Kabarak Journal of Research & Innovation Volume 16 Number 3 (2026)
ISSN 2305-784X (print) ISSN 2410-8383 (online)
https://journals.kabarak.ac.ke/index.php/kjri/

A Biometric Authentication Model for Enhancing Single Sign-On Security: Design and Experimental Evaluation

Authors
Pravine O. Ogeto[1], Nelson Masese[1] & Ruth Oginga[1]

Affiliations
[1]School of Science Engineering and Technology, Kabarak University

Corresponding Author:
Pravine O. Ogeto - *email* potara@kabarak.ac.ke

Article History: *Submitted: 23rd October 2025; Accepted: 13th October 2026; Published (online): 3rd November 2026*

Abstract

Single Sign-On (SSO) simplifies access to multiple applications but increases authentication risk because compromise of one reusable credential can expose several services. This study developed and experimentally evaluated a biometric authentication prototype intended to reduce reliance on passwords in SSO workflows. The study used an applied, design-oriented approach combining a structured review of SSO and authentication literature, a survey of Kenya Urban Roads Authority (KURA) employees, Design Thinking, rapid prototyping, and controlled biometric testing. From a planned sample of 171 employees, 48 questionnaire submissions were received; two respondents declined consent, leaving 46 valid responses for analysis (26.9% of the planned sample). Forgotten passwords were the most frequently reported challenge (30/46, 65.2%), followed by system lag (17/46, 37.0%), account lockouts (15/46, 32.6%), and difficulty accessing one-time passwords (14/46, 30.4%). The implemented proof of concept contained two distinct authentication paths: a WebAuthn public-key path in which user verification is performed by the authenticator and the server stores public-key credentials, and an experimental FVC2004 fingerprint-matching path in which uploaded .tif samples simulate biometric capture. The biometric simulation comprised 44 genuine and 50 impostor authentication attempts. Three genuine attempts were rejected, and one impostor attempt was accepted, yielding a false rejection rate of 6.82% and a false acceptance rate of 2.00%. The results demonstrate prototype feasibility and biometric matching performance under controlled conditions, not proven resistance to all credential-compromise threats or effectiveness in a live KURA deployment. Further organizational, usability, penetration, spoofing-resistance, and scalability testing is required before operational adoption.

Keywords:
Biometric Authentication; Credential Compromise; Experimental Evaluation; Fingerprint Verification; Single Sign-On; WebAuthn

Introduction

Single Sign-On (SSO) enables a user to authenticate once and access multiple applications, reducing repeated logins and the burden of password management. However, centralizing

authentication can increase the impact of security breaches. If the identity provider or a reusable authentication secret is compromised, an attacker may gain access to several connected services. Baum et al. (2020) addressed this single-point-of-failure problem through PESTO, a distributed SSO design intended to remain secure under defined server-compromise scenarios. Measurement studies also show that deployed SSO systems do not always follow recommended security practices. Westers et al. (2023) introduced SSO-Monitor, an automated tool for examining the security and privacy of SSO implementations across websites. Their analysis identified client-secret leakages, weak or missing cross-site request forgery protection, insecure SSO flows, and privacy leakages, illustrating that implementation quality remains important alongside protocol design.

User preferences and organizational implementation practices introduce additional concerns. In a study involving 200 participants, Morkonda et al. (2024) found that usability preferences and habitual behavior influenced login decisions. Displaying permission differences also led many participants to choose more privacy-friendly SSO options. Singh et al. (2024) interviewed 45 cybersecurity professionals about identity and access management. Participants reported different challenges across cloud and on-premises deployments, including default configurations, service-account management, certificate and API configuration, limited log analysis, weak password policies, unpatched vulnerabilities, and risks associated with SSO compromise. Organizations often use passwords with one-time passwords or other multi-factor authentication mechanisms, but an additional factor does not eliminate every authentication threat. Bianchi and Valeriani (2023) demonstrated a forward-replay attack against time-based OTPs in which manipulating a device clock could allow an attacker to collect codes for later use.

Mahdad et al. (2021) evaluated seven commercially deployed OTP-based two-factor authentication schemes against malware in the terminal attack model. Their work examined how malware on a login terminal can undermine OTP-based protections without necessarily compromising the second-factor device or the authentication service. Shibayama and Kikuchi (2021) described a password-reset man-in-the-middle attack involving SMS OTPs. Their analysis highlighted how SMS notification previews and code autofill functions can obscure warning information that might otherwise alert a user to a suspicious authentication request. Otta et al. (2023) systematically surveyed MFA methods for cloud infrastructure and reviewed the security and deployment challenges associated with these approaches. These studies show that adding an OTP or another factor does not, by itself, remove all risks arising from implementation weaknesses or user interaction.

WebAuthn takes a different approach by using public-key credentials scoped to a relying party. The World Wide Web Consortium (W3C, 2026) specifies that biometric user verification is performed locally by the authenticator and that biometric data is not disclosed to the relying party. The WebAuthn model also uses challenge-based authentication and origin-scoped credentials, which are designed to reduce exposure to phishing and replay when implemented correctly (W3C, 2026).

Biometrics can complement public-key authentication by linking use of an authenticator to a physical user, but they are not secrets and should not be treated as a stand-alone guarantee of security. Jain et al. (2022) reviewed persistent concerns in biometric systems, including spoofing and adversarial attacks, template reconstruction, demographic information leakage, bias, fairness, explainability, and privacy. Yang et al. (2021) reviewed biometric authentication

and biometric-cryptographic techniques in Internet of Things security, identifying application challenges and possible approaches to protecting biometric systems. The National Institute of Standards and Technology (NIST, 2025) requires biometrics to be used in conjunction with a physical authenticator and provides guidance on biometric performance, presentation-attack detection, and protection of biometric information. This guidance supports treating biometrics as one part of a broader authentication architecture rather than as a stand-alone guarantee or simply replacing a password with a centrally stored fingerprint template.

This study addressed the gap by using the weaknesses reported by SSO users to develop and test the prototype. The prototype integrated the SSO process, public key authentication and biometric verification. Baum et al. (2020) proposed PESTO as a distributed SSO design intended to reduce reliance on a single fully trusted identity-provider server. Frederiksen et al. (2023) proposed an attribute-based SSO approach using multiparty computation and threshold cryptography to distribute the identity-provider role and limit the exposure of user attributes and access patterns. Carroll and Latifi (2025) compared passkeys on Android and iOS and discussed the data-protection implications of keeping biometric processing on the user's device. Jain et al. (2022) examined broader concerns about biometric performance, spoofing, fairness, and privacy. Yang et al. (2021) reviewed biometric authentication and cryptographic approaches in Internet of Things security. Westers et al. (2023) measured security and privacy weaknesses in deployed SSO implementations, but these studies did not evaluate the hybrid prototype examined here. This research study therefore focuses on translating organizationally reported authentication challenges into a prototype and reporting its functional behavior and controlled fingerprint-matching results.

Literature Review

Theoretical Framework

This study follows two theoretical frameworks. One is the Zero Trust Security Model which was introduced by Kindervag (2012) and has become one of the most influential cybersecurity frameworks for securing modern information systems. The model is founded on the principle of never trust, always verify, which assumes that no user, device, or system should be automatically trusted regardless of whether it is located inside or outside an organizational network. Every access request must therefore be continuously verified before access to protected resources is granted (Kindervag, 2012).

The second is the Technology Acceptance Model which was developed by Davis (1989) to explain factors that influence the acceptance and use of information technologies. The model demonstrates that user adoption of technology is primarily determined by two factors: perceived usefulness and perceived ease of use. Perceived usefulness refers to the degree to which an individual believes that using technology will improve performance, while perceived ease of use refers to the degree to which an individual believes that technology will be simple and effortless to use (Davis, 1989).

Empirical Review

Identifying weaknesses in current SSO authentication mechanisms

In their experiment, Tolbert et al. (2022) identified significant weaknesses in existing SSO authentication mechanisms, particularly phone-based authentication (PBA). They found that all six tested phone-based authentication configurations were successfully compromised through malicious-site attacks. In the user study involving 13 participants, all eight participants tested in the malicious-site scenarios experienced successful attacks, with only one reporting

suspicious symptoms during the interview. Similarly, all seven participants tested in the timing-attack scenarios were successfully attacked, and none noticed or reported suspicious symptoms. Overall, 12 of the 13 participants did not notice the attacks, demonstrating that existing phone-based SSO authentication mechanisms can be vulnerable to attacks that users may fail to detect (Tolbert et al., 2022). Ozkan and Bicakci (2020) observed that OTP-based authentication mechanisms remain exposed where shared secret values are compromised.

Designing an Integrated secure biometric authentication model as a security enhancement for SSO

Morake et al. (2021) observed that biometric technologies enhance both security and convenience by reducing dependence on passwords while improving the user authentication experience. Similarly, Alrawili et al. (2024) reported that biometric authentication systems provide stronger protection against credential theft and phishing attacks compared to conventional authentication mechanisms. Despite these benefits, biometric authentication systems also present several challenges. Hussaini (2024) identified privacy and security concerns associated with the collection, storage, and processing of biometric data. Alrawili et al. (2024) further noted that biometric systems remain susceptible to spoofing attacks and face regulatory and compliance challenges related to handling sensitive personal information. In addition, recent studies have highlighted emerging threats such as deep-fake-based attacks targeting facial and voice recognition systems, raising concerns about the resilience of certain biometric modalities against sophisticated adversaries (He et al., 2025). These strengths and weaknesses informed the design of the authentication model by emphasizing the need for secure biometric template protection, phishing-resistant authentication mechanisms, and effective safeguards against unauthorized access.

Implementation of the secure biometric authentication model as a security enhancement for SSO

Westers et al. (2023) examined real-world Single Sign-On deployments using SSO-Monitor, an automated tool for analyzing SSO security and privacy. Their analysis identified security weaknesses, including client-secret leakages, weak or missing Cross-Site Request Forgery (CSRF) protection, and insecure SSO flows. The study also identified privacy leakages that could expose users to tracking without their knowledge. These findings highlight the importance of secure implementation and configuration of SSO systems and support the need for stronger authentication mechanisms to reduce the risk of unauthorized access. Slamet et al. (2021) emphasized the importance of securing authentication communications and credentials, although modern cryptographic approaches were required. These insights from these studies guided the implementation of a secure biometric authentication model designed to enhance SSO security while maintaining usability.

Evaluation of the model in reducing unauthorized access

Yang et al. (2021) reviewed biometric authentication approaches for Internet of Things (IoT) security, examining different biometric traits, biometric-cryptographic systems, and challenges associated with their implementation. Their review also discussed performance measures used to assess biometric authentication systems, including the False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and recognition accuracy. FAR measures the rate at which unauthorized users are incorrectly accepted, whereas FRR measures the rate at which legitimate users are incorrectly rejected. The review informed the selection of performance measures for the present study, which assessed fingerprint-matching performance using FAR, FRR, and overall attempt-level accuracy.

Similarly, Alrawili et al. (2024) surveyed biometric authentication applications and evaluation approaches, highlighting the importance of FAR and FRR in assessing the trade-off between security and usability. Their findings showed that lower FAR values indicate stronger protection against unauthorized access, whereas lower FRR values improve user convenience by minimizing rejection of legitimate users. These findings also informed the research study of the importance of evaluating both security effectiveness and user experience when assessing authentication systems.

Methodology

Research Design

This study used an applied, design-oriented approach. The study combined a structured literature review, a questionnaire survey of Kenya Urban Roads Authority employees, iterative prototype development guided by Design Thinking, and controlled experimental testing. The literature review and survey provided evidence of weaknesses in existing SSO authentication mechanisms and informed the identification of user and security requirements. These requirements guided the design and implementation of a hybrid experimental prototype incorporating a WebAuthn-based public-key authentication pathway and a separate FVC2004 fingerprint-matching pathway. Functional testing assessed the prototype's operational behaviour, while controlled fingerprint-matching experiments evaluated its performance using genuine and impostor attempts. The findings were analysed using descriptive performance measures, including the false acceptance rate and false rejection rate. These activities were linked sequentially, with findings from the literature and survey informing requirements, requirements guiding design, design informing implementation, and experimental results providing evidence of the prototype's performance and limitations.

Table 1 summarizes how each study objective is linked to the methods, supporting evidence, and intended outputs.

Table 1: Objective, Method, Data and Outputs

Study purpose	Method	Data/evidence	Output
Identify weaknesses in existing SSO authentication	KURA survey plus structured literature review	Valid survey responses (n = 46) and relevant research/standards	Prioritized SSO weaknesses and security requirements
Design the authentication model	Design Thinking: empathize, define, ideate, model	Survey findings, literature themes, security requirements	Architecture, data flow, sequence logic, five core components
Implement the prototype	Rapid prototyping using React.js, Laravel, MySQL, WebAuthn-style flows, and FVC2004 simulation	Design artefacts, source code, test data	Operational hybrid authentication proof of concept

Study purpose	Method	Data/evidence	Output
Evaluate the prototype	Functional tests and controlled biometric verification	44 genuine attempts; 50 impostor attempts; authentication logs	Functional evidence, FAR, FRR, limitations

Design Thinking and Requirements Translation

Design Thinking was used to convert observed user problems and literature-based security concerns into implementable requirements. The stages were not treated as labels only; each produced a concrete output used in the next stage. Table 2 summarizes the activities and intended outputs associated with each Design Thinking stage.

Table 2: Design Thinking and Requirements Translation

Stage	Activity performed	Output used in the prototype
Empathize	Survey responses and literature were examined to understand password fatigue, lockouts, OTP difficulties, credential compromise and usability concerns.	User and security needs.
Define	The problem was reframed as excessive dependence on transferable credentials within an SSO environment.	Requirement for stronger, phishing-resistant authentication and controlled fallback.
Ideate	Passwords, OTPs, smart cards, biometrics and public-key options were compared.	Selection of biometric verification plus a WebAuthn public-key path and SSO integration.
Model/Prototype	Architecture, data flow, credential storage, user interfaces and authentication workflows were implemented iteratively.	Operational proof of concept and administrative functions.
Test	Functional behavior and fingerprint matching were evaluated; limitations were recorded.	Test outcomes, error metrics and refinement priorities.

Study Population, Sampling and Survey Procedure

The study population comprised 297 permanent KURA employees. A planned sample of 171 was calculated using Yamane's finite-population formula with a 5% margin of error. Stratified random sampling was used rather than purposive sampling. The sampling frame was divided into five organizational areas because they interact with information systems in different ways: ICT staff manage technical and security infrastructure; Human Resource and Administration staff access employee-information systems; Engineering/Roads and Asset Corridor Management staff use project and operational systems; Finance and Accounts staff use sensitive financial systems; and Supply Chain Management staff access procurement and supplier systems. Proportional selection across these strata was intended to broaden the range of authentication experiences represented.

The online questionnaire received 48 submissions. Of these, 46 respondents consented to participate and two declined. The final survey analysis therefore used 46 valid, consenting responses, equivalent to 26.9% of the planned sample of 171. The raw submission rate was 28.1% (48/171). This response was substantially smaller than the planned sample and creates a risk of non-response bias. Accordingly, the survey findings are presented as descriptive evidence from respondents rather than as estimates that can be confidently generalized to all KURA employees.

Questionnaire Development, Validity and Reliability

The questionnaire was administered through Google Forms and contained closed-ended items for respondent characteristics and authentication challenges, together with open-ended opportunities for additional comments. Items were derived from the study questions and literature on SSO and authentication security. Content validity was assessed through review by information-technology and information-security experts for relevance, clarity, and coverage, after which wording was refined. All participants received the same online instrument and response options. The study record did not document a separate pilot sample or a psychometric reliability coefficient. Because the instrument was used mainly to collect categorical experience frequencies rather than to form a multi-item latent scale, Cronbach's alpha was not treated as a required statistic. This limitation is stated explicitly rather than inferring an unrecorded reliability estimate.

Prototype Architecture and WebAuthn

The architecture distinguishes two technically different authentication mechanisms. The first is a WebAuthn public-key authentication path. In a standards-conformant WebAuthn ceremony, biometric or PIN-based user verification occurs locally within the authenticator; the private key remains under the authenticator’s control, and the relying-party server stores a credential identifier and public key rather than a fingerprint template (W3C, 2026). The server issues a challenge and verifies the signed assertion before establishing the authenticated session. The second is an experimental fingerprint-matching path used to evaluate biometric performance. In this path, FVC2004 .tif images are uploaded to simulate sensor input; features are extracted and compared with an experimental template store, and the prototype returns a match result.

Accordingly, this study describes the implemented artefact as a hybrid experimental prototype. Its WebAuthn-related code follows public-key registration and authentication concepts, while its FVC2004 pathway performs conventional server-side biometric matching for research purposes. The FAR and FRR results reported in this study apply to the FVC2004 matching experiment and should not be interpreted as performance measurements of WebAuthn itself.
W3C (2026) specifies that WebAuthn biometric recognition is performed locally within the authenticator and that biometric data is not disclosed to the relying party. The FIDO Alliance (n.d.) likewise explains that biometric information used during passkey authentication remains on the user’s device, while the remote service receives confirmation that user verification succeeded. Figure 1 illustrates the separation between the WebAuthn public-key authentication path and the experimental FVC2004 fingerprint-matching path.

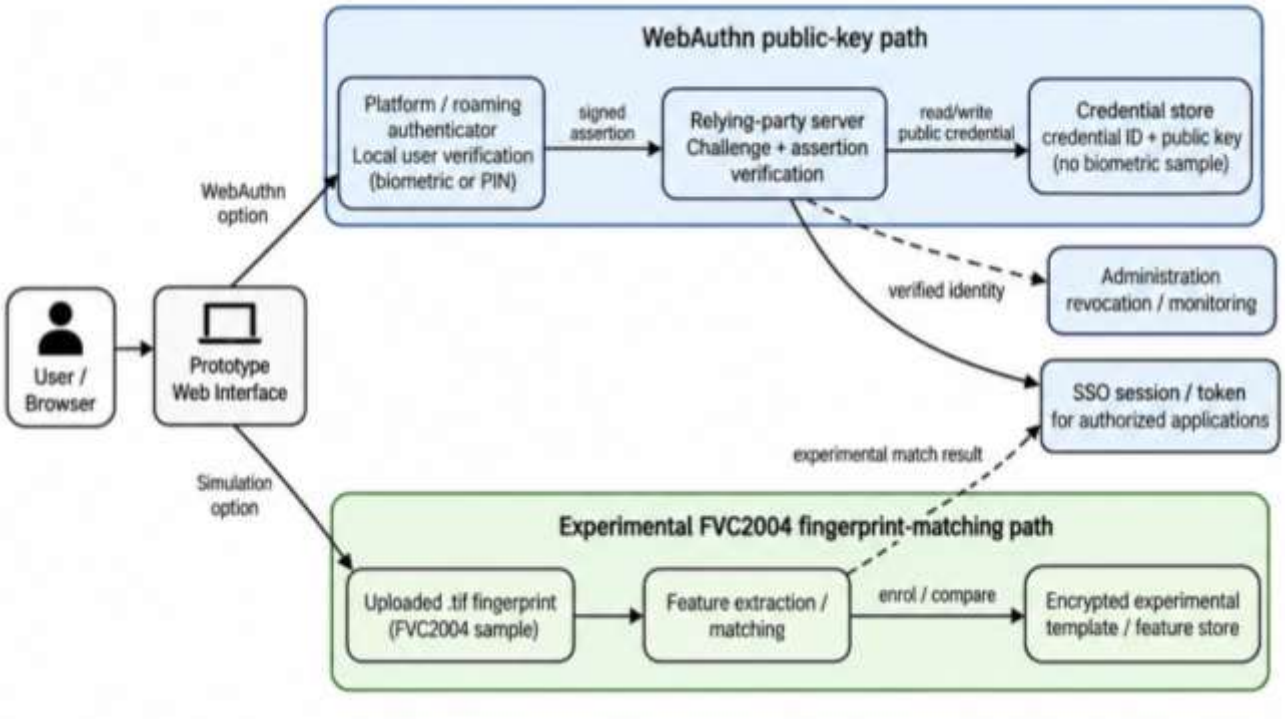


Figure 1. Architecture separating the WebAuthn public-key path from the experimental FVC2004 matching path.

Template Protection, Secrets and Communication Security

For the experimental fingerprint-matching path, AES-based encryption was specified for biometric templates and authentication data. AES is a standardized symmetric block cipher defined in FIPS 197 (NIST, 2023). In the prototype, application secrets were kept outside the database in environment configuration rather than embedded in published source-code examples. Database access was mediated by the server application and role-based application controls. For a production deployment, communication among the browser, authenticator, relying party, and any central biometric verifier would require an authenticated, protected channel such as TLS/HTTPS, consistent with NIST guidance for transmitted biometric information (NIST, 2025). The exact AES mode, key-rotation process, hardware protection, and production secret-management lifecycle were not fully documented in the source study and therefore are not claimed as validated controls.

Configuration details are presented using redacted values to avoid disclosing application keys, usernames, database information, hosts, URLs, or passwords. Examples use placeholders such as APP_KEY = [REDACTED], DB_USERNAME = [REDACTED], DB_PASSWORD = [REDACTED], and APP_URL = https://[host]. This approach provides sufficient implementation detail for scholarly explanation without exposing sensitive configuration information.

Threat Model

The threat model defines the protected assets, attacker capabilities, relevant attack vectors, and the extent to which each threat was addressed. The protected assets were authentication credentials, SSO sessions or tokens, biometric templates used in the experimental path, public-key credentials, and user account access. The assumed attacker could possess stolen passwords, operate phishing pages, replay captured messages, attempt impostor fingerprints, or obtain

database contents. A fully compromised client device or a successful presentation attack was considered possible but was not experimentally reproduced. Table 3 summarizes the principal threats, corresponding design mitigations, and whether each threat was empirically tested in this study.

Table 3: Threat Model

Threat/attack vector	Attacker capability	Design mitigation	Empirical status in this study
Stolen or reused password	Possesses a password or password database dump	WebAuthn path reduces dependence on reusable shared secrets; SSO access follows successful stronger authentication.	Architectural mitigation; not a live breach simulation.
Phishing	Operates a fraudulent login origin to capture credentials	Origin-scoped WebAuthn credentials and public-key challenge response are designed to resist credential replay at another origin.	Supported by standards rationale; phishing campaign not executed.
Replay	Reuses a captured authentication response	Fresh server challenge/nonces in WebAuthn-style flow.	Architectural mitigation; dedicated replay penetration test not retained.
Impostor biometric attempt	Presents a non-matching fingerprint sample	Fingerprint matcher rejects samples below the decision threshold.	Tested with 50 impostor attempts; 49 rejected, 1 accepted.
Presentation/spoof attack	Uses an artefact or fake biometric sample	Would require presentation attack detection and trusted sensor controls.	Not tested; important limitation.
Database compromise	Obtains server-side stored data	Public-key path stores public credentials only; experimental templates were encrypted at rest.	Database-breach attack not executed; key management not fully validated.
Compromised endpoint or authenticator	Controls user device or malware environment	Attestation, protected key storage and device trust can reduce risk in a production FIDO deployment.	Not tested.

Evaluation Protocol and Metrics

Functional testing covered registration, enrollment, authentication, credential handling, administrative functions, and SSO handoff. Biometric testing used fingerprint images from the FVC2004 benchmark to simulate capture through a .tif upload interface. Maio et al. (2004) described FVC2004 as a competition for evaluating fingerprint-verification algorithms using data collected with different sensors and testing conditions. Cappelli et al. (2006) examined the

theoretical and practical issues involved in evaluating fingerprint-verification systems and reported the results of the FVC2004 evaluation as a controlled benchmark.

The study records documented 44 genuine authentication attempts and 50 impostor attempts. The number of unique fingers or subjects and the repetition schedule were not recorded; therefore, the results are reported at the attempt level without inferring a subject count. This omission limits reproducibility and is acknowledged as a study limitation.

The false acceptance rate (FAR) was calculated by dividing the number of impostor attempts incorrectly accepted by the total number of impostor attempts. The false rejection rate (FRR) was calculated by dividing the number of genuine attempts incorrectly rejected by the total number of genuine attempts. Ninety-five percent confidence intervals were calculated using Wilson's binomial method. FAR and FRR are reported as descriptive performance measures under the controlled experimental conditions, not as evidence of statistical significance. FAR below 3% and FRR below 10% were researcher-defined prototype acceptance criteria, not international standards or inferential hypothesis tests.

Ethical Considerations

Ethical approval for the study was obtained from the Kabarak University Scientific and Ethics Review Committee, and a research permit was obtained from the National Commission for Science, Technology and Innovation (NACOSTI). Participation was voluntary, and informed consent was obtained from all participants before data collection. Participants were informed of the purpose of the study, their right to withdraw at any stage, and the measures taken to protect confidentiality. No personally identifiable information was collected. Questionnaire responses were anonymized and stored securely using password-protected systems accessible only to the researcher.

Results

Survey Response and Existing SSO Weaknesses

Among the 46 valid survey responses, forgotten passwords were reported by 30 respondents (65.2%), system lag by 17 (37.0%), account lockouts by 15 (32.6%), difficulty accessing OTPs by 14 (30.4%), biometric failure by 2 (4.3%), and lost smart cards by 1 (2.2%); five respondents (10.9%) reported no challenge. These frequencies are descriptive; no inferential hypothesis testing was conducted.

The survey indicates that password management was the most frequently reported issue among respondents. It does not establish the prevalence of each weakness among all KURA employees because the valid response rate was 26.9%. The low frequency of reported biometric failure is not treated as evidence that biometric systems perform well; it describes only respondents' reported experiences. Actual biometric performance was evaluated separately through the controlled fingerprint experiment. Figure 2 presents the reported authentication challenges by frequency.

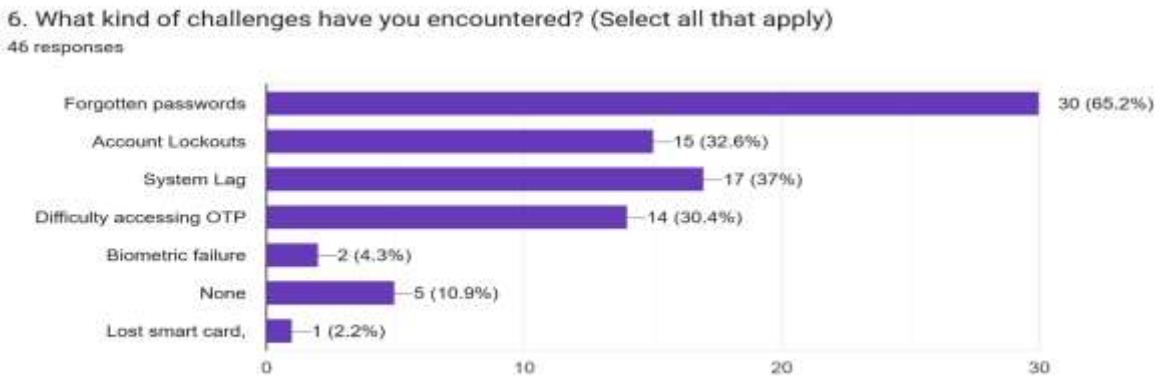


Figure 2. Authentication challenges reported by valid survey respondents (n = 46).

Design Outputs

Five core components were designed: user enrollment, authentication, credential/template storage for the relevant path, SSO integration, and revocation/renewal. Four planned design artefacts were also completed. The Component Design Rate (5/5 = 100%) and Readiness Score (4/4 = 100%) are reported as project-completion indicators; they are not statistical measures and do not demonstrate statistical significance. The 80–100% design criterion was a researcher-defined internal completion target used to decide whether the prototype was sufficiently specified to proceed to implementation. Table 4 summarizes these two indicators and their interpretations.

Table 4: Design Outputs

Indicator	Computation	Observed result	Interpretation
Component Design Rate	5 designed components / 5 planned	100%	All planned components were specified; completion measure only.
Readiness Score	4 completed design artefacts / 4 planned	100%	All planned diagrams/workflows were prepared; readiness measure only.

Prototype Implementation and Functional Tests

The prototype was implemented with a web-based client, Laravel server-side logic, a MySQL data store, WebAuthn-style public-key registration and authentication code, and an FVC2004 fingerprint-simulation interface. The fingerprint simulator accepted .tif files so that enrollment and comparison could be tested without a physical fingerprint sensor. This environment served as an experimental substitute for live-device biometric capture and did not reproduce device secure enclaves, sensor attestation, presentation-attack detection, network variability, or operating-system authenticator behavior. Figure 3 shows the upload interface used to simulate fingerprint input with FVC2004 .tif samples.



Figure 3. FVC2004 .tif upload interface used to simulate fingerprint input.

Table 5 summarizes the prototype's functional test cases, expected and observed outcomes, and the limitations associated with each test.

Table 5: Prototype Implementation and Functional Tests

Test case	Expected outcome	Observed outcome	Qualification/limitation
User registration	Account created and user record available for authentication.	Registration workflow operated in the prototype.	Demonstrative functional test, not a production acceptance test.
FVC fingerprint enrollment	Uploaded .tif sample processed and enrolled for later comparison.	Enrollment and storage workflow operated.	Simulated sensor input.
Genuine fingerprint authentication	Registered sample accepted when similarity exceeded threshold.	41 of 44 genuine attempts were accepted.	Three false rejections occurred.
Impostor fingerprint authentication	Unregistered/non-matching sample rejected.	49 of 50 impostor attempts were rejected.	One false acceptance occurred.
WebAuthn registration/login flow	Server issues options/challenge and verifies public-key credential response.	Code path generated challenge/options and processed credential assertions.	Whole prototype was hybrid; not a conformance certification.
SSO handoff	Verified identity establishes session/token for authorized applications.	Prototype demonstrated post-authentication SSO handoff.	No multi-application production federation load test.
Credential administration	Revocation/renewal and role-based administration available.	Administrative functions were present in the implementation.	Formal negative/abuse test log was not retained.

Formal negative or abuse-test logs were not available; therefore, the functional evaluation is presented as a demonstrative prototype test rather than an exhaustive quality-assurance assessment. The observed false-acceptance and false-rejection outcomes are reported as biometric classification errors.

Biometric Matching Results

The controlled test comprised 94 authentication attempts: 44 genuine and 50 impostor. Of the 44 genuine attempts, 41 were correctly accepted and three were falsely rejected; of the 50 impostor attempts, 49 were correctly rejected and one was falsely accepted as shown in Table 6.

Table 6: Biometric Matching Results

Actual class	Accepted by prototype	Rejected by prototype	Total
Genuine/authorized	41 (correct acceptance)	3 (false rejection)	44
Impostor/unauthorized	1 (false acceptance)	49 (correct rejection)	50

Table 7 reports a FAR of 1/50 = 2.00% (95% Wilson CI: 0.35%–10.50%), and an FRR of 3/44 = 6.82% (95% Wilson CI: 2.35%–18.23%). Overall attempt-level accuracy was 90/94 = 95.74%. The confidence intervals are wide because the number of attempts was small.

Table 7: FAR, FRR, and Overall Accuracy Estimates

Metric	Numerator / denominator	Estimate	95% Wilson CI	Interpretation
FAR	1 false acceptance / 50 impostor attempts	2.00%	0.35% to 10.50%	Attempt-level impostor acceptance under the experimental conditions.
FRR	3 false rejections / 44 genuine attempts	6.82%	2.35% to 18.23%	Attempt-level genuine rejection under the experimental conditions.
Overall accuracy	90 correct / 94 total attempts	95.74%	Not calculated	Not used as a security benchmark

Security Scope Against the Threat Model

The experiment directly measured fingerprint-classification behavior only. It did not empirically establish end-to-end resistance to phishing, replay, presentation attacks, malware on a compromised device, or database exfiltration. W3C (2026) specifies relying-party-scoped public-key credentials and challenge-based authentication in WebAuthn, providing an architectural rationale for resistance to phishing and replay when the specification is implemented correctly. NIST (2025) sets additional requirements and recommendations for biometric performance, presentation-attack detection, and protected transmission; those requirements were not evaluated as part of this experiment. These standards-based properties should not be reported as attack-test results unless the deployed implementation has been subjected to adversarial testing. Similarly, encrypted experimental templates reduce exposure at rest, but encryption alone does not demonstrate resilience to server compromise if encryption keys and application access are also compromised.

Discussion

The survey findings reinforce the practical burden created by password dependence. Forgotten passwords affected 65.2% of valid respondents, while account lockouts and OTP-access difficulties were also reported. These are descriptive results from 46 respondents and cannot establish the prevalence of these experiences among all KURA employees because the valid response rate was 26.9%. Prior studies help explain why OTP-based controls do not remove every authentication risk. Bianchi and Valeriani (2023) demonstrated the feasibility of forward-replay attacks against time-based OTPs when an attacker can manipulate a device clock. Mahdad et al. (2021) examined OTP-based two-factor schemes under a malicious-terminal threat model, showing why terminal security matters even when a separate second-factor device is used.

Shibayama and Kikuchi (2021) analyzed how SMS previews and autofill features can help an attacker exploit password-reset OTP workflows. Otta et al. (2023) reviewed MFA for cloud infrastructure and discussed the security and deployment challenges associated with different MFA methods. Singh et al. (2024) reported additional identity and access management issues identified through interviews with cybersecurity professionals, including configuration and management weaknesses and the potential consequences of SSO compromise. The architectural contribution of this study is the explicit separation of biometric user verification from the relying-party server's role in WebAuthn. W3C (2026) specifies that biometric recognition can be carried out locally by an authenticator without revealing biometric data to the relying party. The FIDO Alliance (n.d.) similarly describes passkey authentication as keeping biometric information and processing on the user's device.

The prototype's FVC2004 pathway is therefore best understood as a separate experimental biometric matcher used to quantify FAR and FRR. This distinction separates the standards-based WebAuthn authentication mechanism from the experimental server-side fingerprint-matching pathway used for biometric evaluation. The biometric experiment showed one false acceptance among 50 impostor attempts and three false rejections among 44 genuine attempts. These values indicate how the matcher behaved under the selected FVC2004 simulation, but they do not prove overall system security or user usability. FAR and FRR measure classification errors; they do not capture phishing resistance, compromised endpoints, template theft, session management, authorization errors, or user satisfaction.

Jain et al. (2022) highlighted several wider biometric-system concerns, including spoofing, adversarial attacks, template reconstruction, demographic information leakage, bias, and user privacy. These concerns illustrate why a small set of match/non-match outcomes cannot provide a complete assessment of biometric security. The wide confidence intervals also show that a small number of attempts can produce unstable point estimates. A much larger protocol with documented unique subjects, repetitions, sensor conditions, and demographic composition would be required for a stronger performance claim. NIST (2025) provides biometric performance and presentation-attack guidance that goes beyond the researcher-defined thresholds used in this prototype. The present experiment was not designed as a NIST conformance evaluation; the thresholds were internal exploratory targets, not international benchmarks.

The security implications are therefore conditional. WebAuthn's public-key authentication model offers a way to reduce reliance on reusable secrets, while biometric user verification can

strengthen the link between an authenticator and its user. W3C (2026) explains that WebAuthn authenticators perform biometric recognition locally and do not disclose biometric data to the relying party. The FIDO Alliance (n.d.) similarly describes passkeys as using public-key credentials while keeping biometric processing on the user's device. Carroll and Latifi (2025) discussed the data-protection implications of this match-on-device approach when comparing passkeys on Android and iOS. By contrast, centralized biometric matching introduces additional privacy, key-management, database-breach, and presentation-attack risks that must be addressed explicitly.

A production implementation should favor authenticator-local biometrics wherever possible and use central biometric storage only when justified by a documented risk assessment. It should also apply strong encryption, access controls, key management, logging, revocation, and privacy safeguards. Generalizability remains limited in two ways: the organizational evidence came from a low-response survey at one Kenyan public institution, and the biometric evidence came from a controlled FVC2004 dataset and a .tif upload simulation rather than a live KURA deployment. The findings support prototype feasibility and quantify the experimental matcher under the tested conditions; they do not demonstrate that the same error rates, usability, or threat resistance would occur in an operational environment.

Conclusion

This study developed and evaluated a hybrid biometric SSO prototype in response to user-reported password and OTP challenges. Among the 46 consenting KURA respondents, forgotten passwords were the most frequently reported authentication challenge. The implemented proof of concept combined an SSO workflow, WebAuthn-style public-key functions, and a separate FVC2004 fingerprint-matching simulation. In 44 genuine and 50 impostor attempts, the experimental matcher produced an FRR of 6.82% and FAR of 2.00%. These results demonstrate technical feasibility and defined biometric matching performance under controlled experimental conditions. They do not establish a statistically significant reduction in credential compromise, complete WebAuthn conformance, usability in a live workforce, or resistance to all relevant attacks. The principal value of the study is therefore the integrated prototype and its clarified architecture, together with empirical attempt-level evidence that can guide a more rigorous organizational validation phase.

Recommendations

A live organizational pilot should be conducted before deployment. The pilot should use actual platform or roaming WebAuthn authenticators, measure enrollment success, authentication latency, user completion rates, fallback use, and support burden, and compare the new workflow directly with the organization's existing password and MFA mechanisms. Security validation should include penetration testing and explicit adversarial scenarios: phishing and origin confusion, replay, session/token theft, credential stuffing, compromised endpoints, authorization bypass, database compromise, and secret-management failures. Fingerprint or facial deployments should additionally undergo presentation-attack testing and liveness/PAD evaluation consistent with applicable biometric standards. Biometric evaluation should be repeated with a pre-specified protocol that records the number of unique users or fingers, samples per subject, genuine and impostor comparison generation, sensor conditions, threshold selection, score distributions, confidence intervals, and demographic performance where relevant. The underlying scores should be retained so that ROC/DET curves and EER can be reproduced independently.

Future work should include formal user-based usability testing rather than inferring usability from FRR. Validated instruments such as the System Usability Scale or comparable task-based measures can be combined with completion time, error recovery, satisfaction, accessibility, and help-desk indicators. Scalability and concurrency testing should also be performed against realistic enterprise loads.

Production architecture should prefer standards-conformant WebAuthn/FIDO2 with authenticator-local biometric verification so that biometric samples are not transmitted to the relying party. Where central biometric matching is operationally necessary, organizations should conduct a privacy impact assessment and implement strong template protection, managed encryption keys, least-privilege access, authenticated protected channels, logging, revocation, retention limits, and incident-response procedures.

Acknowledgement
I thank Dr. Nelson Masese and Dr. Ruth Oginga of Kabarak University for their guidance and constructive feedback throughout the research. I also thank Kabarak University, the participating KURA employees, family members, and friends for their support.

Authorship Statement
Pravine Otara contributed to conceptualization, methodology, investigation, formal analysis, data curation, and writing of the original draft. Dr. Nelson Masese and Dr. Ruth Oginga contributed to supervision, validation, scholarly guidance, and writing - review and editing. All authors reviewed and approved the final manuscript.

Funding
This research received no external funding.

Declaration of Competing Interests
The authors declare that they have no competing interests.

Research Approval
Ethical approval for the study was obtained from Kabarak University Scientific and Ethics Review Committee, under approval number KUREC-260925. Research authorization was granted by National Commission for Science, Technology and Innovation, which issued research license number NACOSTI/P/25/4180448. All necessary institutional and regulatory approvals were obtained before commencement of the study. Informed consent was obtained from all study participants before their participation in the research.

Licensing Statement
© 2026 The Author(s). This article is published by *Kabarak Journal of Research & Innovation (KJRI)* under the **Creative Commons Attribution 4.0 International (CC BY 4.0) License**, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Alrawili, R., Alqahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Computers & Electrical Engineering, 119*, Article 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

Baum, C., Frederiksen, T. K., Hesse, J., Lehmann, A., & Yanai, A. (2020). PESTO: Proactively secure distributed single sign-on, or how to trust a hacked server. In 2020 IEEE European Symposium on Security and Privacy (pp. 587–606). IEEE. https://doi.org/10.1109/EuroSP48549.2020.00044

Bianchi, G., & Valeriani, L. (2023). Time is on my side: Forward-replay attacks to TOTP authentication. In Security and privacy in social networks and big data (pp. 109–126). Springer. https://doi.org/10.1007/978-981-99-5177-2_7

Cappelli, R., Maio, D., Maltoni, D., Wayman, J. L., & Jain, A. K. (2006). Performance evaluation of fingerprint verification systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(1), 3–18. https://doi.org/10.1109/TPAMI.2006.20

Carroll, A., & Latifi, S. (2025). Comparative analysis of passkeys (FIDO2 authentication) on Android and iOS for GDPR compliance in biometric data protection. Electronics, 14(20), 4018. https://doi.org/10.3390/electronics14204018

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

FIDO Alliance. (n.d.). User authentication specifications overview. https://fidoalliance.org/specifications/download/

Frederiksen, T. K., Hesse, J., Poettering, B., & Towa, P. (2023). Attribute-based single sign-on: Secure, private, and efficient. Cryptology ePrint Archive. https://eprint.iacr.org/2023/915

He, S., Lei, Y., Zhang, Z., Sun, Y., Li, S., Zhang, C., & Ye, J. (2025). Identity deepfake threats to biometric authentication systems: Public and expert perspectives. arXiv. https://arxiv.org/abs/2506.06825

Hussaini, B. (2024). Risks and challenges associated with biometric authentication systems (Bachelor's thesis, Jönköping University). Jönköping University. https://hj.divaportal.org/smash/get/diva2:1901989/FULLTEXT01.pdf

Jain, A. K., Deb, D., & Engelsma, J. J. (2022). Biometrics: Trust but verify. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(3), 303–323. https://doi.org/10.1109/TBIOM.2021.3115465

Kindervag, J. (2012). Build security into your network's DNA: The Zero Trust Network Architecture. Forrester Research. https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

Mahdad, A. T., Jubur, M., & Saxena, N. (2021). Analyzing the security of OTP 2FA in the face of malicious terminals. In Information and communications security (pp. 97–115). Springer. https://doi.org/10.1007/978-3-030-86890-1_6

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2004). FVC2004: Third fingerprint verification competition. In Biometric authentication (pp. 1–7). Springer. https://doi.org/10.1007/978-3-540-25948-0_1

Morake, A., Khoza, L. T., & Bokaba, T. (2021). Biometric technology in banking institutions: The customers' perspectives. South African Journal of Information Management, 23(1), Article a1407. https://doi.org/10.4102/sajim.v23i1.1407

Morkonda, S. G., Chiasson, S., & van Oorschot, P. C. (2024). Influences of displaying permission-related information on web single sign-on login decisions. Computers & Security, 139, 103666. https://doi.org/10.1016/j.cose.2023.103666

National Institute of Standards and Technology. (2023). Advanced Encryption Standard (AES) (FIPS 197, updated). https://doi.org/10.6028/NIST.FIPS.197-upd1

National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4). https://doi.org/10.6028/NIST.SP.800-63B-4

Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). A systematic survey of multi-factor authentication for cloud infrastructure. Future Internet, 15(4), 146. https://doi.org/10.3390/fi15040146

Ozkan, C., & Bicakci, K. (2020, December). Security analysis of mobile authenticator applications. In 2020 International Conference on Information Security and Cryptology (ISCTURKEY) (pp. 18–30). IEEE. https://doi.org/10.1109/ISCTURKEY51113.2020.9308020

Shibayama, R., & Kikuchi, H. (2021). Vulnerability exploiting SMS push notifications. In 2021 16th Asia Joint Conference on Information Security (pp. 23–30). IEEE. https://doi.org/10.1109/AsiaJCIS53848.2021.00014

Singh, A. P., Kuzminykh, I., & Ghita, B. (2024). Industry perception of security challenges with identity access management solutions. In 2024 IEEE International Black Sea Conference on Communications and Networking (pp. 312–315). IEEE. https://doi.org/10.1109/BlackSeaCom61746.2024.10646296

Slamet, C., Syaripudin, U., Kaffah, F.M., & Tiasto, B.E. (2021). Implementation of Rivest Cypher 4 algorithm in Security Assertion Mark-up Language protocols on Single Sign-On services. IOP Conference Series: Materials Science and Engineering, 1098. https://doi.org/10.1088/1757-899X%2F1098%2F3%2F032109

Tolbert, M. M., Hess, E. M., Nascimento, M. C., Lei, Y., & Shue, C. A. (2022, August). Exploring phone-based authentication vulnerabilities in single sign-on systems. In International Conference on Information and Communications Security (pp. 184–200). Springer. https://doi.org/10.1007/978-3-031-15777-6_11

Westers, M., Wich, T., Jannett, L., Mladenov, V., Mainka, C., & Mayer, A. (2023). SSO-Monitor: Fully automatic large-scale landscape, security, and privacy analyses of single sign-on in the wild. arXiv. https://doi.org/10.48550/arXiv.2302.01024

World Wide Web Consortium. (2026). Web authentication: An API for accessing public key credentials, Level 3. W3C Recommendation. https://www.w3.org/TR/webauthn/

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for Internet-of-Things security: A review. Sensors, 21(18), 6163. https://doi.org/10.3390/s21186163