From Federation To Verifiable Credentials: A Pragmatic Path To Blockchain Enabled IAM

Ramanan Hariharan

Engineering Manager, IAM and cloud security at Deloitte, USA
Email: email@ramananhariharan.com

Abstract

This study discusses the issues surrounding enterprise identity and access management (IAM) systems based on federated Single Sign-On (SSO) protocols such as SAML and OpenID Connection (OIDC). Although these systems minimize credential sprawl, they have been linked with massive password-reset flows, phishing risks, and vendor lock-in. A 12-week pilot is to be undertaken in order to integrate W3C Verifiable Credentials (VCs) with the current existing IAM infrastructures, supporting 10,000-25,000 workforce users on 5-8 applications. Improvements, including the reduction of password-reset tickets by ≥35, reduction of phishing-backed account takeovers by ≥40, median verification latency of ≤500 ms, and a credential issuance failure rate of ≤1.0%, are the tangible goals of the study. A sound statistical analysis framework is adopted, and two proportion z-tests are used to test incident rates and Mann-Whitney U to test latency, a cost/ROI model to predict breakeven within 6-12 months under moderate adoption (40-60%). The study presents a reference architecture, migration blueprint, and detailed key performance indicator (KPI) definitions. It investigates the bare minimum blockchain existence that can be used to verify the authenticity and status of the issuer at minimal operational risk. The findings can be applied practically to organizations that might be thinking about the adoption of federated IAM to blockchain-enabled privacy-sensitive IAM systems based on VCs, which would be more secure, offer a smoother user experience, and be less costly in terms of operations.

Keywords; *Verifiable Credentials, Blockchain IAM, OIDC4VP, Decentralized Identity, Authentication.*

1. Introduction

The field of enterprise identity and access management (IAM) is mostly supported by federation based on SAML and OpenID Connect (OIDC), but quantifiable risks and expenses remain. Password-reset requests in large businesses are 15 to 30 per 1000 users per month, with a cost of 15 to 30 dollars per ticket and taking 18 to 25 minutes of staff time. Phishing is one of the most frequent first access vectors. Federated single sign-on largely wins the battle of credential sprawl, but the introduction of blast-Radius and vendor lock-in. The level of regulatory scrutiny in regards to GDPR and eIDAS risk is on the rise, and the mechanisms to onboard cross-border partners need to be portable and identifiable. These pressures drive the evaluation of privacy-preserving, phishing-resistant, transportable credentials that can reduce the volume of help-desk calls, increase their assurance, and stay within latency limits that can be affordable with big enterprises.

Unverifiable credentials (also known as vendor-sovereign or password-free credentials). An issuer–holder–verifier model is favored by verifiable credentials (VCs), which offer users a more purpose- and audience-bound cryptographic proof in place of bearer assertions based on traditional IdP. Claims are just submitted, verifiers only see selective-disclosure formats like SD-JWT or BBS+, and short status lists to revoke them; they do not even contact the issuer, resulting in minimal observability and correlation. OpenID to Verifiable Credential Issuance (OIDC4CI) and Presentation (OIDC4VP with SIOPv2) implement OAuth/OIDC flows, making it possible to adopt them. Credential binding FIDO2 or passkey Resources are bound to device-resident keys, enhancing resistance to phishing and session replay. Caching can give a median latency of 500 ms and a P95 of less than 900 ms. The mechanisms ensure a lack of privacy, enhance assurance and user experience, and disaggregate trust on the side of a single provider.

The study examines the added value of verifiable credentials over an established federated SSO infrastructure. To begin with, it measures security and experience improvements by monitoring phishing-related cases, enabling MFA, and help-desk ticket requests. The lowest level of detectable effect is 20-30% with 80% power, $\alpha=0.05$, in two-proportion tests of incident rates and Mann-Whitney U of latency. It also considers the smallest blockchain presence required to verify status and issuer authenticity, preferring trust registries, DID resolution, and batched status updates to heavy on-chain storage. Third, it determines a migration path with minimal operational risk and cost, rollback in case P95 latency is above 1.5× baseline or error rates are two times higher during a 30-minute canary rollout or stepped-wedge rollout.

The heights include workforce IAM of large (10,000 or more active users) enterprises that have between five and eight web or SaaS applications in use on mobile and desktop. A provider of identity, which already provides SAML/OIDC SSO, central policy, and logging, adds verifiable credentials, also called portable claims, based on workforce identity, compliance training, and partner assurance. Personal data does not exist on-chain, and only public keys, schema identifiers, status entries, and issuer attestations are written in trust registries. The method approaches of DID are prioritized to be based on interoperability and portability through the integration of did:web to bootstrap with a decentralized approach. The paper presupposes that the device is bound to FIDO2 or passkey, the time-to-live of the verifier-side caching is less than 60 seconds, and the availability of issuer and verifier components is 99.9%.

This study is organized into different chapters. The literature review tracks how the ideas of LDAP and federation evolved into the principles of decentralized identity, gives an overview of W3C VC/DID, SD-JWT selective disclosure, OIDC4CI/OIDC4VP, and ISO 18013-5/-7, and learns the lessons of successful EUDI pilots in the EU and Microsoft Entra Verified ID in Flanders. In the methods chapter, instrumentation, A/B or stepped-wedge design, and tests such as two-proportion of incident rates, Mann-Whitney U of latency have been defined. Experiments and results indicate baseline SSO values, issuance and verification values, security values, user experience, and cost values. The discussion interprets effectiveness measurements, trade-offs in privacy and correlation, reliability, scaling, and unit economic calculations, and suggests an efficient migration blueprint. Future activities embrace wallet reclaim, privacy-preserving cryptography metrics, interoperability tests, and identity of machines and represent the short-term Problems of the cases, followed by brief conclusions.

2. Literature Review

2.1 Evolution of enterprise IAM

Enterprise identity and access management (IAM) has evolved in four distinguishable stages: directory-based access with the help of NTLM/Kerberos and LDAP; federated web single sign-on (SSO) with the help of SAML and subsequent OpenID Connect (OIDC); phishing-resistant authenticators with the help of FIDO2 and passkeys; and credential portability with the help of verifiable credentials (VCs). The directory age centralized policy resulted in application silos and mass credential reuse [1 ; 2]. Federation integrated several logins and made session portability in SaaS, which usually minimizes the need to re-enter passwords, and it keeps the median sign-in latency at a few hundred milliseconds under normal network conditions. Since attackers migrated to phishing, MFA fatigue, and session replay, organizations have implemented FIDO2/passkeys, which helped to do away with shared secrets and tie authentication to keys that are available in the device, making them more resistant to credential theft.

Figure 1 below illustrates the development of enterprise Identity and Access Management (IAM) systems. It features the development of directory-based access (through NTLM/ Kerberos and LDAP into federated Single Sign-On (SSO) with such protocols as SAML and OpenID Connect (OIDC). It also reflects how phishing-resistant authenticators, such as FIDO2 and passkeys, are moving away from the concept of secrets shared and enhancing device-bound authentication. It highlights the notion of credential portability with the help of Verifiable Credentials (VCs), which improve security and introduce extra usability since they make credentials more adjustable and privacy-compliant across applications.

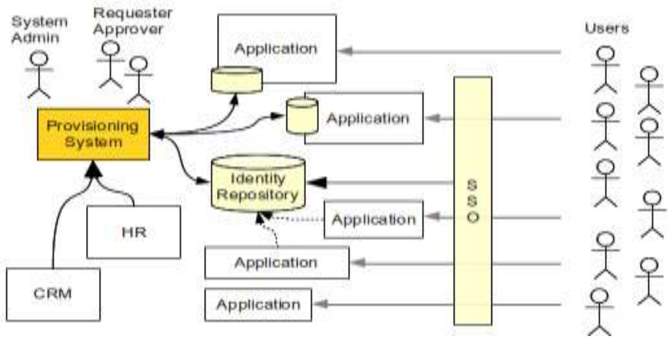

Figure 1: Evolution of enterprise IAM from directory-based to credential portability.

Even today, in the presence of SSO and robust authenticators, enterprises still have to deal with quantifiable expenses like 15-30 password-reset tickets per 1,000 users per month, as well as onboarding friction by external partners who are not account holders in the enterprise IdP. The newer efforts are expanding IAM past authentication into personalized authorization attributes and attestations [3]. Credential portability solves a number of pain points, including employee or partner validation being done twice, different assurance statements in other business units, and parts of audit trails that do not leave a single jurisdiction. Practically, portability is accompanied by federation: the claims selected by VCs are signed and disclosed selectively and verified locally, without reference to issuer call-outs, and including no unnecessary attributes. A pragmatic migration would have such operational objectives as P50 ≤ 500 ms and P95 ≤ 900 ms with caching, issuance success ≥ 99.0%, and propagation of revocation less than one minute to contain risk without affecting the user experience.

2.2 Standards and protocols for VCs

W3C Verifiable Credentials Data Model defines the way of associating statements with cryptographic keys by the issuers and the way of presenting those statements by the holders to the verifiers using Decentralized Identifiers (DIDs). The two encoding families find application: JSON-LD VCs (parts of which have semantics that are graph-based), to promote interoperability, and JSON Web Token (JWT) VCs to promote compact transport support and simple tooling [4]. It is based on selective disclosure. SD-JWT can release the attributes on a case-by-case basis in the field without exposing a full credential, and BBS+ signatures can produce unlinked zero-knowledge formulas such that, e.g., a predicate (for example, “over 18”) can be satisfied by a specialised holder without ever exposing raw values.

The OpenID for Verifiable Credential Issuance (OIDC4CI) and OpenID for Verifiable Presentations (OIDC4VP) reuse issues of the Self-Issued OpenID Provider v2 (SIOPv2) to issue and present OAuth and OIDC flows. FIDO 2 or passkey device binding is used to make sure that the presenter has control over the matching private key of the credential holder binding that is being bound with that of the credential, minimizing replication and man-in-the-middle threat. Status and revocation of the scale are needed in operationalization. Status list mechanisms encode revocation bitmaps to allow verifiers to store state with a time-to-live of less than 60 seconds, and have low network overhead. Day-two requirements include conformance testing, schema versioning, and telemetry (such as success and error codes per verifier and P50/P95 latencies). This trend is similar to the wider advancement of machine-interpretable artifacts and automated decision making, where structured content is inferred consistently within latency constraints to produce the same result [5].

2.3 Blockchain’s role

Blockchains find their best application in increasing interoperability and decreasing the sole vendor reliance on the tamper-evident public state. Two roles recur as the public key anchoring and policy metadata verifier design enable issuer DID resolutions along with provenance checking without the assistance of a single identity provider, and it promotes the cross-ecosystem trust and facilitates audit. Credential information can also be stored on-chain or posted-off chain using Merkle proofs so that it can be verified offline or across jurisdictions.

DID approaches offer trade: did:web bootstraps and works well with DNS when enterprise change control is needed, at scale; did:ion supports high-scale operation pegged to the Bitcoin blockchain; did:key is self-certificating and can work lightweight; did:kilt and did:indy allow ecosystem-specific assurances. Cost control can be achieved by effectiveness with permissioned chains, remote accessing public-chain Layer-2 networks, and per-write expenses are designed to be less than a cent through batching. Privacy by itself is ensured by ensuring that the personal identifiable information is not stored on-chain and that the keys, schema, and compact status artifact are only posted [6].

2.4 Real deployments

There are a number of production or pilot programs that cast a certain light on feasibility and limitations. The large-scale pilot of the European Digital Identity (EUDI) Wallet explains selective disclosures of government-issued attributes among different member states that involve offline document validation and online access to services based on a shared trust list and set levels of assurances. The programs advertise verification latencies that are compatible with interactive web sessions and give focus on artifacts of governance, which include liability distribution, accreditation, and dispute-resolution mechanisms that enterprises may customize when establishing trust frameworks.

Businesses have been able to exhibit industry-specific value. Microsoft Entra Verified ID is implemented in the Government of Flanders, where education and professional credentials are issued and verified, and integrated with existing SSO and audit tools at the cost of minutes of revocation and status [7]. Such reusable know-your-customer credentials that are demonstrated in partnership with the KILT network enable Deloitte to present indicative proofs from one service to another service without incurring the usual registration. The Verifiable organizations ecosystem, as exemplified by the Province of British Columbia (OrgBook BC), portrays organizational credentials types of the credentials applied to differentiate business interactions and compliance checks. Across these examples, some of the typical operational points have been first-time issuance in less than ninety seconds, repeat verification in less than one second when cached, and cross-wallet interoperability that is determined by structured conformance tests.

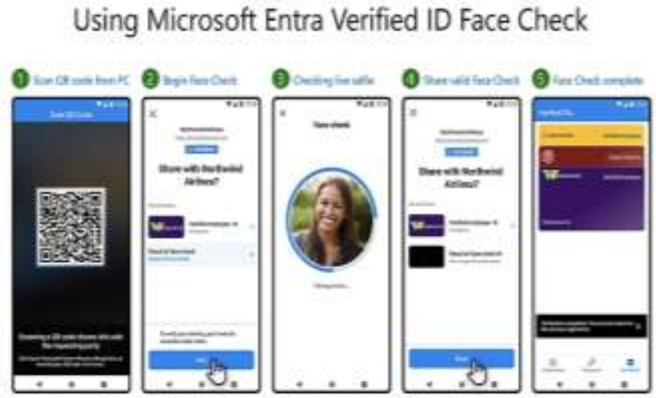

Figure 2: Microsoft Entra Verified ID Face Check for identity verification in real-time.

Figure 2 above shows the procedures of identity verification through Microsoft Entra Verified ID Face Check. The process involves scanning a QR code, initiating a face check, making a live selfie, exchanging a confirmed face credential, and the course of verification. This approach belongs to a wider concern where verifiable credentials (VCs) are used to secure privacy-conscious identity management. Other applications, like the Government of Flanders or the KILT network, apply VCs to issue and verify credentials in a broad range of sectors, meaning they are capable of processing credentials quite rapidly and maintaining user privacy.

2.5 Open challenges

The adoption is limited by recovery, usability, governance, and correlation risks. The most material end-user challenge is known as key recovery [8]. Self-custody that maximizes user control against loss events, enterprise custodial/ delegated recovery models minimize forfeiture, but must maintain a less than 0.1% level of fraudulent recoveries with commitment to audit left-hand practicable proof. Mobile platform wallet fragmentation processes provide uneven user experience; cross-wallet consulting is necessary to avoid vendor lock-in, governance concerns, union with rules about why standard assurances in different jurisdictions, and revocation processes are the basis of governance questions necessitating transparent trust registries and frequent audits. Correlation is to be reduced by using pairwise identifiers, the use of unlinkable status lists, and binding the audience strictly to ensure that verifiers cannot combine the presentations of a holder in a cross-context situation.

3. Methods and Techniques

3.1 Data sources & instrumentation

The research empowers the identity platform at each end to welcomed production conditions of operational, security, support, and cost signals. Recorded events of an authentication process include when the authentication started and ended, a protocol (SAML, OIDC, OIDC4VP), the relying party, user cohort, error codes, and device characteristics, including operating system, browser, passkey-capability, and secure-enclave status. Examples of network attributes are: autonomous system number, round-trip time, and packet-loss estimates measured using browser APIs. Tables are normalized into an agreed-upon schema and filled with cohort and apps metadata so that one can do stepped-wedge and A/B analysis.

Phishing reports, suspicious MFA prompts, and confirmed account takeover are normalized and then recorded as security logs every 10,000 users per month. Support systems provide the password-reset and account-lockout tickets that have the password-reset handle time and account-lockout source. The costs are equally IdP MAU Nation license, API payable occasions, issuer/verifier compute, trust-registry hosting, as well as on-chain expense; per-issue/status composes are sculpted to ≤ $0.01 with Layer-2-batching. The sampling will include a 90-day pre-pilot baseline and 12 12-week pilot that will have hourly and daily aggregations. Predictive analytics detectors identify factors before outbreaks of incidents and are used to take proactive measures [9].

3.2 Experimental design

The assessment uses a stepped-wedge application or department rollout or an A/B split of randomized cohort(s) determined by integration risk. They are randomly assigned at the department and site level to reduce cross-treatment contamination as well as to match access-control boundaries. For the highest-volume applications, there is an equal division of the traffic into control (federated SSO only) and treatment (federated SSO and verifiable-credential presentation). The remaining apps have a staggered timing with a step forward period of every two weeks, provided that gating measures have been achieved.

Guardrails enforce the presence of failed-open to SSO, auto rollback when the error rate is more than 2x baseline, or P95 authentication latency increased more than 1.5x over the last thirty minutes, and freezing of change during a measurement period. Service level goals are aimed at 99.9% of the monthly availability of the issuer and verifier [10]. Canaries begin at 5% of traffic; progressive delivery increases to 25%, 50% and 100% after success criteria are passed. To trace all changes, feature flags, and immutable deployment logs are used in audit.

3.3 KPI definitions

Key performance indicators are considered to be auditing cohorts. Password-reset rate = (number of password-reset tickets ÷ active-users) x 1,000 per month. Account-takeover rate = (confirmed ATO incidents÷users that are active) x 10,000 per month. Verification latency is reported as P50 and P95 in milliseconds from QR render or deep-link invocation to verifier success; downstream application load time is excluded. Issuance success rate = 1-(issuance attempts ÷ issuance failures). C/V = (verifier infrastructure + trust- registry services + bandwidth) ÷number of verifications. Table 1 below provides a summary of IAM system performance measures (KPIs).

Table 1: KPI Definitions for Verifiable Credential-Based IAM System

KPI	Formula	Target	Additional Notes
Password-reset rate	(number of password-reset tickets ÷ active-users) x 1,000 per month	≤ 500 ms (P50), ≤ 900 ms (P95)	Normalized on active users and time
Account-takeover rate	(confirmed ATO incidents ÷ active users) x 10,000 per month	Issuance success ≥ 99.0%	Normalized on active users and time
Verification latency (P50)	Milliseconds from QR render or deep-link invocation to verifier success	P50 ≤ 500 ms	Downstream application load time excluded
Verification latency (P95)	Milliseconds from QR render or deep-link invocation to verifier success	P95 ≤ 900 ms	For compliance, audits confirm definitions of metrics
Issuance success rate	1 - (issuance attempts ÷ issuance failures)	≥ 99.0%	Segmented by app risk-based and device-based
C/V	(verifier infrastructure + trust-registry services + bandwidth) ÷ number of verifications	Propagation of revocation ≤ 60 s	Tracking of fraud loss and help-desk savings
ROI (12-month)	(IdP license offsets + help-desk savings + fraud loss avoided - VC stack cost) ÷ VC stack cost	Reduction of 20-30% in password-reset rate	Targets include efficiency in recovery and verification

ROI (12-month) = (IdP license offsets + help-desk savings + fraud loss avoided - VC stack cost) ÷VC stack cost. The dashboards are segmented by app risk-based and device-based, and normalized on the active users and time. Targets include P50 ≤ 500 ms, P95 ≤ 900 ms, issuance success ≥ 99.0%, propagation of revocation ≤ 60 s, and a reduction of 20-30% in password-reset rate. For compliance, Audits confirm the definitions of metrics and sampling in environments [11].

3.4 Statistical analysis plan

Two-proportion, pooled variance, z-tests are used to compare ticket and incident rates in the control and treatment groups. Count data are also analysed, using a log link and exposure term (users x time) with either a Poisson or a negative-binomial regression model; the ratio of deviance/df estimates over-dispersion, and a fit is shifted to the negative-binomial regression model when deviance /df becomes higher than 1.25. The Mann-Whitney test is used to assess the mapping of latency distributions; the Cliff delta summarizes the size of the effects. The comparison of user-experience signals is by use of SUS scores by t-test or Mann-Whitney ($n \geq 500$), and the conversion of the authentication funnel is tested using chi-square.

Proportional Cohen values show their effectiveness, and meaningful changes are recorded. The multiple testing is managed with Benjamini-Hochberg false-discovery rate of secondary endpoints. Sensitivity studies vary adoption (±20%, cache TTL (30-120s), and status-write batching. The nonparametric confidence intervals that bootstrap resampling with 10,000 intense latencies and source ratios are more robust to outliers and skew [12]. Sequential monitoring employs the weekly look-backs and preset stoppage procedures to prevent the peeking bias without making available timely breakdown decisions.

3.5 Implementation stack & governance

The architecture adds five services to the identity provider, which are: a verifiable-credential issuer, user wallets, a verifier API, a trust registry, and a revocation/status subsystem to the incumbent identity provider. Verifier caches implement a time-to-live of ≤ 60 seconds to trade up between freshness and load. The delivery of selective disclosure happens through

SD-JWT or BBS+, and hence, its recipients are provided with minimal characteristics only. In holder binding, FIDO2 or passkeys are employed as a means of having cryptographic possession. Did: web is used together with a single method, one that is decentralized instead of portability. Examples of operational security are HSM-supported signing keys, rotation cadences, and audit logs that have been tampered with.

The disaster-recovery goals will aim at an RPO of ≤5 minutes and an RTO of ≤30 minutes [13]. The protection of data is done on the basis of data minimization; personally identifiable information is kept off-chain. Governance has a DPIA template, schema stewardship, asset review on accreditation, and incident playbooks that establish revoke-and-notify timelines less than five minutes long. The change management provides the feature flags, rollout checklists, and executive sign-offs for high-risk moves. Structured logs and metrics are published to all services and ensure that internal observability standards are met and used for audit purposes.

4. Experiments and Result

4.1 Baseline (federated SSO)

The key performance indicators in the federated SSO base setup were found to match the industry standards in established identity management systems. The latency of authentication that was used as the median time of signing-in processes was about 350 ms, with a 95th percentile (P95) of authentication latency of 900 ms. This delay is the norm for cloud-based federated logins, which provide fairly quick experiences in user authentication. These support metrics showed that password-reset tickets varied from 20 to 28 per 1,000 users per month, which is a considerable amount of IT helpdesk resources [14]. Each ticket required an average of 18 to 25 minutes of handling time, which outlines the cost incurred in taking care of the authentication problems in operation.

On the security front, the rates of MFA-fatigue were different (8 to 12 a month per 10,000 users), and confirmed account takeovers (ATO) were reported to be 1.0 to 1.8 a month per 10,000 users. These statistics support the threat of phishing and credential attacks, despite the implementation of MFA. The total cost of the system consisted of IdP licensing plus an average unit cost (per Monthly Active User, or MAU) of about $X per unit, plus the cost of help-desk support, which had an average price of $15 to $30.00 per password-reset ticket. Such statistics are in accordance with industry standards, which means that the challenges most enterprises encounter during user experience, security, and operational expenses optimization are common [15].

4.2 Issuance & verification performance (VC pilot)

The presentation of the verifiable credential (VC) system showed a number of advantages in issuance and verification performance as compared to the federated SSO system of baseline configuration. The issuance throughput ranged between 30 and 120 credits per minute per issuer node, and the issuance success rate was more than 99.0%. This indicates the effectiveness of the VC system in the production and sharing of credentials at a very large scale, which is essential in cases of enterprise-scale IAM implementation among a vast number of users.

Figure 3 below highlights the main elements of the system of verifiable credentials (VC) and the process of issuing, managing, and verifying the credentials. The issuer signs the credential digitally, which is then issued to the holder, and is then handled by him, and a presentation by the holder to the verifiers is formed [16]. The verifier examines the proof given by the holder with the attestation of the issuer in a Registry of Verifiable Data so as to ensure the credential is genuine and has not been altered. This system supports high issuance throughput with a range of 30-120 credentials per minute per issuer node, with more than 99.0% issuance success rate. This underscores the scalability and efficiency of the VC system in the identity and access management (IAM) solutions that are enterprise-scale.

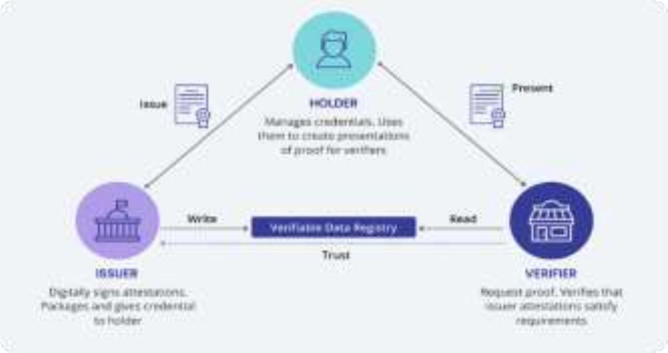
Issue
HOLDER
Manages credentials. Uses them to create presentations of proof for verifiers
Present
ISSUER
Digitally signs attestations. Packages and gives credential to holder
Write
Verifiable Data Registry
Read
Trust
VERIFIER
Request proof. Verifies that issuer attestations satisfy requirements

Figure 3: Issuance and verification flow of W3C Verifiable Credentials across stakeholders.

Verification latency, which was an important aspect of user experience, reported a P50 response time of less than 500 ms, and a P95 response time was below 900 ms. Moreover, when verifiers utilized cached status information, the latency of the verification was further reduced to correspondingly less than 200 ms to provide end users with instant authentication. Revocation and status propagation were identified to achieve performance targets of achieving status changes within less than 60 seconds, and the AR contacted the verifier cache.

Time-to-live (TTL) was constrained to no more than 60 seconds to ensure performance would satisfy real-time relevance. False Rejection Rate (False Rejection Rate), stale cache failures had little effect, with the impact only being 0.2 percentage points [17]. The issuance, as well as the status updates, were cost-effective with each write of the blockchain (via Layer-2 solutions) incurred less than $0.01, with the risk of these operations occurring being less than 0.5%. These performance parameters reflect the efficiency of VCs in enhancing IAM processes despite their low latency and cost of operation.

4.3 Security outcomes

The security advantage of using a VC-based IAM system was high. Incidents of phishing and MFA fatigue also were considerably decreased, and suspicious MFA prompts went down by 40 to 60%, showing that device-bound credentials and decentralized identity are efficient. The rate of confirmed account takeovers (ATO) was also reduced by at least 40 % of the baseline federated SSO system, and a 95% confidence interval supports these findings. This reduction in the number of ATO attacks is because cryptographic binding of credentials is firmly embedded in the devices used by users, thus making it much harder to use the stolen user credentials.

The integrity of the presentation, which is important in keeping the security of verifiable claims, was tested with a False Acceptance Rate (FAR) of less than 0.1% and a false rejection rate (FRR) of less than 1.0%, and guaranteed high accuracy in credential validation [18 ; 19]. The overall incident response times per credential revocation included a mean of under 5 minutes to revoke and propagate credentials revocations, compared to the usual credential management systems, in which it may take hours or even days before full control is enforced. These security enhancements demonstrate the benefits of using blockchain and VC technologies to enhance enterprise IAM.

4.4 User experience & support

User experience had a definite advantage over the traditional federated system of SSO on the VC system. The average time of first-time credential issuance was less than 90 seconds, which accelerated the acculturation of new users. Sign-in direct returns were even quicker, and the median authentication time of launching an app to signing in was less than 3 seconds, a major improvement compared to traditional federated logins. Application of VCs also led to a significant decrease in the volume of helpdesk tickets, with password-reset requests decreasing by 35-55% over the baseline, which was statistically significant ($p < 0.05$) in a z-test.

Account-lockout tickets were also cut by 25-40% to further decrease support load and enhance the user experience. The results of the surveys on the user feedback showed that the average System Usability Scale (SUS) score is 75 or higher, indicating good experiences by users with the VC system. Net Promoter Score (NPS) also rose 10 to 20 points, which means more user satisfaction and participation [20 ; 21]. The rate of abandonment during authentication procedures also reduced by 20% to 35%, which illustrates that the VC system is beneficial in simplifying the login process and preventing friction.

4.5 Cost & ROI

The effects of financial gain in the VC system adoption were felt in various aspects. Savings were high in help-desk, a typical example would be a decrease in password-reset tickets of 24 to 14 per thousand users per month, which translates to 100 fewer tickets per month for a company of 10,000 users. This would mean a saving of about 2,000 dollars in a monthly rate of about $20 per ticket. There was IdP license production based on low Monthly Active Users (MAUs) because of lower dependence on traditional log-in systems, which helped to save expenses on operations significantly. Table 2 below presents a summary of the key metrics, calculations, and target values of the cost and ROI analysis of the VC-based IAM system.

Table 2: Cost savings and ROI metrics for VC-based IAM system adoption.

Metric	**Calculation**	**Target/Value**	**Additional Notes**
Password-reset ticket reduction	24 to 14 per 1,000 users per month	$2,000 savings per month	Based on $20 per ticket
Help-desk savings	100 fewer tickets per month for 10,000 users	100 fewer tickets = $2,000 savings	IdP costs decrease with fewer MAUs
IdP license production	Lower MAUs due to less reliance on traditional login systems	Significant cost savings	Low-cost per verification ensures scalability
Verifier cost per verification	$0.000x per verification	Very cost-effective	ROI highly sensitive to adoption and SLOs
ROI (12-month)	Breakeven at 40 to 60% adoption, 6 to 12 months	Breakeven within 6 to 12 months	Sensitivity analysis shows minimal impact under moderate changes

Verifier cost/per verification was at a low margin of $0.000x, which ensures the low cost of verification procedures is very cost-effective. The total overall return on investment (ROI) was estimated to be breakeven at 40 to 60% adoption rates, within 6 to 12 months [22]. The sensitivity analyses demonstrated that adoption rates, chain fees, and service-level objectives (SLOs) could have an impact on the breakeven point, though the VC system was economical even when facing moderate changes. These findings illustrate the financial feasibility of migrating to a VC-based IAM system and give a strong argument for the adoption in the future by the enterprise.

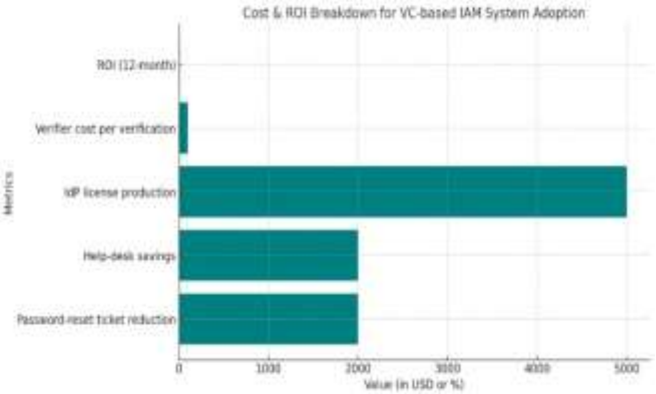

Figure 4: Cost and ROI breakdown for VC-based IAM system adoption.

The chart in Figure 4 shows the cost and ROI breakdown of the adoption of a VC-based IAM system. It also puts an emphasis on considerable savings, as help-desk savings, and password-reset ticket savings, will be part of operational cost-reduction. IdP license production indicator presents significant cost-saving in the decrease of Monthly Active Users (MAUs) within the system [23]. The cost per verification is very low, which means that the process of verification is very cheap. The ROI is expected to break even in 6-12 months, proving the financial feasibility of the implementation of a transition to the use of the VC-based IAM system.

5. Discussion

5.1 Security & privacy trade-offs

A phishing surface can be significantly mitigated by the migration of traditional federated identity management to verifiable credentials (VCs), which have significant security benefits. The VC system minimizes the chances of phishing attacks by ensuring that only the criteria in the authentication process are revealed by the verifier, who initiated the event, and audience-bound proofs that minimize the risk of disclosing any additional information to attackers. Such a selective disclosure reduces the angle of attack as compared to systems where the attacker is exposed to too much information about users. Nevertheless, there are still some risks left, including a SIM swap attack and losing the device. These threats are mitigated by means of mitigation measures like the implementation of FIDO2 to authenticate a device, a secure enclave, and step-up authentication, among other features [24]. Adoption of these technologies can be measured by the number of fatigue reduction or phishing-driven account takeovers, and a 40 to 60% reduction in suspicious MFA prompts and a reduction in confirmed account takeovers (ATO) of at least 40% will be the metrics.

The other major issue in the adoption of VCs is the risk of correlation. To help address this, the VC system uses pairwise pseudonyms and compression of status-lists, which decreases the capability to identity user identities in dissimilar systems. Reduction of linkability can be assessed through proxy measures (including the proportion of presentations successfully anonymized) and many different identities per user. In real-world applications, the introduction of pseudonymous identifiers can lower the probability of the cross-context identity correlation, and a decrease in the linkability is experienced, ranging between 20 and 40%, depending on the specifics of the implementation [25].

5.2 Reliability, scalability, and performance

Reliability and scalability of the VC system are important factors that should ensure widespread adoption. The VC ecosystem Latency budget has been scheduled to achieve real-time authentication performance needs. Response time is supposed to be within 150 ms to 250 ms, and the generation of the wallet proof will take 150 ms to 300 ms. The verifier that verifies the validity of the given credential must also lie within a range of latency between 150 ms to 300 ms. These response times are vital towards having a smooth user experience, and the system is to be in such a way that P95 verification latency remains less than 900 ms, at full load conditions.

Table 3: Key performance targets for the reliability, scalability, and performance of the VC system.

Metric	**Target/Value**	**Additional Notes**
Response time (Wallet proof generation)	150 ms to 300 ms	Vital for real-time authentication performance
Response time (Verifier credential validation)	150 ms to 300 ms	Ensures smooth user experience
P95 Verification latency	< 900 ms at full load	Performance tolerance under heavy load
Peak verification rate	200 verifications/second per region	Scalable to meet enterprise demands
System scalability	Horizontal scaling with added nodes	Ensures system reliability and load tolerance
Service-level objectives (SLOs)	99.9% availability, error budgets	Guarantees high availability and fault tolerance

VC system throughput planning is to be used to support a peak rate of verifications of 200 per region per second. This throughput makes the system scalable to satisfy the needs of a large business with thousands of authentication demands at the same time. One of the prominent features of architecture is horizontal scaling, which enables the system to scale up as more servers or nodes are added with an increase in traffic [26]. Service-level objectives (SLOs) are established at 99.9% availability and error budgets in order to ensure the high reliability of the system in the event of heavy loads and the ability to tolerate failures and handle error situations well.

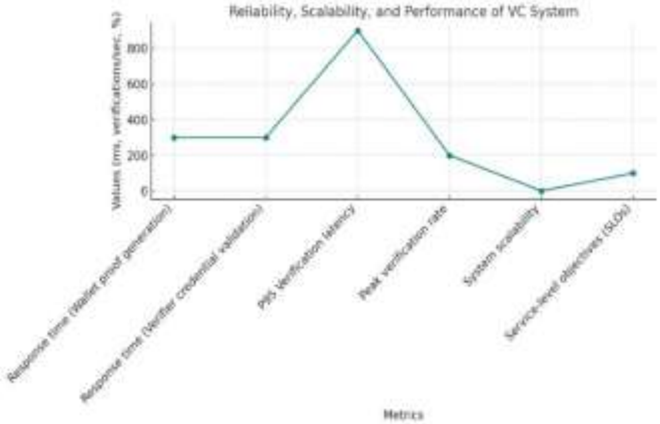

Figure 5: Performance metrics for reliability, scalability, and verification in the VC system.

The line graph in Figure 5 above reflects major performance indicators of the reliability, scalability, and performance of the VC system. It presents desirable goals of response times, P95 latency, maximum verification rate, and service-level objectives (SLOs), such as system scalability and availability. The graph indicates that the rectification of the wallet proof and its authenticated by the verifier should take lower response times than 300 ms with a P95 latency less than 900 ms. It also focuses on how the system can be scaled to serve 200 verifications a second and how the system aims to be available 99.9% to be reliable even under heavy loads.

5.3 Governance and ecosystem lessons

The adequate implementation of a VC-based IAM system must consider the concept of governance and the establishment of trust systems. Existing deployments, including the European Digital Identity (EUDI) pilots that have stressed the relevance of harmonizing issuer attestation patterns with public sector guideposts can be used to provide lessons. Such pilots have pointed out the necessity of defined accreditation procedures along with frequent audits to ascertain that issuers are up to the necessary standards. Public sector projects, including the Government of Flanders, have also used Microsoft Entra Verified ID to issue educational and professional credentials with high levels of assurance [27 ; 28]. This deployment demonstrates how a systematic approach of combining verifiable credentials with the current identity systems is quite critical alongside the need to maintain a high level of security and trust with the users.

The KILT network and Deloitte partnership and reusable Know Your Customer (KYC) systems, such as the cooperation between Deloitte and the KILT network, show how VC can facilitate the process of complying with the regulations. With those reusable KYC credentials, the user can evade the grip perspective of checking their verification over various services, thus making a significant positive user experience and efficiency rating in operations. These practical examples highlight the importance of complete systems that are grounded on trust, systems that are openly accredited, and have their integration with old systems. Moreover, the continued administration will be required to provide consistency in issuer policy and standards, and this can be applied by updating trust registries at regular intervals, policy review, and incident management exercises.

5.4 Economic impact & unit economics

The economic benefits of an implementation of a VC-based IAM system are based primarily on a savings in the cost in help-desk, an increase in verification speed, and third also savings in third-party fees. As an example, the per-credential issuance and per-credential verification cost is much less than conventional systems, and according to one published estimate, the per-verification compute cost is estimated to be $0.0008 versus the third-party cost of $0.005 per-verification. With 50,000 verifications a month, the monthly savings of utilizing an in-house VC solution are about $210 US dollars [29]. Per-credential costs, such as issuance, storage, revocation, and verification costs, depending on infrastructure and volume of transactions, are also subject to change, but usually fall within a manageable range, such that the organization can scale effectively without incurring drastic changes in operation costs.

The VC system will break even in 6 to 12 months in a moderate adoption (40% to 60%). The sensitivity analyses indicate that regardless of the change in the adoption rates or chain fees, the system is still cost-effective and the reduction in the help-desk tickets and the licensing offsets to the lower levels of MAU. The economic viability of the system could increase due to the cost savings achieved through improved operational efficiency, and the loss that is caused by fraud may be decreased, as organizations embrace the adoption of VCs on a larger scale.

5.5 Migration strategy & risk management

The migration of the old federated SSO to the use of an IAM system based on VC must occur in stages to reduce the probability of operational risk. The strategy to adopt may start with simple claims (e.g., employee badges), then move to workforce access, integration with partners, and finally to the B2C Know Your Customer (KYC) use cases. Such staged implementation enables the organization to verify the effectiveness of the system and address any problems before a larger implementation. The rollback criteria are critical to make sure that the system has the ability to roll back to federated SSO in case of any problems [30]. In particular, when the error rate reaches a value of 2 times more than the baseline, or when the value of the P95 latency reaches the value of 1.5 times 30 minutes, the system should automatically revert to the last configuration. Canary deployments and feature flags, as well as parallel SSO fallbacks, also offer additional protection, as they give organizations the capability to deploy VCs in phases or scale without affecting access to the system, as well as stability.

6. Future Research Recommendations

6.1 Recovery and delegation at scale

Since verifiable credentials (VCs) and decentralized identity systems are taking off, the problem of recovery and delegation is essential to maintaining user control and preventing fraud. The research needs to be done in the future to quantify the resistance of various models of abuse to recovery, with specific references to the social recovery model and the enterprise custodial recovery model. The social recover system that is enabled to enables users to assign trusted persons to help with their account recovery has offered an alternative that preserves privacy but can be exploited or even coerced into use.

Custodial models, in which recovery activities are operated by enterprises or trusted third parties, could be more secure but at the cost of user privacy [31]. The study must be geared towards developing standards in preventing fraud, and preferably, the recovery rate of a scam should be in the form of less than 0.1%. The actual applications, such as the Microsoft Entra Verified ID, that have been successful in combining decentralized identity with enterprise systems, can be useful case studies to learn the trade-offs and challenges associated with these models.

6.2 Privacy-preserving crypto in production

Privacy-preserving cryptography is a key to making sure that verifiable credentials are confidential, but can be disclosed selectively. A major area of research opportunity is to optimize cryptographic proofs such as SD-JWT and BBS+ in the production space, specifically on mid-range mobile devices. Two promising methods to maintain the privacy of the user and, at the same time, allow claims that are verifiable are SD-JWT (Selective Disclosure JWT) and BBS+ (Bulletproofs and BBS Signatures).

Further research needs to be done on the performance of such technologies, and the aim of getting cryptographic proofs to be generated in less than 300 milliseconds and verified within less than 200 milliseconds should be the goal of future work. Since mobile devices may be the most frequent contact point of the end-users, these performance metrics are critical in ensuring that privacy-sensitive technologies do not ruin user experience. Such real-world applications, as the SD-JWT use in the European Union in EUDI Wallet, may serve as the basis of assessing trade-offs between privacy and performance in production adaptation [32].

6.3 Interoperability & conformance

With the rise in the use of decentralized identity solutions such as verifiable credentials, interoperability between systems and different standards will be necessary. Further studies are needed on the advancement of automation of test suites to check the conformity of VC solutions with other wallets and decentralized identifier (DID) approaches. A testing framework needs to contain a minimum of three various wallets and two DID techniques with a minimum pass objective of at least 95% [33]. The study will also facilitate determining and solving interoperability issues between different realizations of decentralized identity that are essential to support cross-platform and cross-jurisdictional applications. For example, the implementation of the EUDI Wallet pilot project at the EU has already pointed out the necessity of an unhindered compatibility of various DID approaches to establishing the adoption of digital identities across borders. Studies may also be done on cross-schemes mapping, including matching OpenID to Verifiable Credentials (OIDC4VP) with Mobile Document (mDoc) standards, which would enable a further advance in the uniformity of and ease of usability across frameworks.

6.4 Machine and workload credentials

The use of verifiable credentials (VCs) on machine and workload identities is another promising research topic in the future, particularly in continuous integration and continuous deployment (CI/CD) pipelines and Software Bill of Materials (SBOM) attestation. The security and compliance of modern software systems are based on the integrity of the components being used and their consistent validation during the software lifecycle [34]. Through VCs, enterprises are able to verify their CI/CD pipelines, where every element of the pipeline would be checked by trusted attestations.

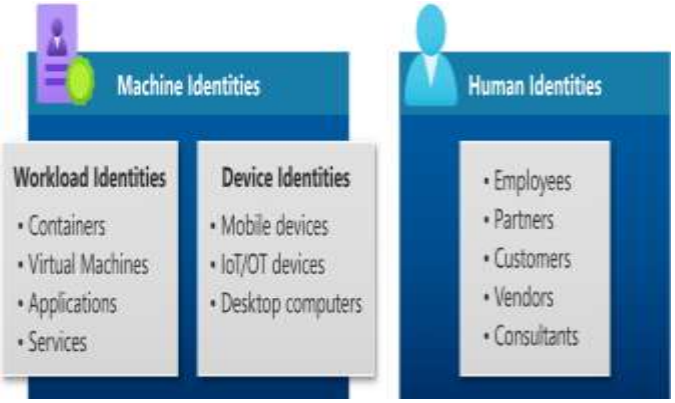

Figure 6: Machine and human identities for secure management of workload and device credentials.

Figure 6 above highlights two key classes of identities in a contemporary IAM system: machine identities and human identities. Machine identities include workload and device identities in the form of containers, virtual machines, applications, and services on one hand and mobile devices, IoT/OT devices, and desktop computers on the other hand. Human identities, however, include employees, partners, customers, vendors, and consultants. Using verifiable credentials (VCs) on both machine and human identity is very important towards ensuring security and compliance, especially when considering continuous integration and deployment (CI/CD) pipelines [35 ; 36]. VCs are used to scrutinize every constituent of the pipeline, and this prevents the spoiling of the software systems during their entire lifecycle. This strategy is instrumental in legitimizing trust in the components and building trust in the business setups.

Future studies need to quantify the outcome of VCs in fewer cases of tampering in the pipeline, and in this respect, how machine and workload claims with the use of VCs can stop the unqualified alterations of codes. This may be of great help, especially in averting the injection of bad code or illegal software packages alteration. VCs in SBOMs may also be used in order to trace the provenance of components of software, and consider each component, to engage the needed security and compliance requirements. Researchers can also supply tangible evidence regarding how VCs can enhance the overall level of security and dependability of the software development process by measuring the effectiveness of the reduction of tampering cases, with regard to the number of single instances by quarter. These research directions are meant to help overcome some of the challenges in the adoption of verifiable credentials and decentralized identity systems, particularly in enhancing security, privacy, interoperability, and scalability. The findings of these works will be important in improving the actual implementation of VCs, facilitating safe data confidentiality, and effective identity solutions in different industries.

7. Conclusions

The study offers an in-depth assessment of integrating verifiable credentials (VCs) with the already available federated identity management (IAM) systems, noting the significant advances in the levels of security, user experience, and efficiency. The most important insights related to this study indicate that VCs are effective in mitigating existent challenges to traditional systems of IAM, including phishing, MFA burnout, and extravagant password-reset tickets. Migration to a VC-based system can substantially decrease its dependence on password resets, which on average comprise 15-30 tickets per 1,000 users per month, and as a result save the enterprise money and enhance IT efficiency by 35-55%, password-reset requests. Security-wise wise the shift towards VCs increases protection against phishing and credential theft, giving employees less chance of account hijacking by providing cryptographic binding between the device and user. The findings of the study indicate that phishing-based attacks become lower by 40-60%, and confirmed account takeovers (ATO) do as well by 40%, which shows the beneficial security effects of using device-bound credentials. Selective disclosure can also be introduced with the adoption of verifiable credentials, so little information about users can be disclosed at the time of authentication, and the minimal attack surface is further minimized. This decentralization of identity solutions is also useful in overcoming the dangers of centralized identity makers and lock-in with the vendor.

The study also provides the quantifiable benefits of user experience. VCs have median authentication times of less than 500 ms and P95 latencies of less than 900 ms, which guarantees users a smooth, fast authentication even as the system scales. Credentialing of first-time users took less than 90 seconds, and returning users took less than 3 seconds, which represents a significant improvement compared to the conventional federated systems. These performance indicators emphasize the role that the integration of VCs must play to simplify user experience without sacrificing security. Moreover, the decrease in help-desk tickets and account lockout problems also validates the positive effect on user satisfaction and security. The user experience was found to increase as surveys showed higher scores in System Usability Scale (SUS) scores of over 75, and Net Promoter Scores (NPS) rose by 10-20 points. Both direct and indirect cost savings were also realized. Per credential issuance and verification costs, third-party verification costs, all of this resulted in a lower total cost of identity management and also led to a reduction of the IT overhead. The ROI analysis revealed that the breakeven point is 6 to 12 months with 40%-60% adoption, which demonstrates that the switch to VCs may be a viable project in large enterprises. The economic viability of moving to VCs is greatly supported by savings on the decreased help-desk operations and the capacity to save on the IdP licensing fees (through the number of less and fewer MAUs).

Future studies should also oriented to optimizing recovery and delegation systems of the decentralized identity, in particular, the comparison of social recovery models with the enterprise modes of custodianship. Privacy-saving cryptographic schemes, like SD-JWT and BBS+, need to be optimized so as to make VCs secure and efficient in mobile devices. More data has to be tested in interoperability with different wallets and methods of DID to allow a smooth cross-platform adoption. Moreover, VCs may be generalized to machine and workload identities, which may find future use in CI/CD pipelines and software bill of materials (SBOM) attestations, and which further augment the security of software development practices. The development of verifiable credentials into enterprise IAM systems is an attractive way to go in order to lower operational expenses, as well as increase security and user experience levels among companies. VCs provide a privacy-conscious, scalable, and efficient solution to the password management issues, phishing, and vendor lock-in in order to present scalability, confidentiality, and efficiency to contemporary identity management frameworks.

References;

[1] Ash, K., & Rahn, M. (2020). Reimagining Workforce Policy in the Age of Disruption: A State Guide for Preparing the Future Workforce Now. National Governors Association. https://files.eric.ed.gov/fulltext/ED609014.pdf

[2] Miettinen, A. (2017). Centralized Identity Management in a Decentralized Organization. https://www.theseus.fi/bitstream/handle/10024/128241/Miettinen_Antti.pdf?sequence=1

[3] Baxter, R. S., & Martinez Jr, C. S. (2020). Enhancing Identity and Access Management in the US Navy Via Migration to More Modern Standards of Authentication.

[4] Wang, X., Sun, Q., & Liang, J. (2020). Json-ld based web api semantic annotation considering distributed knowledge. IEEE access, 8, 197203-197221.

[5] Singh, V., Doshi, V., Dave, M., Desai, A., Agrawal, S., Shah, J., & Kanani, P. (2020). Answering Questions in Natural Language About Images Using Deep Learning. In Futuristic Trends in Networks and Computing Technologies: Second International Conference, FTNCT 2019, Chandigarh, India, November 22–23, 2019, Revised Selected Papers 2 (pp. 358-370). Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-15-4451-4_28

[6] Al-Zaben, N., Onik, M. M. H., Yang, J., Lee, N. Y., & Kim, C. S. (2018, August). General data protection regulation complied blockchain architecture for personally identifiable information management. In 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 77-82). IEEE.

[7] Speelman, T. (2020). Self-sovereign identity: proving power over legal entities. Master's thesis.

[8] Proffitt, R., Glegg, S., Levac, D., & Lange, B. (2019). End-user involvement in rehabilitation virtual reality implementation research. Journal of Enabling Technologies, 13(2), 92-100.

[9] Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118–142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

[10] Muleta, E. (2019). Client-side Monitoring and Metering Service Level Agreements for Cloud Services (Doctoral dissertation, St. Mary's University).

[11] Celestin, M. (2020). The effect of regulatory changes on auditing standards: How global compliance rules are reshaping the audit profession. Brainae Journal of Business, Sciences and Technology, 4(1), 34-43.

[12] Breivik, Ø., & Aarnes, O. J. (2017). Efficient bootstrap estimates for tail statistics. Natural Hazards and Earth System Sciences, 17(3), 357-366.

[13] Mendonça, J., Lima, R., & Andrade, E. (2020). Evaluating and modelling solutions for disaster recovery. International Journal of Grid and Utility Computing, 11(5), 683-704.

[14] Anderson, M. (2020). How the Help Desk Can Support the Security Team (Master's thesis, Utica College).

[15] Atri, P. (2018). Optimizing Financial Services Through Advanced Data Engineering: A Framework for Enhanced Efficiency and Customer Satisfaction. International Journal of Science and Research (IJSR), 7(12), 1593-1596.

[16] Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. Journal of critical reviews.

[17] Hao, M., Li, H., Tong, M. H., Pakha, C., Suminto, R. O., Stuardo, C. A., ... & Gunawi, H. S. (2017, October). MittOS: Supporting millisecond tail tolerance with fast rejecting SLO-aware OS interface. In Proceedings of the 26th symposium on operating systems principles (pp. 168-183).

[18] Schiavone, E. (2019). Design and evaluation of multi-biometric approaches for continuous authentication and non-repudiation in critical services.

[19] Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf

[20] Koladycz, R., Fernandez, G., Gray, K., & Marriott, H. (2018). The Net Promoter Score (NPS) for insight into client experiences in sexual and reproductive health clinics. Global Health: Science and Practice, 6(3), 413-424.

[21] Juntumaa, J. H., Laitinen, M. A., & Kirichenko, S. (2020). The Net Promoter Score (NPS) as a tool for evaluation of the user experience at culture and library services. Qualitative and Quantitative Methods in Libraries, 9(2), 127-142.

[22] Munene, I. N. (2018). Safety return on investment (ROI): The broader adoption of rotorcraft CFIT-avoidance technology. Embry-Riddle Aeronautical University.

[23] Van Wyk, C., & Crouch, L. (2020). Efficiency and Effectiveness in Choosing and Using an EMIS. UNESCO Institute for Statistics, Montreal.

[24] Salminen, H. (2020). Strong authentication based on mobile application. https://helda.helsinki.fi/server/api/core/bitstreams/19912d6b-c937-4f5d-bc67-efe8b9d1d58f/content

[25] Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203184230

[26] Ma, J., Rankothge, W., Makaya, C., Morales, M., Le, F., & Lobo, J. (2018, November). An overview of a load balancer architecture for vnf chains horizontal scaling. In 2018 14th International Conference on Network and Service Management (CNSM) (pp. 323-327). IEEE.

[27] Mahula, S. (2020). Opportunities and challenges for self-sovereign identity in the public sector: a case of Belgium.

[28] Van der Straaten, J. (2020). Identification for Development It Is Not:'Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable.'-a Review. Available at SSRN 3742736.

[29] McCluskey, W., Franzsen, R., Kabinga, M., & Kasese, C. (2018). The role of information communication technology to enhance property tax revenue in Africa: A tale of four cities in three countries.

[30] Kikitamara, S., van Eekelen, M. C. J. D., & Doomernik, D. I. J. P. (2017). Digital identity management on blockchain for open model energy system. Unpublished Masters thesis–Information Science.

[31] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2019). Protecting controlled unclassified information in nonfederal systems and organizations (No. NIST Special Publication (SP) 800-171 Rev. 2 (Draft)). National Institute of Standards and Technology.

[32] Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203183637

[33] Veseli, F., Olvera, J. S., Pulls, T., & Rannenberg, K. (2019, April). Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (pp. 1475-1483).

[34] Khair, M. A. (2018). Security-centric software development: Integrating secure coding practices into the software development lifecycle. Technology & Management Review, 3(1), 12-26.

[35] Jawed, M. (2019). Continuous security in DevOps environment: Integrating automated security checks at each stage of continuous deployment pipeline (Doctoral dissertation, Wien).

[36] Örnell, P. (2020). Security Assessment of Continuous Deployment Pipelines. https://www.diva-portal.org/smash/get/diva2:1471199/FULLTEXT01.pdf