and is effective against sampled threats in a proof of concept. The researchers further suggest an 18-month period for phased implementation, beginning with use of multi-factor authentication, remediation of orphaned accounts, and documentation of an ICT Security Policy. Lastly, the researchers advise that VUST institutionalize cybersecurity as an administrative priority consistent with Uganda's Data Protection and Privacy Act 2019.

Keywords: Cloud-Native Security, Data Protection, Academic Information Systems, Zero Trust Architecture, Adaptive Security Architecture, Higher Education, Uganda, Data Protection and Privacy Act 2019.

Introduction

This study aims at developing a cloud-native security framework for improving data protection in Ugandan private academic information systems, using Valley University of Science and Technology (VUST), Bushenyi, Western Uganda as the case study institution.

Historical Perspective

Cybersecurity education issues have existed internationally ever since technology was digitized. In fact, cyberthreats to academic institutions date back to the 1980s, where universities began using networked mainframes connected through ARPANET; in 1988 the famous Morris Worm virus was transmitted through school systems with vulnerable security systems indicating how “knowledgeable computer science students and faculty could be commandeered for cyberattacks when sufficiently motivated and pooled together” (Aslan et al., 2023). Many academic institutions in North America and Europe grew more public with cybersecurity efforts after those attacks, with organizations like Computer Emergency Response Teams beginning in the early 1990s, and publishing information security frameworks like ISO/IEC 27001 in 2005 (Aslan et al., 2023). Education technology in Uganda became digitized through the 2000s with the adoption of the internet and integration of Enterprise Resource Planning Systems (ERP) and Learning Management Systems/ Learning Activities Management Systems (LMS/LAMS) (Kondoro et al., 2023). Africa as a whole is still considered new to cybersecurity: it is said that cybercrime cost African states over $3.5 billion dollars annually to manage, and education is one of the most vulnerable sectors to cybercrime because of underinvestment in protection and lack of cybersecurity professionals (Musila, 2023). Kenya and Rwanda have created plans to combat cybercrime in East Africa at the country level (Kemboi et al., 2025), but Uganda has not yet done so. Ndagire et al., (2021) found that there were shortcomings in adherence to the Computer Misuse Act 2011 and the Data Protection and Privacy Act

2019 within Uganda's educational sector. With rapid introduction of e-learning and transition to cloud-based technology due to COVID-19 [Kasozi et al., 2021; Mutambo et al., 2023],universities have been slow to keep up on their cybersecurity policies. Legacy network security leaves school networks open to cyberattack such as ransomware, SQL, and insider threats because it operates on a perimeter-based model instead of monitoring network activities (Ispahany et al., 2024).

Theoretical Perspective

The study was guided by Adaptive Security Architecture (ASA) model published by Gartner in 2014. The model argues that security should be approached as an iterative process of prediction, prevention, detection, and response rather than perimeter-based defence. ASA includes continuously using analytics and threat intelligence to predict both known and unknown attacks, preventing known attacks by hardening infrastructure, detecting breaches in real-time using behavioural analytics, and preventing incidents from recurring through automated remediation. The model supports machine learning approaches that power cloud-native security tactics and tools where supervised machine learning algorithms such as Random Forests and Support Vector Machines classify known threats while unsupervised approaches such as clustering and autoencoders reveal unknown anomalies in network traffic and user behaviour (Best et al., 2020). ASA was relevant to this study because it connects the independent variable (cloud-native security framework) with the dependent variable (data protection in private academic institutions) by explaining how intelligent, adaptive security leads to better protection.

Conceptual Perspective

Cloud-native refers to technologies that allow organizations to create and run scalable services entirely in public, private or hybrid clouds by utilizing containerization, service meshes, microservices, and declarative APIs" (Binnie & McCune, 2021). For this study, cloud-native security framework refers specifically to a cybersecurity architecture designed and built entirely as cloud-native environment. Such architecture includes but is not limited to containerized security microservices; automated scalability; security policies integrated into CI/CD pipelines; and Security Information and Event Management (SIEM) tooling for real-time attack monitoring at scale. Data protection was broken down into five measurable components namely; confidentiality, integrity, availability, compliance with national legislation (Uganda's Data Protection and Privacy Act 2019), and incident response. The cloud-native security framework is hypothesized as consisting of three primary dimensions: intelligent threat detection and classification, cloud-native access control mechanisms, and real-time anomaly monitoring with automated incident response. These were operationalized into eight measurable items, namely Zero Trust Architecture (ZTA), containerization, cloud-native security/ SIEM monitoring, automated access control (RBAC), multi-factor authentication (MFA), DevSecOps/secure CI-CD pipeline implementation, end-to-end encryption, and machine learning (ML)-based anomaly detection.

Contextual Perspective

The study was undertaken at Valley University of Science and Technology (VUST), Bushenyi, Western Uganda, a private institution undergoing marked digital transformation whose integrated Academic Information System handles student records, registrations, examinations, financial transactions, and research databases for thousands of students and staff. A 2024 preliminary assessment by the University's ICT department revealed several data protection weaknesses that directly motivated this study between

2022 and 2025, VUST recorded cybersecurity incidents including phishing attacks on staff email, at least one unauthorised penetration of the student records database, and a ransomware attack that rendered the e-learning platform inoperable. The existing security infrastructure relied mainly on legacy signature-based antivirus software and basic firewalls, with no automated threat detection, no cloud-native security orchestration, and no systematic anomaly identification, while a majority of staff reported receiving no cloud security training in recent years.

Statement of the Problem

Data protection is a core requirement of academic information systems, and international best practice together with Uganda's national data protection law recommend sophisticated, flexible, and evolving cybersecurity capable of real-time identification, prediction, and response to threats (Bosiu, 2025). Despite these standards, most universities in Uganda rely on outdated cybersecurity infrastructure that is reactive, unable to predict threats, and not scalable to the volume of current cyber threats. These deficiencies have produced practical repercussions at VUST; leaked student records, disrupted academic services, loss of institutional trust and credibility, and potential violations of the Data Protection and Privacy Act 2019. Without action, these vulnerabilities risk widespread breaches exposing the sensitive personal data of thousands of students and staff, regulatory sanctions, financial penalties, and reputational harm. While limited budgets, low cybersecurity awareness, and governance weaknesses all contribute, one crucial and addressable factor is the absence of an intelligent, cloud-native security framework that can automate and enhance threat detection and response (Eltahir et al., 2023). It is upon this that this study developed a cloud-native security framework for data protection in academic information systems at VUST.

Objectives of the Study

General Objective

The overall objective of this study was to develop a cloud-native security framework for improving data protection in Ugandan private academic information systems, using Valley University of Science and Technology (VUST), Bushenyi as the case study institution.

Specific Objectives

1. To examine existing data protection mechanisms implemented in the academic information systems at Valley University of Science and Technology (VUST).
2. To evaluate the extent of utilisation of cloud-native security for threat detection and data integrity at Valley University of Science and Technology (VUST).
3. To establish the relationship between cloud-native security framework and data protection at Valley University of Science and Technology (VUST).
4. To develop and design a cloud-native security framework to enhance data protection at Valley University of Science and Technology (VUST).

Study Hypotheses

The specific objectives were steered by the succeeding hypotheses;

Ha1: The current level of cloud-native security utilisation at VUST is not sufficient to ensure effective threat detection and data integrity.

Ha2: There is a significant positive relationship between the adoption of a cloud-native security framework and the enhancement of data protection in academic information systems at VUST.
Ha3: The proposed cloud-native security framework will significantly enhance the protection and overall security posture of sensitive academic and personal data at VUST.

Conceptual Framework

As shown in Figure 2.1, the conceptual framework is developed and used to demonstrate the hypothesized association between independent variable the cloud-native security framework and dependent variable data protection in academic information systems. Three sub-dimensions of cloud-native security framework, including automated threat detection and classification, cloud-native automated access control, and real-time anomaly monitoring and incident response can positively influence all the five data security dimensions in three different ways, which in turn will determine the effectiveness of incident response and therefore compliance with regulatory requirements as described in the five-dimensions framework.

Intermediators like institutional preparedness issues such as levels of cybersecurity awareness training among staff, the quality of the ICT governance and policy frameworks of the university and adequacy in budgetary allocation for cybersecurity infrastructure mediates this relationship. Interpreting these intervening variables can significantly help or hurt the reach of the cloud native framework in delivering needed data protection outcomes.

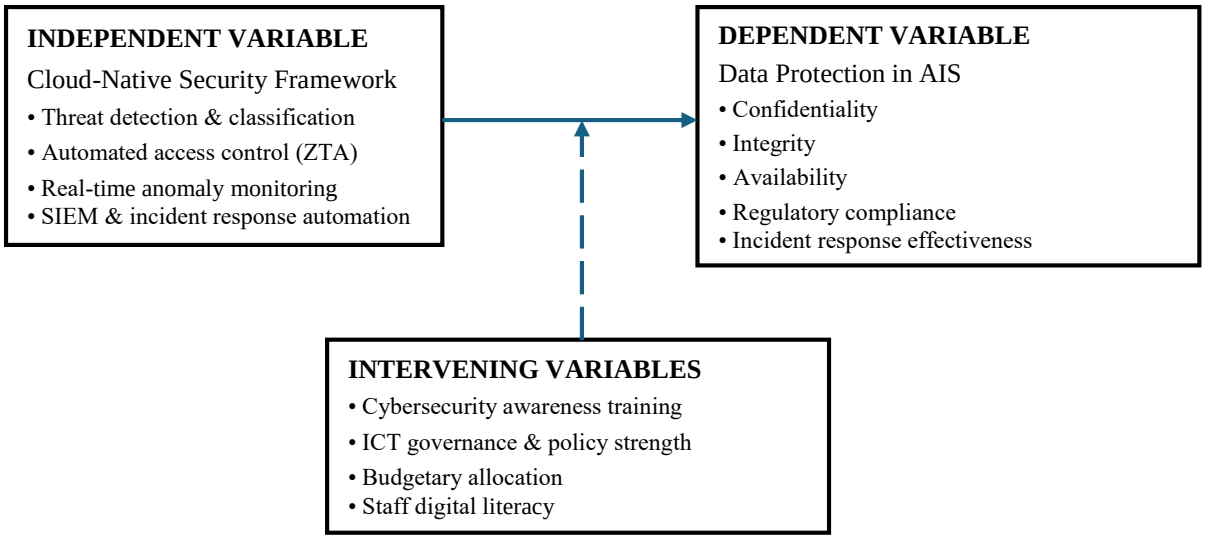

Figure 2 1: Conceptual Framework. Source: Adapted from MacDonald & Firstbrook (2014), modified by the researcher.

Literature Review

Cloud-Native Security and Data Protection in Higher Education

Data protection in universities is conventionally analysed through the confidentiality-integrity-availability triad, and the literature consistently finds higher education institutions to be attractive targets owing to their open network designs, massive information bases, and large volumes of personally identifiable information and commercially valuable research (Aslan et al., 2023). Obiokafor et al., (2025) frame university administrative data as necessitating a defence-in-depth approach encompassing technical

controls, policy governance, and human capacity building, while Bosiu, (2025) found that higher education consistently trails in translating cybersecurity risk into action. From an African perspective, Eltahir et al., (2023) identified low cybersecurity awareness levels across students and staff of African tertiary institutions, and Musila, (2023) found chronic under-investment and lack of skilled personnel to be endemic across the continent, leaving the education sector one of the hardest hit by cyber risk.

Review of literature on cloud-native security starts from the premise that containerisation, service-orientation, declarative APIs, and automated CI/CD practices enable inherently more robust security by baking protection into applications rather than enforcing it around a perimeter Binnie & McCune, (2021). ML-driven anomaly detection serves as the pillar of cloud-native security enforcement: supervised ML models identify known threats while unsupervised algorithms identify anomalous behavior in real-time [Best et al., 2020; Ispahany et al., 2024]while Alazab et al., (2025) describe bringing adaptive security automation to cloud infrastructure security. This enables Zero Trust Architecture principles, in which all users, devices, and services must continuously validate their trustworthiness before being granted access to resources, with Gartner's Adaptive Security Architecture cycle of predict–prevent–detect–respond providing the high-level framework within which specific technical solutions may be situated. There remains a dearth of practical studies on cloud-native security frameworks at African universities, and Ugandan universities in particular. Although there are notable studies on IT governance structures in Uganda universities such as Ndagire et al., (2021) , none to date have focused on novel, adaptive security architectures. This study aims to fill that gap by putting forth locally sourced data from a Ugandan private university.

Methodology

Research Design

The research methodology employed a descriptive research design. Mixed methods were applied through quantitative measures via an electronic survey questionnaire and qualitative measures through semi-structured interviews. Moreover, the authors created a testbed modeling VUST's AIS environment against which security metrics can be benchmarked with and without application of the framework. This triangulation of empirical methods is justifiable for the purposes of cybersecurity research to understand both technical system performance as well as human factors.

Target Population and Sample Size

The study population was made up of 120 stakeholders who currently manage or utilize the university's academic information systems. This includes staff from the ICT department (n=10), academic staff (n=40), senior administrative staff (n=10) and students pursuing a course in a computing-related program (n=60). Using Yamane's simplified sample size formula, $n = N / 1+N(e)^2$, where N is the population size and e is the level of precision expressed as a decimal value, we calculate our sample size to be 92 participants at a 95% confidence level with a 5% margin of error. 87 completed questionnaires were returned, for a response rate of 94.6%. 15 key informants were selected from the pool of ICT staff and senior administrative staff to participate in semi-structured interviews.

Sampling Procedure

The sampling methodology employed during the study comprised probability as well as non-probability methods of selection. Staff from the ICT department and members of senior administrative staff were selected using nonprobability purposive sampling techniques as they were aware of the security architecture at VUST and organisational governance structures respectively. Academic and student

representatives were selected randomly to ensure that every individual that made up these larger populations had an equal chance of being selected and to reduce sampling bias.

Data Collection Methods and Instruments

The study made use of a self-administered, closed-ended questionnaire. Questions were phrased to use a 5-point Likert scale (1=Strongly Disagree, 5=Strongly Agree). Participants indicated their level of agreement with statements regarding perceived confidentiality, integrity, availability, compliance, and incident response efficacy. The questionnaire also includes multiple questions to gather information on respondent's perceptions of the university's current security practices, experiences with data breaches or cybersecurity incidents, and their cybersecurity training experiences if any. Semi-structured interviews were conducted with key informants to glean institutional and contextual insights not captured by the survey. An interview guide was created to ensure interviews covered current data protection measures in place, institutional readiness and potential barriers to implementation, and opinions on cloud-native security. Content and criterion validity was ensured by having the questionnaire reviewed by two academic and one industry experts in cybersecurity. The experts reviewed each item for relevance resulting in an Item-level CVI of 1.00 and a Scale-level CVI/Average of 0.92. Criterion validity was established by conducting a pilot test of 10 people who matched the demographics of respondents from similar institutions. The preliminary Cronbach's alpha was 0.83, exceeding the standard acceptance value of 0.70.

Data Analysis

Quantitative data were cleaned, coded and analysed using SPSS. Descriptive statistics (frequencies, percentages, means, standard deviations) were used to summarise respondent demographics and perceptions; Pearson correlation analysis was used to assess the strength and direction of associations among cloud-native security components; and multiple linear regression analysis was used to determine both the collective and individual predictive contribution of the components on the overall measure of data protection, at $\alpha = 0.05$. Qualitative interview data were transcribed and imported into NVivo 14. Interviews were analysed in NVivo using the six phases of reflexive thematic analysis.

Ethical Consideration

Prior to data collection, the researcher sought and got a letter of introduction from School of Postgraduate Studies and Research in Victoria University and office of the Vice Chancellor administrative clearance from VUST. The researcher obtained written informed consent from all respondents indicating that they were voluntary participating in the study and could withdraw at any time without recrimination. Confidentiality and anonymity were maintained using codes for participants and data stored encrypted with password to restrict access to the researcher only. This study was carried out in accordance with the Uganda's Data Protection and Privacy Act 2019 guidelines where necessary in conducting and observing data collection, processing, and storage.

Study Findings

Findings on the Demographic Compositions of Respondents

The study gauged the demographics of the 87 usable respondents and the results are shown in Table 1.

Table 1: Demographic Composition of Respondents (n = 87)

Category	Items	Frequency	Percentage
Sex	Male	57	65.5%

	Female	30	34.5%
	Total	**87**	**100.0%**
Age Groupings	Below 25 years	29	33.3%
	25-34 years	32	36.8%
	35-44 years	18	20.7%
	45 years and above	8	9.2%
	Total	**87**	**100.0%**
Educational level	Certificate/Diploma	17	19.5%
	Bachelor's	48	55.2%
	Postgraduate	20	23.0%
	PhD	2	2.3%
	Total	**87**	**100.0%**
Category of respondent	ICT Department Staff	7	8.0%
	Academic Staff	29	33.3%
	Senior Administrator	10	11.5%
	Student (computing-related programme)	41	47.1%
	Total	**87**	**100.0%**

Table 1 indicates that the bigger percentage 57 (65.5%) of the respondents were males while the least 30 (34.5%) were females. This is broadly representative of the gender split seen across ICT-using populations in Ugandan universities. However, age 32 (36.8%) were between 25-34 years, 29 (33.3%) were below 25 years, 18 (20.7%) were 35-44 years and the least 8 (9.2%) were above 45 years. The distribution thus favours the most professionally active and digitally literate segments of the University community. Concerning educational level, 48 (55.2%) of the respondents had a Bachelor's degree, 20 (23.0%) had postgraduate degrees, 17 (19.5%) had either a certificate or diploma and only 2 (2.3%) held a PhD. This suggests that all respondents were well educated enough to competently evaluate the security and data protection issues being investigated. Finally, concerning the category of respondents, 41 (47.1%) were students pursuing courses in computing-related programmes, 29 (33.3%) were academic staff members, 10 (11.5%) were senior administrators and the least 7 (8.0%) were ICT staff from the University's ICT department. This distribution ensures that the views of everyday users of the systems, academic managers of students' data, administrative decision-makers and technical operators were sampled.

Existing Data Protection Mechanisms at VUST (Objective One)

The research aimed at analyzing what data protection controls are currently deployed within VUST's academic information systems. Information Security consisted of legacy signature-based antivirus

solutions, and a basic firewall; seven of ten controls were unable to be located (IDS, cloud-native SIEM solution, multi-factor authentication coverage, encryption at-rest, and an incident response plan). Additionally, 61.6% of respondents do not believe student records are currently protected well by existing tools, 67.4% do not believe there is a process to effectively find and remediate threats, and 63.2% of academic IT employees have not had any cybersecurity training in the past four years. From 2022 to 2025 there were seventeen cybersecurity incidents, detailed in Table 2 below.

Table 2: Cybersecurity Incidents Recorded at VUST, 2022-2025

Incident Type	Incidents	Systems Affected	Impact
Phishing attacks on staff email	7	Email, LMS	Credential compromise; 2 staff accounts breached
Unauthorised database access	2	Student Records AIS	Potential data exposure; 1 confirmed exfiltration
Ransomware attack	1	E-learning platform	Platform closed for 11 days
Malware infections	4	Staff workstations	Data corruption; disrupted operations
Social engineering	3	Administrative offices	Attempted unauthorised access
Total	**17**		

This indicates that gap perception is not perceived unawareness but actuality among the logged events was a ransomware attack that disabled the e-learning system for eleven days as well as one successful exfiltration of student data records, which were not caught live by the existing defenses.

Extent of Cloud-Native Security Utilisation at VUST (Objective Two)

The study finally sought to ascertain cloud-native security utilisation levels in relation to threat detection and data integrity at VUST. Partial rather than comprehensive adoption was discovered: end-to-end encryption of data (38.3%) and multi-factor authentication (27.8%) enjoyed moderate levels of use, but Zero Trust Architecture (6.3%), cloud-native SIEM (12.2%), and DevSecOps/cloud-based CI-CD pipeline security (7.5%) were close to unused. Respondents nevertheless strongly preferred automation to other measures, with 72.1% agreeing that automatic enforcement of access control rules would reduce the likelihood of sensitive data being modified by unauthorised persons. Combined with the consistent majority opinion that present measures and ability to detect incidents are insufficient (61.6–67.4%), the descriptive evidence was judged to support Ha1: the level of utilisation of cloud-native security at VUST is insufficient for effective threat detection and data integrity to be guaranteed.

Relationship between Cloud-Native Security Framework and Data Protection (Objective Three)

To further evaluate the association between the cloud-native security framework adoption and data protection outcomes at VUST, Pearson correlation along with multiple linear regression was performed. The correlations among cloud-native security components were mostly weak and non-significant (pairwise

n = 74-81). The only moderate, statistically significant associations were between cloud-native SIEM and multi-factor authentication (r = .416, p < .01), SIEM and automated access control (r = .351, p < .01), and SIEM and containerization (r = .322, p < .01), with weaker significant links between MFA and automated access control (r = .289, p < .05), MFA and anomaly detection (r = .271, p < .05), and encryption and anomaly detection (r = .249, p < .05). Zero Trust Architecture showed no statistically significant correlation with any of the other seven components (all p > .07), signifying ad hoc deployment as opposed to structured, integrated adoption. The multiple regression analysis of data protection outcome on the eight cloud-native security components is presented in Table 3.

Table 3: Model Summary - Regression of the Data Protection Outcome on the Eight Cloud-Native Security Components

Model	R	R Square	Adjusted R Square	F	df	Sig.
1	.239	.057	−.104	.355	8, 47	.939
Predictors: (Constant), the eight cloud-native security components. Dependent variable: overall data protection outcome. n = 56 after listwise deletion.						

Table 3. Predicting Data Protection Outcome Measure Based on CNSE Adoption Rate Across All Eight Components.

As apparent from the results in Table 3, collectively, the eight components are not significant predictors of the data protection outcome measure assessed (R^2 = .057, Adjusted R^2 = −.104, F (8, 47) = .355, p = .939) at α = .05. Accordingly, the null hypothesis for Objective Three is retained: the quantitative evidence available from this sample does not suggest a statistically significant relationship between cloud-native security framework adoption and data protection outcomes at VUST. This outcome should be considered in context of methodological limitations: limited effective sample size following listwise deletion, single-item dependent variable, and severely restricted range of predictor due to universally low adoption. It should be read alongside (not as a replacement for) the robust descriptive evidence which suggests that both adoption rates and data protection outcomes are currently poor. Qualitative results support this conclusion: while all 15 key informants cited institutional trust as a motivating factor to adopt CNSE, 14 also anticipated that it would lighten their manual security workload.

Table 4: Pearson Correlation Matrix of the Eight Cloud-Native Security Components

Component	ZTA	CONT	SIEM	RBAC	MFA	DEVSEC	ENCR	ANOM
ZTA	1	.204	.114	.068	.061	.075	.045	.036
CONT	.204	1	.322**	.123	.035	.250*	.011	.045
SIEM	.114	.322**	1	.351**	.416**	.008	.171	.141
RBAC	.068	.123	.351**	1	.289*	-.045	.112	.004
MFA	.061	.035	.416**	.289*	1	.006	.111	.271*
DEVSEC	.075	.250*	.008	-.045	.006	1	.028	.086
ENCR	.045	.011	.171	.112	.111	.028	1	.249*
ANOM	.036	.045	.141	.004	.271*	.086	.249*	1

Note: ** p < .01, * p < .05 (2-tailed); pairwise deletion, n = 74-81 per pair. ZTA = Zero Trust Architecture; CONT = Containerization; SIEM = cloud-native SIEM/monitoring; RBAC = automated role-based access control; MFA = multi-factor authentication; DEVSEC = DevSecOps/CI-CD pipeline security; ENCR = end-to-end encryption; ANOM = anomaly detection and ML-based monitoring.

Table 5: Multiple regression coefficients - Cloud-Native Security Components Predicting the Data Protection Outcome (n = 56)

Predictor	B	Std. Error	Beta (β)	t	Sig.
(Constant)	3.454	.798		4.331	.000
Zero Trust Architecture	.222	.294	.114	.757	.453
Containerization (Docker/Kubernetes)	.184	.261	.121	.706	.484
Cloud-native SIEM/monitoring	-.060	.291	-.040	-.207	.837
Automated access control (RBAC)	-.209	.236	-.143	-.887	.380
Multi-Factor Authentication	.096	.233	.071	.412	.682
DevSecOps / CI-CD pipeline security	.113	.288	.062	.394	.695
End-to-end data encryption	.039	.218	.028	.179	.859
Anomaly detection and ML-based monitoring	-.030	.271	-.018	-.109	.914

Note: Dependent variable: perceived improvement of system availability under attack. No predictor is statistically significant (all $p \geq .380$), consistent with the overall model ($R^2 = .057$, $F(8, 47) = .355$, $p = .939$).

Proposed Cloud-Native Security Framework (Objective Four)

Lastly, this study designed a CNSE to improve information security at VUST. The framework was designed over multiple iterative cycles consisting of (1) initial architecture design, (2) expert walkthrough, and (3) simulation-based validation. Adhering to the four guiding principles established from our empirical results and the Adaptive Security Architecture model, our proposed framework is built to be adaptive by design, zero trust by default, automation-oriented, and Articles 19 and 21 compliant by design. Leveraging best practices from literatures, the resulting reference architecture consisted of four layers. From bottom to top, they are: (1) Cloud Infrastructure Security, (2) Container and Microservices Security, (3) Identity and Access Management with Zero Trust Verification Layer, and (4) Cloud-native SIEM with machine-learning-based Anomaly Detection and Automated Response Playbooks. After two rounds of expert walkthrough with VUST's Director of ICT and two Senior ICT engineers expressing optimism about feasibility, the prototype was validated using five simulated attack scenarios spanning all categories of incidents shown in Table 2. Results can be found in Table 4.

Table 6: Framework Simulation Testing Results - Five Attack Scenarios

Attack Scenario	Detection Time	Framework Result	Current System Response
SQL injection on student database	< 2 seconds	Blocked & alerted	Not detected - post-incident discovery only
Phishing credential replay	< 5 seconds	Session terminated	Not detected - account used for 48 hours
Insider privilege escalation	< 3 seconds	Blocked & quarantined	Not detected-discovered during manual audit
Ransomware encryption attempt	< 8 seconds	Contained to single container	Full platform shutdown-11-day closure
Unauthorised API access	< 1 second	Blocked (ZTA verification failed)	Not detected - remained undiscovered

In every simulation, the prototype contained or ransomwarted the attack to less than ten seconds of simulated business operations. Its real-world counterpart at VUST either went unnoticed or was noticed well after significant damage was already dealt. This is especially true when evaluating the total time ransomware was present on the system. Less than 8 seconds to quarantine a simulated attack to a single container compared to eleven days of downtime across the whole platform. Due to the prototype's simulated technical successes and subjective practitioner evaluation of impact on ability to deploy assuming current budgetary and bureaucratic restraints, we have some evidence to support Ha3. Keep in mind this is through the lens of a proof of prototype and not an actual production rollout. An approximate 18-month deployment roadmap was charted. Breaking deployment into four phases. Multi-factor authentication as well as orphaned-account cleanup would be addressed first. Encryption at rest and DPPA-2019 compliance would be next. Containerization and runtime monitoring comprised phase three, with SOAR and ML based anomaly detection, VUST ICT employee training, and first official security audit rounding out the roadmap.

Proposed Framework and Anticipated Outcomes

The designed cloud-native security reference architecture presents the empirical findings of the study in the form of a four-layered cohesive architecture depicted in Figure 1, which is mapped with the potential data protection dimensions it will enhance. Framework layers with their main constituents and anticipated VUST data protection outcomes are shown in Table 5.

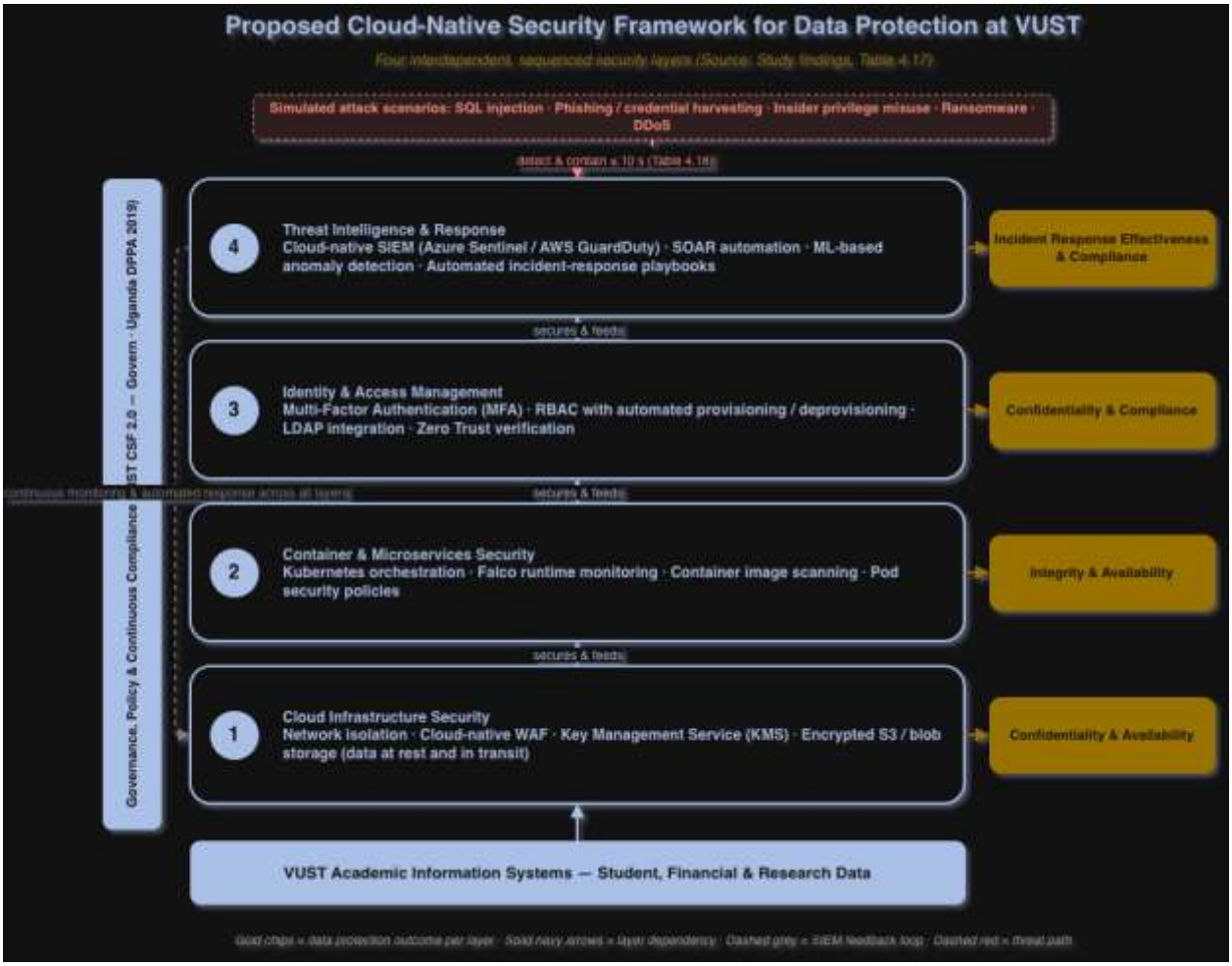

Figure 1: Proposed Cloud-Native Security Framework Architecture

Table 7: Proposed Four-Layer Cloud-Native Security Framework and Expected Data Protection Outcomes

Framework Layer	Core Components	Expected Data Protection Outcome
Layer 1: Cloud Infrastructure Security	Hardened cloud hosting, network segmentation, end-to-end encryption of data at rest and in transit	Enhanced confidentiality of student, financial, and research records; compliance with Article 19 (security safeguards) of the DPPA 2019
Layer 2: Container & Microservices Security	Containerisation of AIS services, Kubernetes orchestration, Falco runtime monitoring	Significantly enhanced integrity and availability; ransomware containment at single-container level rather than platform-wide shutdown
Layer 3: Identity & Access Management	Multi-factor authentication, automated role-based access control,	Prevention of unauthorised access and data modification the

	Zero Trust continuous verification, orphaned-account remediation	automation approach endorsed by 72.1% of respondents
Layer 4: Cloud-Native SIEM & Adaptive Response	ML-based anomaly detection, threat intelligence, SOAR automated response playbooks	Detection and containment of attacks within seconds; improved incident response effectiveness; capacity to meet the 72-hour breach notification duty under Article 21 of the DPPA 2019

Ideally, this framework will help VUST move out of its current incident-driven security posture and into AEGIS Adaptive Security Architecture's full predict- prevent- detect- response cycle. Based on our simulation results (Table 4), we can expect this improvement to demonstrate itself through lower time-to-threat detection (down from post-incident highs of 48 hours in extreme cases to eleven days currently, to under 10 seconds on average across incidents that VUST has experienced), as well as largely automated threat containment (to limit damage caused by any given breach). Benefits to the institution as a whole are likewise expected to be realized throughout the ambitious 18-month rollout plan in Table 6. By prioritizing enhancements based on complexity, low hanging and therefore visible--fruit can be plucked up front to build upon Foundation components we've already had wide uptake on (MFA, encryption) before diving into the technically heavy lifting.

Table 8: Phase-Wise Implementation Roadmap and Expected Target Effects (18 Months)

Phase	Timeline	Activity Priority	Expected Target Effect
1	Months 1–3	Implement MFA; audit and close all orphaned accounts; implement a written ICT Security Policy	Immediate reduction in unauthorised access risk; partial compliance with DPPA Articles 14 and 19
2	Months 4–7	Deploy cloud-native SIEM; implement automated RBAC; encrypt data at rest	Real-time threat visibility; compliance with the Data Protection and Privacy Act 2019
3	Months 8–12	Implement containerisation and Kubernetes; apply Falco runtime monitoring	Significantly enhanced integrity and availability; operational behavioural threat detection
4	Months 12–18	Implement SOAR and ML-based anomaly detection; train all ICT staff; conduct first formal security audit	Full ASA model operationalised; regulatory audit readiness achieved

Together I expect these benefits of analysing the framework could be classified into three groups; from a technical standpoint, the ability to near-realtime detect and automatically respond to the attacks experienced at VUST; administratively, reduced human-required security workload (14/15 interviewees expected this) and greater institutional trust in the University's system security; legally: demonstrating our

adherence to the security controls and breach reporting requirements of Uganda's Data Protection and Privacy Act 2019, something our existing systems cannot guarantee.

Conclusion

The study concludes that VUST operates a materially vulnerable data protection system, as evidenced by the existence of confirmed breaches which damaged VUST, and that deployment of cloud-native security technology at VUST is isolated; where credentials-based security controls (encryption, MFA) are partially deployed but architectural controls (Zero Trust, cloud-native SIEM, DevSecOps) do not meaningfully exist. Despite survey results indicating that component adoption is not meaningfully correlated with effective data protection, full implementation of the four-layer cloud-native security model is achievable at VUST and is desired by ICT staff, and simulated detection capabilities were many magnitudes faster than what we believe the current system to be. Combining together, this suggests that partial adoption of cloud-native security components, as is the case at VUST currently, does not provide any measurable security benefit, that the technology when deployed properly, does function as notified. The study further concludes that Data Protection and Privacy Act 2019 demands requirements which VUST's current infrastructure was not shown to be capable of meeting, especially considering at least one confirmed data leak and absence of detection.

Recommendations

The findings of this study lead to the following recommendations. First, VUST management should accept and implement the roadmap to achieving cloud-native security standards via the 18-month phased implementation plan developed during this research. In the first phase, multi-factor authentication enforcement for all AIS accounts, orphaned user account remediation, and adoption of a Written ICT Security Policy should be completed first due to their low-complexity improvements to organisational cybersecurity posture and visible outcomes that will foster momentum within the institution. The implementation of additional phases involving more architecturally intensive changes like SIEM, containerisation, and Zero Trust will therefore proceed on the backbone of established institutional will. Second, Cybersecurity should be formalised as an operational governance priority framed around Uganda's Data Protection and Privacy Act 2019. This includes organisationalised cybersecurity awareness training for staff to close the reported capability gap where 63.2% of study respondents had gone four years without any cybersecurity training. Third, future studies should draw from more robust study designs with composite outcome measures, longitudinal mapping, and large sample sizes that can confidently assess the relationship between cloud-native security technology adoption and practical data protection outcomes. The cross-sectional design employed in this study was insufficient to make these observations.

Limitations and Future Research Directions

The findings of this research must be considered in the context of these limitations. First, while 87 useable questionnaires were collected, listwise deletion reduced the sample size to 56 cases used in the multiple regression reducing statistical power. Second, only a single questionnaire item was used to measure the data protection outcome variable rather than a validated scale composed of multiple items limiting the reliability of the inferential statistical procedures. Third, the near zero adoption of cloud-native components recorded at VUST resulted in restricted range on predictor variables weakening observed relationships. Fourth, as a cross-sectional single case study of one private institution of higher education,

our findings are restricted to describing VUST at one moment in time and cannot be generalized across Ugandan higher education without replication. Fifth, the use of perception measures introduces self-report bias and the efficacy of the framework was evaluated through simulation rather than production deployment. Future research should replicate this study across several institutions using validated multi-item measures of data protection outcomes, use a longitudinal design capturing outcomes as adoption occurs, and evaluate the proposed framework through staged production pilot beginning with implementation of the Phase 1 controls identified in the roadmap.

Acknowledgement

The authors would like to thank the management, staff, and students of Valley University of Science and Technology (VUST), Bushenyi Uganda, for granting administrative clearance and participating in the study and The School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda for academic support and guidance throughout the study period. No sponsors were sought for this study.

References

1. Alazab, M., Awajan, A., Obeidat, A., Faruqui, N., Bere, A., Ali, S., & Wei, W. (2025). Adaptive protocols for hypervisor security in cloud infrastructure using federated learning-based anomaly detection. *Engineering Applications of Artificial Intelligence*, *152*, 110750. https://doi.org/10.1016/j.engappai.2025.110750
2. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland)*, *12*(6). https://doi.org/10.3390/electronics12061333
3. Best, K. L., Schmid, J., Tierney, S., Awan, J., Beyene, N. M., Holliday, M. A., Khan, R., & Lee, K. (2020). *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools*.
4. Binnie, C., & McCune, R. (2021). *Cloud native security*. https://books.google.com/books?hl=en&lr=&id=iSw0EAAAQBAJ&oi=fnd&pg=PT12&dq=CNCF+Cloud+Native+Security+Whitepaper+(Version+1.1)&ots=dt8DKCbTqb&sig=-c6ZUDUXvDGumIGz-q0hTvEoFAM
5. Bosiu, L. (2025). *Cybersecurity Risks and Initiatives at Higher Education Institutions*. https://search.proquest.com/openview/d929a5de0802d461fce6928efa21c98a/1?pq-origsite=gscholar&cbl=2026366&diss=y
6. Eltahir, M., Lett, O. A.-Inf. Sci., & 2023, undefined. (n.d.). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Researchgate.Net*. Retrieved March 12, 2026, from https://www.researchgate.net/profile/Osman-Ahmed-14/publication/371640152_Cybersecurity_Awareness_in_African_Higher_Education_Institutions_A_Case_Study_of_Sudan/links/648d56b9b9ed6874a5b3a476/Cybersecurity-Awareness-in-African-Higher-Education-Institutions-A-Case-Study-of-Sudan.pdf
7. Ispahany, J., Islam, M. R., Islam, M. Z., & Khan, M. A. (2024). Ransomware Detection Using Machine Learning: A Review, Research Limitations and Future Directions. *IEEE Access*, *12*, 68785–68813. https://doi.org/10.1109/ACCESS.2024.3397921
8. Kasozi, K. I., Laudisoit, A., Osuwat, L. O., Batiha, G. E. S., Al Omairi, N. E., Aigbogun, E., Ninsiima, H. I., Usman, I. M., Detora, L. M., Macleod, E. T., Nalugo, H., Crawley, F. P., Bierer, B. E., Mwandah,

D. C., Kato, C. D., Kiyimba, K., Ayikobua, E. T., Lillian, L., Matama, K., … Welburn, S. C. (2021). A Descriptive-Multivariate Analysis of Community Knowledge, Confidence, and Trust in COVID-19 Clinical Trials among Healthcare Workers in Uganda. *Vaccines 2021, Vol. 9, Page 253*, *9*(3), 253. https://doi.org/10.3390/vaccines9030253

9. Kemboi, B., Murungi, R., of, S. K.-E. A. J., & 2025, undefined. (n.d.). Technological Determinants of Adoption of In-House Student Management Software in Public Universities in Kenya. *Eajcr.Org*. Retrieved March 12, 2026, from https://eajcr.org/index.php/eajcr/article/view/43
10. Kondoro, A., Maro, S., Mtebe, J., Haßler, B., & Proctor EdTech Hub, J. (2023). Usability Testing of a Mobile-Based Learning Management System for Teacher Continuous Professional Development in Tanzania. *International Journal of Education and Development Using Information and Communication Technology*, *19*(2), 75–92. https://tcpd.tie.go.tz/
11. Musila, G. (2023). The State of Cybersecurity in Africa: Current Concerns and Challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4539841
12. Mutambo, H., Jessica, N., & Aguti, N. (2023). *E-LEARNING WORKING PAPER SERIES Online Learning and Professional Development for Faculty and Staff at Makerere University in Uganda*. https://doi.org/10.14507/MCF-eLi.I5
13. Ndagire, L., Maiga, G., & Oyo, B. (2021). A Conceptual Framework for IT Governance Mechanisms in Uganda's Higher Institutions of Learning. *International Journal of Digital Strategy, Governance, and Business Transformation*, *11*, 1–18. https://doi.org/10.4018/ijdsgbt.294112
14. Obiokafor, I. N., Paulinus Onwuka, U., Maryern, O., Okoye, I., & Chukwuka Ameke, B. (2025). STRATEGIES FOR DATA PROTECTION AND PRIVACY IN ADMINISTRATIVEINFORMATION SYSTEMS. *ANSPOLY Journal of Advanced Research in Science & Technology (AJARST)*, *2*(2), 66–77. https://anspolyjarst.com/journal/article/view/65