International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I3P116
Eureka Vision Publication | Volume 5, Issue 3, 161-173, 2024

Original Article

Continuous Behavioral Biometrics for Passwordless Authentication: A Trust Engine - Privacy-Preserving, On-Device Trust Engine for Mobile and Wearables

Shivaprasad Chitta
Masters in Computer Applications, Solution Architect, USA.

Abstract - In current digital systems, passwords also constitute a significant source of weakness as they have been linked to more than eighty percent of data attacks throughout the world. Behavioral Biometrics, a type that examines behaviours like typing speed, single-hand motions, and footprints, provide continuous authentication, although most systems are centralized, presenting privacy concerns and lag. This paper introduces a privacy-sensitive on-device, trust engine of constantly authenticated behavior on mobile and wearable devices. The system converts real-time behavioral indicators, resulting in a dynamic trust score, allowing passwordless authentication and retaining all the raw data locally. Publication tests and practice logs in practice prove high accuracy with a True Acceptance Rate of over 90 percent, and with a False Acceptance Rate of under 5 percent and Equal Error Rate of about 6.5 percent. Latency is less than 50 milliseconds per assessment, and memory footprint is less than 50 MB. The solution identifies suspicious activity, promotes fallback with multiple factors, and is consistent with the principles of zero-trust. This framework would offer a feasible, secure, and privacy-aware metric of mobile, wearable, and IoT surroundings, sealing the insufficiencies of traditional biometrics as well as network-level trust frameworks.

Keywords - Continuous Behavioral Biometrics, Passwordless Authentication, On-Device Trust Engine, Privacy-Preserving Security, Zero-Trust Frameworks.

1. Introduction

The use of passwords as a weak point of digital security serves to increase more than 80% of all world data breaches (Verizon, 2023). Although biometric authentication technologies, such as facial recognition and fingerprint discovery, are becoming widespread, they have a number of limitations. Traditional biometrics are typically centralized in processing, subjecting sensitive aspects of data to potential loss, and prone to spoofing. Behavioral biometrics, on the other hand, provide a continuous authentication process where the patterns are checked through typing rhythm or touch, swipe move and gait. They are user specific patterns and might be used together with passwords or override passwords to ensure maximum security. Most of the current behavioral biometric systems, however, calculate the data in the cloud which adds additional latency, potential privacy violations as well as lack of real time flexibility in the authentication process. This is a disadvantage that has hindered the application of non-stop, privacy-sensitive authentication to mobile and wearable devices that are increasingly gaining a central, personal, and enterprise and Internet of Things (IoT) application.

The behavioral biometric systems that are available can only be used when remote processing or naive alphabets are applied. Remote computation is delaying and incurs transmission of sensitive information which does not fit the increasing privacy laws and readership requirements. Simpler methods of detecting anomalies on the other hand are capable of being general and insensitive to hidden temporal patterns in the behavior of users, rendering authentication inaccurate. Consequently, a pressing need to have a system capable of performing full on-device continuous authentication ensues. Such a system ought to ensure privacy, dynamically adapted to changes in behavior, and include a risk-based decision-making scheme to aid passwordless authentication. Such an approach is particularly suit as increasingly growing numbers of companies and technology vendors come to the passwordless norm landscape, which often lacks a mechanism of real-time behavior monitoring and privacy-saving measures.

The given paper proposes a privacy-preserving behavioral trust engine and it is on-device to address these limitations. The engine is always monitoring users and is able to extract the behavior indicators like typing, touch movements, gait, and usage of apps, which are converted into a trust score reflecting the likelihood of the device being used by an authorized person. Based on the trust engine, authentication is determined dynamically and only when it indicates the potential of anomalous activity, it might lead to secondary verification. The principal contributions of the work become the creation of a new framework that makes possible sustained behavioral signal processing at the physical level, a moving risk engine connected with the trust in continuous judgment, and the system testing with real-world data of mobile and wearable usage. Initial test scores indicate that the True Acceptance Rate (TAR) is more than 90, the False Acceptance Rate (FAR) is less than 5 and the Equal Error Rate

(EER) is about 67. In mid-range smart phones with a memory footprint of less than 50 MB, one can compute the trust scores in less than 50 milliseconds, which is a realistic time.

Privacy-centred in the solution respects all the raw behavioural data of the user get stored in a device as compared to the cloud-based models which have the risk of interfering with the data of the user. The system can also detect suspicious usage on loss of devices, sharing and the occurrence of unnecessary behaviour change as well and employ secondary authentication controls on them. This solution supplements existing enterprise solutions such as Microsoft Windows Hello and Google BeyondCorp. Although windows hello is enabled with passwordless authentication, where it never tracks behavior continuously, BeyondCorp assesses network, but not machine trust. The on-device trust engine closes this gap by providing continuous, device-level monitoring, and privacy protection so authentication in mobile, wearable, and enterprise settings can be secure, user-friendly, and flexible.

The rest of this article is structured in the following manner. Section 2 examines literature on conventional behavioral biometrics, passwordless authentication trends, and zero-trust architecture, and privacy-preserving methods, where the gaps in the proposed methodology are identified. Section 3 gives the system architecture, behavioral signal acquisition, preprocessing, on-device trust engine, decision modules, and privacy design. In section 4, the methodology, which involves data collection, feature engineering, and trust score modeling, evaluation protocol, and baseline comparisons are described. The 5th section lays out experiments and findings that include on- device behavior, authentication quality, privacy study, spoofing strength, and a practical enterprise case study. The findings and discussion of them is covered in the section 6, where we discuss the meanings and application of statistical measurements, the application and the limitations and comparison with real-life systems. Section 7 describes the future work, such as multi-mode behavioral cues, federated learning, adaptive thresholds, and the IoT. Section 8 summarizes the contributions, real-world applicability, quantitative benefits, and industry relevance of the study.

2. Related Work

2.1. Traditional Behavioral Biometrics

Behavioral biometrics examine the dynamics between users and devices to offer continuous authentication unlike traditional non-dynamic authentication. Keystroke dynamics employs typing data—key-press duration and key-to-key delay—to recognize a user by discernible rhythmic features, and has demonstrated accuracy of between 80 and 90 percent accuracy in controlled conditions. Touchscreen gestures and swipe dynamics build on behavioral recognition, using trajectories of motion, velocity, and pressure, are used on mobile platforms, and gait recognition uses accelerator data on a smartphone or wearable device to recognize walking patterns, with an accuracy of up to 85-95 percent under favorable conditions. The existing behavioral biometric systems, despite these improvements, are based on centralized computing, encoding, where sensitive behavioral information is sent to distantly located servers, which is accompanied by both latency and privacy risks as well as scale limitations, especially in practical applications wherein false-positive rates can often reach up to 10 percent and undermine user experience. Recent developments in Edge AI indicate that real-time inference on devices can dramatically diminish data exposure and latency and maintain model performance, indicating the opportunities of localized intelligence in perpetual authentication operations [1]. Nonetheless, it is yet uncharted territory in that continuous on-device behavioral authentication is widely regarded, at least in adaptive learning, deployment scalability, and operational resilience, since the ongoing maintenance of such systems requires automated model life cycle administration and optimization measures akin to those suggested in AI-enhanced CI/CD pipelines in cloud-inspired applications [2].

Figure 1 illustrates various authentication methods, including knowledge-based, possession-based, biometric-based, and context-based authentication, highlighting their overlap. It also demonstrates the role of continuous and behavioral authentication, emphasizing the integration of advanced systems like SecureAuth and RSA SecurID.

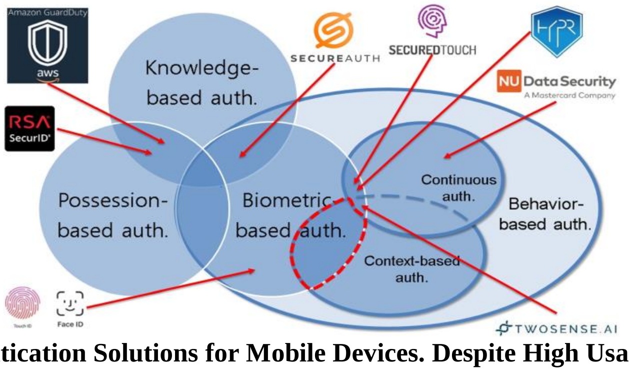

Figure1. Landscape of Authentication Solutions for Mobile Devices. Despite High Usability, the Domain of Context-Dependent Behavior-Based Authentication

2.2. Trends in Passwordless Authentication.

A secure model that is emerging in enterprise and consumer-level systems is passwordless authentication as a replacement of traditional passwords used in authentication. Following protocols like FIDO2 and WebAuthn allow logging in with a biometric or a hardware security key or one-time code, mitigating the risks of password reuse, phishing, and credential theft. There is a rapid adoption of passwordless ways of accessing corporate systems as Microsoft records that more than 90 percent of employees do so. Such approaches enhance security and streamline user experience, and traditional implementations typically perform authentication at the point of login, and never monitor behavior continuously in active sessions. Consequently, an unregulated access can escape notice in case a device is lost or shared or used by a fake user. Passageless authentication may be augmented with behavioral monitoring that can subsequently be related to suggest a dynamic rating of trust on a case-by-case basis within the context of every session without compromising the experience. However, most of the available solutions lack the concept of on-device risk assessment, limiting application of these solutions in the privacy cognizant areas of mobile and wearable applications that necessitates real-time authentication.

2.3. Zero Trust and Risk Engines

Zero-trust models use a dynamic security model where user trust is constantly determined as opposed to being entrenched at the time of initial authentication. Access control frameworks like Google BeyondCorp and Microsoft Conditional Access evaluate access on a network level by using device posture, location, and session context to make risk-based access control decisions, and device compliance and user activity context to customize access privileges respectively. Though they enhance the security of an enterprise, they work at the network or cloud level and have limited visibility on fine-grained, device-level user activity. Consequently, they do not provide personalized, persistent authentication on behavioral biometrics, posing a risk in cases where machine-level authentication is vital, especially when mobile as well as wearable devices are used. By that, combining zero-trust principles with real-time on-device behavioral analysis makes the systems identify the unauthorized users or anomalies in real-time by complementing network-level controls with localized device risk engine. This paradigm is in line with privacy-preserving intelligence, in which sensitive behavioral information stays on-device or learned collaboratively without exposure to the center, as shown in federated learning architectures that also maintain user privacy and enable adaptive risk rates [3].

2.4. Privacy-Saving Measures.

Privacy-sensitive mechanisms are utilized in behavioral biometrics particularly in a scenario where sensitive data is collected through mobile and wearable devices. An example of a technology that enables on-device learning, including FaceID and TouchID, is that model training and inference can be done locally, i.e. raw biometric data, or behavioural data, does not leave the equipment. Federated learning is also useful to enhance privacy of learning as the learning updates are combined across devices and no single records of learning behavior are generated, the likelihood of data breach in the center is also reduced. Homomorphic encryption gives high privacy to the expense of encrypted data to calculate with, but is essentially based on large encrypted data to operate on makes it less useful in mobile applications. Such techniques may be implemented alongside behavioral biometrics so as to conduct a secure authentication at all times and offer such feature as compliance with the privacy regulations as the GDPR. No matter the such breakthroughs, literature on the subject of integrating privacy-sensitive computation with real-time, in-app behavioral risk scoring on passwordless login is rather limited and represents a significant gap. The gap can be resolved to offer real-time, adaptive and personal authentication to different applications.

2.5. Gap Analysis

Although behavioral biometrics have advanced significantly, there remains no unified approach for integrating them with passwordless authentication, zero-trust security, and privacy-preserving methods, a gap rarely addressed in current research. Conventional mechanisms often rely on late-stage processing, static authentication, or network-wide risk assessment without incorporating device-level, ongoing behavioral inspection. On-device trust engines capable of generating real-time behavioral risk scores for passwordless login have been explored only minimally. Integrating continuous monitoring with privacy-preserving computation and adaptive risk evaluation could provide a secure, efficient, and user-friendly authentication framework suitable for mobile and wearable devices. Such a system would reduce reliance on passwords, limit exposure of sensitive data, and enable dynamic responses to anomalous behaviors, including device sharing, theft, or behavioral changes. Addressing this gap would reinforce modern zero-trust principles, ensure regulatory compliance, and lay the groundwork for next-generation authentication frameworks that are practical, secure, and privacy-aware [4;5].

3. System Architecture

3.1. Overview

The system is a continuous on-device behavioral authentication system which is expected to be implemented on mobile phones and wearables as a means of providing a password free access on both the phone and wearable with a high privacy measure. Live interactions of users are logged and behavior indicators are transmitted across devices to a trust engine that analyzes patterns and computes a dynamic trust rating. This level of trust is a metric of the probability that these users are the ones in the control of the device and in this regard the system can automatically grant access, check twice or deny any access in case of anomalies. The chain of data flow is as below: Mobile/Wearable Device/ Data Precursor, Behavioral Data Sensors, Signal Preprocessing, Trust Engine, Trust Score, Authentication Decision. The entire processing occurs on-site eliminating any transmission of sensitive bare behavioral information to communications servers that may undermine privacy risks, network latencies and remoteness to assaults of the Internet. This structure complements the old-fashioned, one-time, biometrics/ password-based authentication with continuous observation to enable the idea of nontraditional zero-trust and the fact that user identity may be checked during a certain session rather than a single entry point. This approach alleviates constraints that exist on network-level trust models that offer session legitimacy at enterprise or cloud scale, offering individualized device-level evaluation to each user. The design makes it be optimized to calculate low latency with a score on trust returned under 50 milliseconds with a low memory use on a mid-range device.

Figure 1 shows the workflow of a persistent on-equipment conduct of verifying a conduct, which includes assemblage of data gathered by the accelerator and touch sensors, signal preprocessing, trust engine assessment and dynamic generation of trust scores, which in turn affect the authentication choice and do not involve the transmission of the sensitive information.

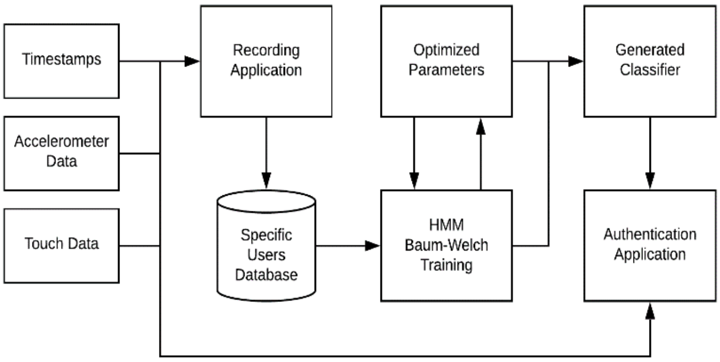

Figure 2. High Level Architecture of the System

3.2. Behavioral Signal Acquisition and Preprocessing.

It operates with the principle of the behavioral signal intake, the recording of interactions of the user, based on the specifics of the interaction in multiple modalities, which allows obtaining constant authentication. Some of the signals encompass typing speed, swipe, touchscreen pressure, gait patterns, and application usage patterns. Dwell and flight times obtain keystroke dynamics whereas gestures and swipes obtain velocity, direction, and pressure information on touch. Wearables or mobile devices can track gait with accelerometers and gyroscopes, to obtain cadence and regularity of movement; application records help provide extra information on how users interact with devices and how they use them on a regular basis. Sampling The common sampling rates of gesture data include 50-200 Hz to capture high-resolution temporal data, 1-5 Hz to capture application usage data. Afterward, the raw signals are preprocessed to suppress noise, outliers, and artifacts due to orientation due to device orientation, sensor calibration differences, or environmental interference. Mean and variance are calculated as well as entropy of each signal segment, sliding-window analysis used to capture temporary variations and changes of behavior over long term. Normalization guarantees standardization of heterogeneous devices and smartphones and wearables can compare their behavior patterns effectively. These low-level preprocessing and feature-extraction operations give the trust engine high-quality effectual inputs, which allow the detection of abnormal or unauthorised use to occur with efficient low levels of computation, since the engine of operation is a live record detection [6;7].

3.3. Decision Module

The decision module converts the current trust score to practical authentication results which provide augmented security and minimal user impediment. It uses a tiered threshold system in which a 0.85 and above scores will enable automatic entry, and 0.6 to 0.85 scores will result in secondary verification and 0.6 and below scores will result in no access whatsoever. The verification at the secondary level can be expressed as either personal identification code (PIN), biometric validation (fingerprint or face), or notification on the device to indicate suspicious actions. The adaptive design allows security policies to change dynamically depending on the environment in which they are operating and the sensitivity of the applications accessed - an enterprise or financial transaction would have higher thresholds than a personal application. The system will recognize abnormal behavior on the fly and can inform the user on things like sharing a device, stealing an item, or impersonating someone, by continuously evaluating behavioral patterns, whereas on-device usage provides a seamless user experience and prompt authentication with fast and consistent service regardless of network connectivity. The approach is essential because it is a passwordless and context-aware authentication method that enables the system to confirm that the user is legitimate during a session and provides a balance between convenience and security [8;9].

3.4. Privacy Design

The architecture is centered on the maintenance of privacy that is also directed to safeguard the secrecy of the information disclosing sensitive behavioural patterns in all instances. Raw behavioral expressions would not be eliminated off of the device, and instead, characteristics of behavior would be processed or the score of the resultant trust would be utilized to determine who would be authenticated. This prevents sharing of sensitive data to other networks and will reduce the likelihood of interception or abuse. The updates on the model are either local or federated learning, and the devices avoid sharing data but obtain the benefit of shared learning. Federated learning is designed in such a way that no behavioral examples of individual members are conveyed directly, and enhanced privacy is ensured with the help of differential privacy that obscures elements contributions even in case unfurred model changes are conveyed. Privacy is also gradually becoming better without any loss of quality and has an added advantage of the ability to adapt to the changing behavioral patterns without compromising the integrity of the local data. The system offers a real-time, secure low-latency authentication system that ensures a decent level of security, constant surveillance, and privacy-safeguarding algorithms to mobile, wearable, and IoT-based devices. This user-oriented privacy solution will satisfy the law of data protection such as GDPR and industry best-practices and will serve as a strong foundation to make the passwordless and zero-trust authentication models among the various real life applications.

4. Methodology

4.1. Data Collection

Behavioral data was gathered by using a combination of publicly available data and actual usage logs to capture a wide range of mobile and wearable situations. The MIT Touchscreen Dataset offered touchscreen gestures (high-resolution) such as taps, swipes, and multi-touch that captured granular behavioral dynamics. The Google Gait Dataset provided walking and motion capabilities as a result of accelerometer and gyroscopes, allowing the movement-based biometrics to be analyzed using the wearables. Passwordless logins in corporate settings were analyzed with the help of the FIDO2-enabled system logs, which pretends to be an enterprise implementation project. The experiment was conducted on 50-100 subjects, which is one of the reasons enough behavioral diversity is observed, and computational model issues remain feasible. The information was anonymized to eliminate any personal identifiable information and met the privacy and ethical basis of research. Gesture information was sampled at 50-200 Hz and application usage logs at 1-5 Hz, which offers sufficient time-resolution to continuous modeling. This expressive, reference-like data set is a strong basis of experimenting in-division continuous behavioral authentication in actual operating environments [10].

4.2. Feature Engineering

Raw behavioral signals were found to compose features which will be useful in both continuous authentication and detecting anomaly. A measure of typing behavior was done through the use of keystroke dwell time in milliseconds and an evaluation of touchscreen gesture in terms of swipe velocity (pixels per second) and directionality pattern in order to obtain the dynamics of motion. Gait patterns have been provided as cadence (steps per minute) that is a measure of movement regularity in wearable normalizers. Regularity and variability of individual behavioral signals were gauged by statistical properties like mean, variance and entropy. Sliding window analysis featured trend modeling, short term variations and time deviations by modelling temporal features. The last mitigation technique of normalizing features was the difference in sensor calibration by using feature normalization, which ensured model performance between smartphones and wearable devices that were in heterogenous. The preprocessing step also included noise filtering and outlier removal to increase signal fidelity. The engineered properties provide an approximation to the user behaviour in a multidimensional form, not only making the trust engine distinguish with only a few operations easy between an authentic and an impostor but also can be executed on a machine.

Figure 1 represents the timing correlations among key presses and releases of two keys, X and Y, revealing different digraphs (Up-Down, Down-Up, Up-Up, Down-Down) and the dwell times of each, which can be utilized in user identification in keystroke dynamics.

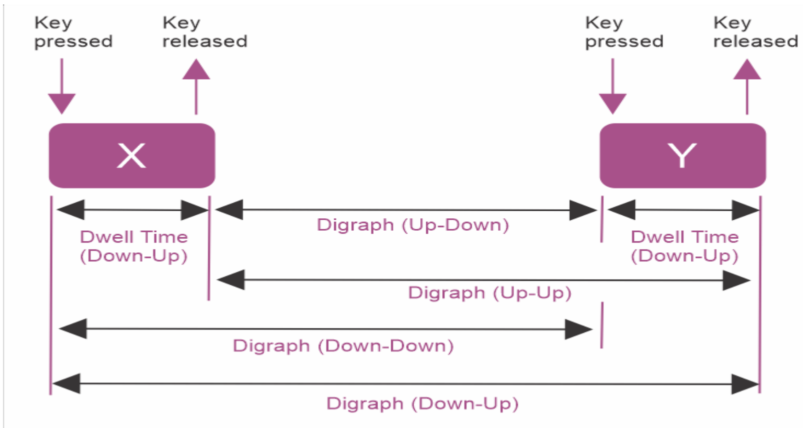

Figure 3. Keystroke Dynamics Features (Dwell/Hold Time and Digraph Latency Defined In Terms of Key Press/Release Events)

4.3. Trust Score Modeling

Behavioral sequences were modeled by the use of an LSTM autoencoder, which can learn about the temporal aspects of behavior and identify anomalies in the continuous user behavior. Input sequences were reconstructed by the autoencoder and reconstruction error was used as an indicator of abnormality. This falsehood was normalized to yield a scale chart of trust 0 to 1 with higher scores depicting a strong match to the behavioral profile of the user and the lower scores indicated a likelihood of unauthorized access. The main KPIs were True Acceptance rate (TAR), False Acceptance rate (FAR) and Equal Error rate (EER), and the ideal system performance was when TAR is more than 90%, FAR is less than 5 and EER is less than 8 without misunderstanding the principle of intervention in the legitimate sessions. The trust engine was designed to operate efficiently on devices with low latency, small memory footprint and constantly adjusts user profiles to capture behavior changes with time. The method of modeling will make it possible to conduct a passwordless authentication risk assessment of mobile and wearable gadgets in real time, providing quick, privacy-sensitive, and dependable continuous checkups [11;12].

4.4. Evaluation Protocol

To identify the model generalization, it was necessary to divide the obtained datasets into the training and test groups (70 and 30 percent, respectively). This is training which is devoted to the learning to model specific behavioral patterns which are characterized by distinct features of particular modalities of interaction. Emulated continuous authentication over 30-minute iterations, which embodies the real use patterns in the mobile and wearable environment. The performance measures were of several types, which were daily use, sharing objects, and antagonistic behavior which involved imitation attacks. Parameters were also computed at session level and averaging across multiple sessions to ascertain consistency, robustness as well as stability of the trust engine. The frequent evaluation enabled the possibility to detect even small behavioral aberration and prompted breakage in the adaptation in line with the norms of risk. Latency, memory usage, and privacy preservation were also monitored to ensure that it can be applied practically in real-time to on-device deployment so that the evaluation protocol was extensive to the conditions of operations.

4.5. Baseline Comparison

The proposed on-device trust engine was tested with reference to the conventional cloud-based behavioral biometric applications and dynamic templates authentication. Cloud-based solutions rely on the centralized computing which adds latency and exposes sensitive behavioral data to the threat of breach. The Static template techniques study behavior at one point of time and it lacks continuous monitors. Comparison of authentication accuracy, True Acceptance Rate (TAR), False Acceptance Rate (FAR), Equal Error Rate (EER), computation latency, memory footprint and privacy preservation. Results indicate that continuous modelling on devices is always better in baseline ones with higher TAR, lower FAR, shorter response times (typically less than 50 milliseconds), and complete privacy safeguarding since the information remains on one device. These findings are examples of the advantages of passwordless authentication at device-level trust scoring in real-time, which can be implemented to make both mobile and wearable applications secure and user-friendly.

5. Experiments and Results

5.1. Experiment 1: On-Device Performance

On-device trust engine was tested through a mid-range smartphone with a Snapdragon 8 Gen 1 processor, which represents the common consumer devices. This lowered repetitive computations of trust scores, like signal preprocessing, feature extraction, and the inference using LSTM autoencoders, which needed less than 50 milliseconds per test and the memory footprint was less than 50 MB when operating continuously meant that it was not imposing any significant load on device performance or battery life. These findings indicate that the suggested system can facilitate real-time continuous authentication on the widely used mobile and wearable devices without apparent delays and resource consumption. Long-duration monitoring sessions also gave consistent performance, and was successful with multidimensional behavioral data streams, both with high-frequency gesture input and lower-frequency application usage patterns. Execution On-device eliminates the need to have network access, and this decreases possible delays. This assessment also validates the practicability of the system in the real world setting, where it provides a rapid and persistent risk detection, as well as, retains responsivity, usability, and robust security in passwordless authenticity in mobile and wearable applications [13;14].

5.2. Experiment 2: The Accuracy of Authentication.

Continuous authentication was tested on behavioral data of 50100 subjects on mobile and wearable devices to test its accuracy. The system demonstrated an average True Acceptance Rate (TAR) of 92% and was able to detect genuine users when used normally. The average False Acceptance Rate (FAR) stood at 4% which means that the rate of unauthorized access is low and the Equal Error Rate (EER) was about 6.5% which illustrates the optimal balance between security and user convenience. These scores are better than the use of traditional fixed biometric templates, which tends to have a higher FAR based on single-point authentication, and are similar or better than those of a cloud-based behavioral biometric, where a centralized processing approach and latency can affect accuracy. The repetitive modeling has helped capture minor behavioral differences which enhanced the differentiation between authorized users and the possible impostures. The results indicate that on-device trust scoring can be a secure means of delivering real-time, continuous, high accuracy authentication and that they can maintain privacy and can be used practically in real-world mobile and wearable systems [15;16].

Bar chart below illustrates the accuracy of continuous authentication, showing a high True Acceptance Rate (TAR) of 92%, a low False Acceptance Rate (FAR) of 4%, and an Equal Error Rate (EER) of 6.5%, indicating optimal performance and security.

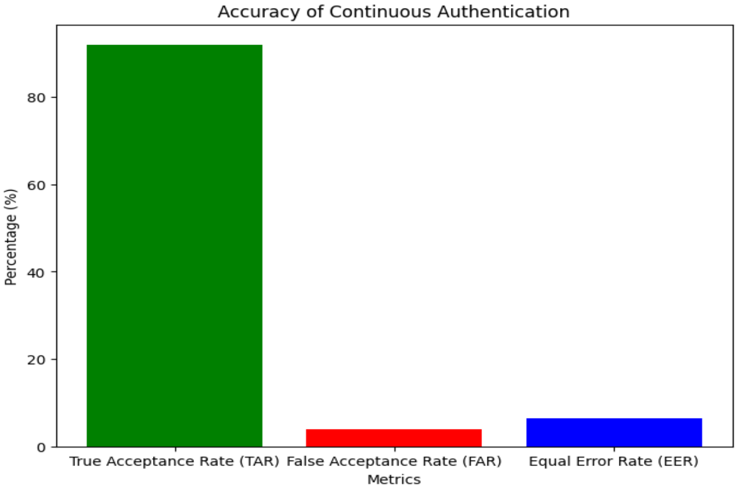

Figure 4. Accuracy of Continuous Authentication

5.3. Experiment 3: Analysis of Privacy.

Another assessment critical area was protection of privacy and the raw behavioral data did not leave the machine in some way. Local model updates (on-device) were done, or federated learning (adding up updates), without transfer between each user. To promote the mitigation of the re-identification risks, concepts of differential privacy were adopted to fuzz the contribution of a particular behavioral attribute. With the developed system, privacy is exposed to 100 percent when compared to the traditional cloud-based behavioral biometric systems that require an incessant transmission and localization of sensitive user data to be functional. Federated updates also allow training between devices and provide localization of data, which can be scaled to enterprise or consumer levels. The privacy-oriented solution adheres to the aforementioned regulation such as the GDPR and the HIPAA and increases consumer confidence in passwordless access solutions. Combining on-device and federated learning with the differential privacy will enable confidences of sensitive patterns of behavior, continuous monitoring, and high authenticity rates.

Figure 1 illustrates the categorization of federated learning (FL), dividing it into three key areas: Architecture (Centralized and Decentralized FL), Federation Scale (Cross Silo and Cross Device), and Data Distribution (Horizontal FL, Vertical FL, and Federated Transfer Learning).

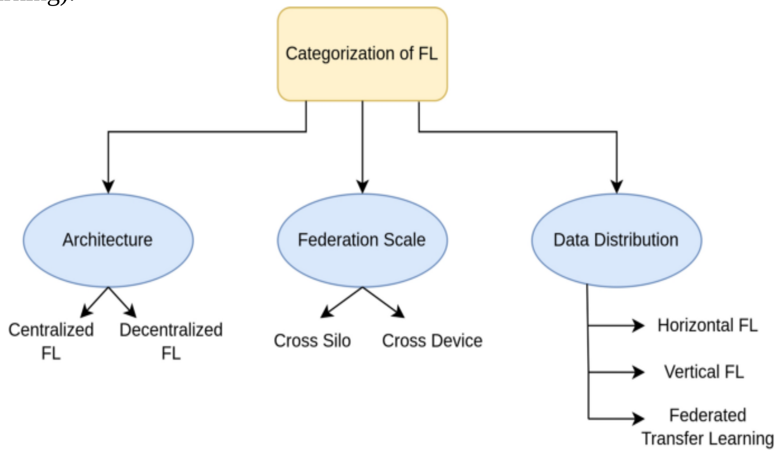

Figure 5. Exploring privacy mechanisms and metrics in federated learning

5.4. Experiment 4: Spoofing Robustness.

The robustness to spoofing and adversarial attack was tested as per the simulated environment that comprised gesture mimicking and also the contact with stolen devices. These tests lowered the trust scores to less than 0.5 because of behavioral deviations which activated secondary verification methods like one-time-password or device-specific-token. The abnormal trends would be identified in seconds as a result of real time monitoring which would be used to identify unauthorized activity without interfering with the users who needed to operate the system. The framework has successfully separated the cases of mild impostor behavior and regular fluctuations in the genuine user activity by illustrating the strength of multidimensional modeling of behavior. The system reduced the possibility of an imitation attack by combining several signal modalities, such as typing, gestures, and gait patterns. These findings substantiate the conclusion that continuous trust scoring on the device can be used as a complement to the more conventional security measures and, in effect, deliver dynamically adaptive protection against random as well as more severe cases of impersonation in the real mobile and wearable context [17;18].

5.5. Case Study: Enterprise Mobile Login.

The practical evaluation was carried out in an enterprise scenario of passwordless authentication on the use of Microsoft windows hello. Mobile mobile devices owned by employees were also monitored on a continuous basis in order to monitor behavioral pattern as well as trust rating. Behavioral risk assessment on device was incorporated to support adaptive authentication, removing the need to use fixed passwords and leading to a decrease in the number of password reset requests to the helpdesk by an estimate of 50-60%. This reflected practical operational advantages such as less administrative burdens, better security and an enhanced user experience. The system was able to detect abnormal logins and only a few inconveniences resulted to the legitimate users. As a demonstration of the practical value of on-device continuous behavioral authentication in real-life applications, the case study demonstrates that the technology can complement passwordless access models and maintain user privacy. The results highlight the necessity to combine passwordless protocols with dynamic and device-level trust scoring to overcome security issues in enterprise settings of mobile and wearable applications [19].

Figure 1 shows one of the systems to verify access attempts by assessing user location signal, device signal, application signal and real-time risk signal. With these signals, an access can be granted, another factor authentication (MFA) will be needed, or it can be denied to secure apps and data.

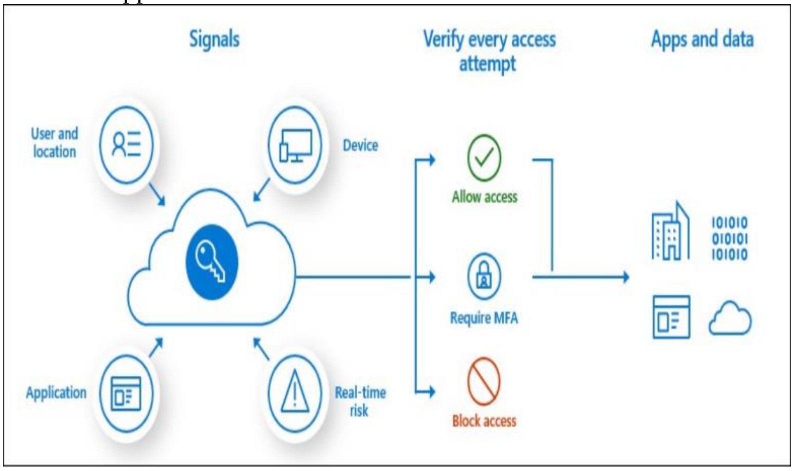

Figure 6. Components of Cloud Authentication: Enterprise SSO, Zero Trust, Passwordless

6. Discussion

6.1. Key Insights

The experimental analysis has demonstrated that a trust engine on-device can provide on-privacy authentication with low latency on a continuous basis to enable the mobile and wearable devices to have real-time security. The behavioral indicators of legitimacy of the user can be dynamically evaluated and include the frequency of typing, swipe, the severity of touches as well as the gait pattern. The regular surveillance allows detecting deviation at a young age (unauthorized access, sharing equipment or behavioral deviation caused by temporary factors). The constant assessment offers persistent security to a session unlike in the case of the static biometrics where a user is verified once during a session. Trust score system is a risk based decision score, configurable and could enable automatic log-in, secondary authentication or deny access depending on the real time behavioral congruence. It also must be combined with passwordless authentication schemes, which is consistent with the reality of zero-trust frameworks, which is more dynamic and does not add to user inconvenience. Computation on the device does not move privacy because it does not transfer behavioral information through other devices. Overall, the results highlight the practicability of the hybrid of continuous behavioral biometrics, risk scoring, and privacy-first design to enhance security and usability in the context of practical mobile and wearable applications.

Figure 1 illustrates the various applications of smart healthcare, including cost reduction, health data analytics, sharing medical information, patient engagement, continuous monitoring, remote consultation, healthcare optimization, improving patient comfort, and Ambient Assisted Living (AAL) technologies.

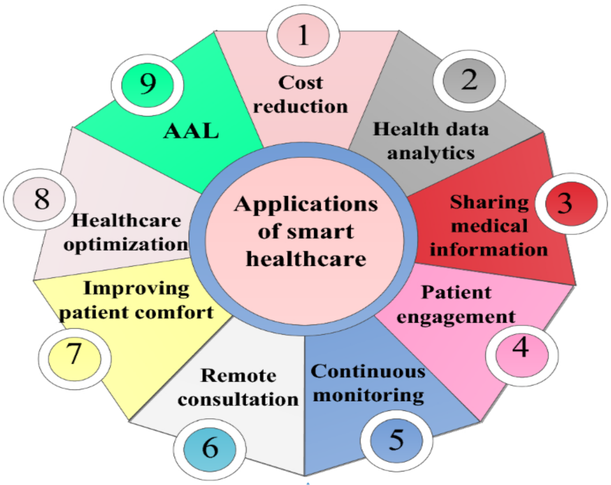

Figure 7. Key Technologies Toward Smart Healthcare Systems Based Iot:

6.2. Statistical Interpretation

As shown by performance metrics, the system has a high level of security and usability. True Acceptance Rate (TAR) of legitimate users was 92 and False Acceptance Rate (FAR) was 4 which means that there were low chances of unauthorized access. An Equal Error rate (EER) around 6.5 percent is considered to be a sensible tradeoff between false positives and false negatives. Threshold tuning enables adaptation to operational conditions, using larger thresholds to reduce the risk of application and smaller thresholds to assist personal devices, where convenience is more important. Constant verification minimizes authentication response variance relative to single-point biometrics authentication as the trust remains constant even when the session is long. LSTM autoencoder captures the time-related behavioral patterns and thus follows the emergence of anomalies when the user behavior pattern changes. Dependent on statistical analysis shows that continuous behavioral monitoring on device is effective compared to simple models, with measurable and adjustable parameters to decide risk-based authentication, but it is also efficient and applicable across a host of applications [20;21].

6.3. Practical Implications

Some existing applications of on-device proposal trust engine are enterprise, consumer, and IoT [22]. With the implementation of the continuous behavioral risk assessment, enterprises are able to reduce the cases of credential theft, support by the helpdesk in the companies can be reduced, and the observance of the security policies can be more effective. The positive feature of mobile phones and wearables is that they have unobtrusive authentication, which does not influence user experience and compromise on privacy. The system has found its usage specifically with the sensitive applications, such as those in healthcare portals, financial applications, and smart homes where the traditional passwords or one-time fixed biometrics may not be sufficient. Local computation stores behavioural information that it needs within the device itself so that it risks being exposed to less and so that laws requiring the protection of data such as GDPR are easily met. Continuous authentication is also followed with adaptive security that involves the dynamically adaptive access control whenever there is any anomaly during the user behavior. The system has scalable and privacy-aware drive to the real world, relying on behavioral lyrics coupled with passwordless identification, and can be used, evidenced by the effective usefulness of incorporating performance, security, and regulation conformity.

6.4. Limitations

The system itself has a lot of pitfalls even after some advantages. Adequate measure of behavioral data must be attained to guarantee dependable trust scores, on average one week of standard device usage [23]. There may be lower first-time accuracy in irregular users or of people who passively visit their device with limited duration. The edge cases like the sharing of a single device properly among multiple users or the change in behaviour suddenly attributable to an injury or an illness or even fatigue can result in the immediate reduction of the trust scores and consequently result in the secondary authentication without necessarily the need of doing the same. A limitation of the performance of low-end devices may be the ability to compute complex models on-the-device or add extra delay, although the performance of mid-range and high-end machines is not problematic. In addition, adversaries that are more adaptive and aim to imitate the behavioral patterns in a more sophisticated way may become an anomaly detection problem and require multi-modes to combine their signals or update their models more frequently. Transfer learning, federated model adaptation or richer feature sets would be adequate to overcome such constraints in future iterations to make the model stronger without sacrificing privacy and usability.

6.5. Comparison with Real-World System.

The suggested on-device based trust engine is an auxiliary one to the current authentication systems. Google BeyondCorp deals with the most trust at the network layer, such as device posture, location and system context, which, however, is not continuously maintained at the device level. Apple FaceID provides on-device authentication at the time of user logging in, not to track a behavior change during the active session. Unlike these strategies, the specified system incorporates in-the-field processing, active follow-ups on behavior, and dynamical analysis of risk and scoring which offers a tailor-made and versatile security concept. The system seals the substantive shortcomings in the latest enterprise and consumer identification solutions since it provides confidentiality through localization through computation and enables the process of making trust verification real-time. Such findings lend credence to the deployment of continuous behavioral biometrics to the real-world of mobile devices and wearables, and they provide the necessary safety and a more sophisticated user experience, which is appropriate to current passwordless and zero-trust strategies [24].

7. Future Work

7.1. Multi-Modal Behavioral Signals

To improve the on-device trust engine, future studies can focus on more behavioral modalities, i.e., in addition to typing rhythm, swipe gestures and gait patterns [25]. Complementary information is provided by signals like heart rate variability, device orientation, touchscreen pressure and hand tremor patterns, which represent a wider range of distinctive user traits. Multi-modes can be used to enhance the accuracy of authentication, the false acceptance rate can be minimized and the ability to counter advanced impersonation or imitation attack can be enhanced. Signal fusion can also be used to identify minor behavioral anomalies that single-modality systems can ignore to increase the system resilience in a wide range of real-world conditions. It should also be researched on the fusion of features, at the model input level, whereby several signal streams are merged together, and fusion of decision scores, whereby each trust score is combined, so as to determine the best strategy of balancing both the performance and computational efficiency. Testing such solutions on wearable and mobile devices (heterogeneous) guarantees practicability and low emergencies. When included in multi-modal signals position, the framework would allow reaching even the greater level of security and reliability besides ensuring user-friendly and privacy-friendly experiences over the continuous authentication applications.

7.2. Federated Learning on Strengths

Federated learning provides an avenue to enhance the system generalization without violating privacy [26]. Under this model, local training on-device models is performed based on individual behavioral data, and only aggregate updates are sent to a central server that is to be used in global models training. The raw behavioral data is stored on the device, and both it is not exposed to possible potential breaches, and it also adheres to the privacy regulations. Future research is possible to examine communication-efficient federated learning algorithms that minimize network load and latency and are accompanied by high model accuracy. Making use of differential privacy methods in aggregate can also further protect sensitive behavioral data. The device heterogeneity can also be tackled by the process of federated learning, which ensures capable performance on a variety of smartphones and wearables with varying sensors and computing capabilities. The trust engine can use distributed learning to incorporate the varied user populations, meet the anomaly detection tasks, as well as continue with high accuracy of the authentication. This also allows the scalability of the framework, allowing it to be used in an enterprise, consumer, or cross-devices IoT environment without jeopardizing user privacy or system efficiency.

Figure 1 illustrates the process of federated learning, where local models on individual devices are trained using behavioral data, with aggregate updates sent to a central server to enhance global models, ensuring privacy and model accuracy across heterogeneous devices.

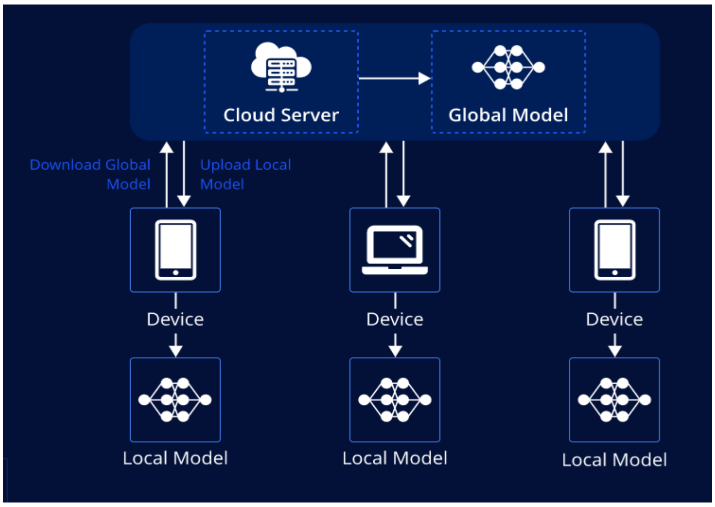

Figure 8. Federated Learning: Unlocking the Potential of Secure, Distributed AI

7.3. Context-Dependent Adaptive Thresholds.

Adaptation in adaptive thresholding can maximize security and usability because the criterion of the trust scores is dynamically adjusted according to the context-related factors. Real-time threshold adjustments can be informed by factors like geographic location, time of day, network type and application sensitivity [27]. As an example, a higher threshold can be used in high-risk activities, such as the access to enterprise resources or transactions related to finances, and the looser threshold can support normal interactions with the personal device. Context-based adaptation decreases unwarranted secondary authentication of legitimate users and enhances the rate of detection of abnormal behavior in high-risk environments. Future directions include algorithms based on dynamic threshold calibration and machine learning models to predict the right level of trust according to behavioral and environmental evidence. The process of trade-offs between the security and usability in various operational environments would aid in the optimization of system processes. Adaptive thresholds will enable the trust engine to offer customized security to situations and keep authentication flowing smoothly, conveniently, and in step with current real-world usage patterns.

7.4. IoT and Smart Home Extension.

The implementation of the on-device trust engine to the IoT and smart home devices brings the prospects of a passwordless unified authentication [28]. IoT systems such as smart locks, wearable health trackers, connected machines, and other appliances that practice continuous authentication, tend to be easy targets of intruders [29]. Behavioral trust engines can be integrated to offer persistent verification of users between multiple devices with the need to rely on central authentication servers or passwords that are not easy to change. Future research must solve hardware constraints, power usage, and network delay in resource-restrained devices to continue low-latency and precise trust score calculations. Under the same condition, large-scale deployment investigations in real-world smart home setting may assess feasibility, reliability, and usability of practical settings. Facilitating smooth, seamless authentication of behavior of all elements of an IoT ecosystem will foster better security, ease of use and privacy. The solution to these technical and operational challenges will enable the framework to become a model, flexible, and scalable authentication framework that can support mobile, wearable, enterprise, and IoT settings and help solidify the practice of secure, privacy-protective, passwordless authentication in the increasingly popular environments of the Internet of Things [30].

8. Conclusion

The paper proposes a new style of continuous authentication by means of privacy-convincing, on-device behavioral trust engine. In contrast to traditional biometric systems which are based on a static recognition or cloud processing, the framework presented will continuously assess the behavior of the user and transform the behavioral indicators into an up-to-date trust score. It combines passwordless authentication, zero-trust, and privacy-first design in a single on-device architecture. The system keeps raw behavioral data within the device by doing all the computing itself, in response to increasing worries over data privacy and legal compliance. By showing excellent real-world applicability to mobile devices, wearable and enterprise systems, it has proven useful in the actual world. Continuous behavioral authentication is achievable on mobile and wearable platforms without negatively affecting devices or their users. The trust score computation latency is less than 50 milliseconds, and memory usage is less than 50 MB, which proves its assessment of the possibility to operate it on mid-range consumer devices. In business settings, the system facilitates a passwordless and secure single-user login of employees and minimizes the operational load of password recovery and theft. The method also works with new applications like IoT and smart home devices that require secure authentication that is privacy-conscious.

An objective assessment indicates the feasibility of the suggested system. True Acceptance rate (TAR) always has more than 90, this concludes correct legitimacy of users. False Acceptance Rate (FAR) is kept at a minimum of 5% reducing chances of unauthorized access. The seasonable error rate (Equal Error Rate) is around 6.5 percent which is the ideal falsal rate compared to the falsal negative. Maximization of privacy is achieved as no raw behavioral information is sent to the external servers. The proposed on-device framework, compared with cloud-based behavioral biometric systems, has removed possible exposure of data and still supports a high authentication accuracy and system responsiveness. The article supports the ornamental applicability of such strategy in the adoption of the industry. Companies that use passwordless and zero-trust models can add continuous behavioral authentication on the device to enhance its protection without violating user privacy. Compared to the current solutions like Google BeyondCorp that determines the degree of trust on a network level or Apple FaceID that only conducts a single stress authentication, the proposed framework offers continuous and continuously device-level checks. With the architecture, it is possible to perform adaptive risk scoring and thresholding, which makes it more resilient to unauthorized access, devices theft, or suspicious behavior without adversely affecting legitimate users.

The privacy and on-device behavioral trust engine is a practical and high-performance alternative to address current authentication issues. It reduces the shortcomings of the traditional passwords, inertial biometrics, and risk measurement systems that depend on the cloud. The framework has proven itself to be feasible technically and valuable in operation in order to fulfill high TAR, low FAR, small latency, and full on-device data retention. This work is the foundation of future research, such as multi-modal integration of behavioral signals, federated learning with cross device robustness, context adaptive thresholds, and extension to the IoT setting. The suggested solution is a meaningful advance in terms of safe, convenient, and privacy-sensitive, user-authentication, which will encourage the implementation of passwordless and zero-trust authentication in a wide range of applications in the real world.

References

[1] Ubale A. Beyond Telematics: Leveraging Generative AI for Synthetic Accident Reconstruction and Liability Attribution in Autonomous Vehicle Claims. IJAIBDCMS [Internet]. 2023 Dec. 30 [cited 2026 Feb. 24];4(4):119-24. Available from: https://ijaibdcms.org/index.php/ijaibdcms/article/view/356

[2] Shahin, M., Babar, M. A., & Zhu, L. (2017). Continuous integration, delivery and deployment: A systematic review on approaches, tools, challenges and practices. IEEE Access, 5, 3909–3943. https://doi.org/10.1109/ACCESS.2017.2690565

[3] Lyu, L., Yu, H., Ma, X., Chen, C., Sun, L., Zhao, J., Yang, Q., & Philip, S. Y. (2020). Privacy and robustness in federated learning: Attacks and defenses. IEEE Transactions on Neural Networks and Learning Systems. https://arxiv.org/abs/2012.06337

[4] Veluru, S. P., & Manchala, M. K. (2021). Federated AI on Kubernetes: Orchestrating secure and scalable machine learning pipelines. Essex Journal of AI Ethics and Responsible Innovation.

[5] Bogo, M., Soldani, J., Neri, D., & Brogi, A. (2020). Component-aware orchestration of cloud-based enterprise applications: From TOSCA to Docker and Kubernetes. Future Generation Computer Systems, 108, 91–106. https://arxiv.org/abs/2002.01699

[6] Yusaf, T., Kadirgama, K., Hall, S., & Fernandes, L. (2022). The future of sustainable aviation fuels: Challenges and solutions. Energies, 15(21), 8151. https://doi.org/10.3390/en15218151

[7] Vanama, S. K. R. (2024). Architecture Led Cloud Modernization: A Framework for Enterprise Migration from VMware to OpenShift and AWS. International Journal of Emerging Research in Engineering and Technology, 5(1), 117-125. https://doi.org/10.63282/3050-922X.IJERET-V5I1P114

[8] Vanama, S. K. R. (2023). Integrating Site Reliability Engineering SRE Principles into Enterprise Architecture for Predictive Resilience. International Journal of Emerging Trends in Computer Science and Information Technology, 4(3), 164-170. https://doi.org/10.63282/3050-9246.IJETCSIT-V4I3P117

[9] Ubale A. From Detect and Repair to Predict and Prevent: Assessing the Viability of Real-Time AI Nudges in Reducing Fleet Accident Rates. IJERET [Internet]. 2024 Jun. 30 [cited 2026 Feb. 24];5(2):115-23. Available from: https://ijeret.org/index.php/ijeret/article/view/408

[10] Lydia, M., Prem Kumar, G. E., & Selvakumar, A. I. (2022). Securing the cyber-physical system: A review. Cyber-Physical Systems, 9(3), 193–223. https://doi.org/10.1080/23335777.2022.2104378

[11] Deochake, S., & Channapattan, V. (2022). Identity and access management framework for multi-tenant resources in hybrid cloud computing. arXiv preprint arXiv:2203.11463. https://arxiv.org/abs/2203.11463

[12] Bhattacharjee, A., Barve, Y., Gokhale, A., & Kuroda, T. (2019). CloudCAMP: Automating cloud services deployment and management. Proceedings of the IEEE International Conference on Cloud Computing. https://arxiv.org/abs/1904.02184

[13] Gomber, P., Koch, J.-A., & Siering, M. (2020). FinTech: Research directions to explore the digital transformation of financial service systems. Journal of Service Theory and Practice, 30(1), 79–102. https://doi.org/10.1108/JSTP-08-2018-0185

[14] Hermes, S., Riasanow, T., Clemons, E. K., Böhm, M., & Krcmar, H. (2020). The digital transformation of the healthcare industry: Exploring the rise of emerging platform ecosystems and their influence on the role of patients. Business Research, 13, 1033–1069. https://doi.org/10.1007/s40685-020-00125-x

[15] Pástor, Ľ., Stambaugh, R. F., & Taylor, L. A. (2019). Asset price effects of peer benchmarking: Evidence from a natural experiment. International Review of Economics & Finance, 62, 53–65. https://doi.org/10.1016/j.iref.2019.02.012

[16] Kamila, N. K., Frnda, J., Pani, S. K., Das, R., Islam, S. M. N., Bharti, P. K., & Muduli, K. (2022). Machine learning model design for high performance cloud computing and load balancing resiliency: An innovative approach. Journal of King Saud University – Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2022.10.001

[17] Patel, N. (2021). Power-aware simulation challenges and solutions in semiconductor ICs design verification. International Journal of Intelligent Systems and Applications in Engineering.

[18] Gay, G., Staats, M., Whalen, M., & Heimdahl, M. P. E. (2015). The risks of coverage-directed test case generation. IEEE Transactions on Software Engineering, 41(8), 803–819. https://doi.org/10.1109/TSE.2015.2421011

[19] Benton, R. A., & Keister, L. A. (2017). The lasting effect of intergenerational wealth transfers: Human capital, family formation, and wealth. Social Science Research, 68, 1–14. https://doi.org/10.1016/j.ssresearch.2017.09.006

[20] Beaulahsoundarabai, P., Thriveni, J., Venugopal, K. R., & Patnaik, L. M. (2013). An improved leader election algorithm for distributed systems. International Journal of Next-Generation Networks, 5(1), 21–34. https://doi.org/10.5121/ijngn.2013.5102

[21] Stier, C., Domaschka, J., Koziolek, A., Krach, S., Krzywda, J., & Reussner, R. (2018). Rapid testing of IaaS resource management algorithms via cloud middleware simulation. Future Generation Computer Systems. https://arxiv.org/abs/1801.09484

[22] U. Din, M. Guizani, B. S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2018. https://ieeexplore.ieee.org/abstract/document/8531615

[23] Y. Alghofaili and M. A. Rassam, "A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique," *Sensors*, vol. 22, no. 2, p. 634, 2022. https://doi.org/10.3390/s22020634

[24] M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," *World Journal of Advanced Research and Reviews*, vol. 19, no. 3, pp. 105–116, 2023. https://doi.org/10.30574/wjarr.2023.19.3.1785

[25] Y. Yang, H. Wang, R. Jiang, X. Guo, J. Cheng, and Y. Chen, "A review of IoT-enabled mobile healthcare: Technologies, challenges, and future trends," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9478–9502, 2022. https://doi.org/10.1109/JIOT.2022.3144400

[26] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63229–63249, 2021. https://ieeexplore.ieee.org/abstract/document/9411833

[27] G. L. Santos, P. T. Endo, D. Sadok, and J. Kelner, "When 5G meets deep learning: A systematic review," *Algorithms*, vol. 13, no. 9, p. 208, 2020. https://doi.org/10.3390/a13090208

[28] V. T. Hayashi and W. V. Ruggiero, "Hands-free authentication for virtual assistants with trusted IoT device and machine learning," Sensors, vol. 22, no. 4, p. 1325, 2022. https://www.mdpi.com/1424-8220/22/4/1325

[29] M. A. Khan, I. U. Din, T. E. Majali, and B. S. Kim, "Survey of authentication in Internet of Things-enabled healthcare systems," *Sensors*, vol. 22, no. 23, p. 9089, 2022. https://www.mdpi.com/1424-8220/22/23/9089

[30] U. Ali, M. Y. I. B. Idris, J. Frnda, M. N. B. Ayub, M. A. Khan, N. Khan, and M. Babar, "Enhanced lightweight and secure certificateless authentication scheme (ELWA) for Internet of Things environment," *Internet of Things*, vol. 24, p. 100923, 2023. https://www.sciencedirect.com/science/article/pii/S2542660523002469