IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 21, 2021, accepted August 30, 2021, date of publication September 3, 2021, date of current version September 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3110310

A Frictionless and Secure User Authentication in Web-Based Premium Applications

RASHIDAH F. OLANREWAJU[1], (Senior Member, IEEE), BURHAN UL ISLAM KHAN[1], MALIK ARMAN MORSHIDI[1], FARHAT ANWAR[1], (Member, IEEE), AND MISS LAIHA BINTI MAT KIAH[2], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur 50728, Malaysia
[2]Department of Computer System and Technology, University of Malaya, Kuala Lumpur 50603, Malaysia

Corresponding author: Burhan Ul Islam Khan (burhan.iium@gmail.com)

This research has been supported by the Ministry of Higher Education Malaysia (MOHE) through its Fundamental Research Grant Scheme under Grant ID FRGS19-068-0676 and Ministry Project ID FRGS/1/2018/ICT01/UIAM/02/1.

ABSTRACT By and large, authentication systems employed for web-based applications primarily utilize conventional username and password-based schemes, which can be compromised easily. Currently, there is an evolution of various complex user authentication schemes based on the sophisticated encryption methodology. However, many of these schemes suffer from either low impact full consequences or offer security at higher resource dependence. Furthermore, most of these schemes don't consider dynamic threat and attack strategies when the clients are exposed to unidentified attack environments. Hence, this paper proposes a secure user authentication mechanism for web applications with a frictionless experience. An automated authentication scheme is designed based on user behavior login events. The uniqueness of user identity is validated in the proposed system at the login interface, followed by implying an appropriate user authentication process. The authentication process is executed under four different login mechanisms, which depend on the profiler and the authenticator function. The profiler uses user behavioral data, including login session time, device location, browser, and details of accessed web services. The system processes these data and generates a user profile via a profiler using the authenticator function. The authenticator provides a login mechanism to the user to perform the authentication process. After successful login attempts, the proposed system updates database for future evaluation in the authentication process. The study outcome shows that the proposed system excels to other authentication schemes for an existing web-based application. The proposed method, when comparatively examined, is found to offer approximately a 10% reduction in delay, 7% faster response time, and 11% minimized memory usage compared with existing authentication schemes for premium web-based applications.

INDEX TERMS Frictionless experience, internet, security, user authentication, web application, web services, cloud computing.

I. INTRODUCTION

In the past few decades, computing-based technology has gradually penetrated all aspects of daily human activities; security and privacy have become a significant concern [1]. The motivation to secure computing systems has changed in the current digital era. The traditional approach of securing computing systems, servers, and reliable audits does not offer a comprehensive security level for communication transactions in the diversified environment. As consequences of a successful attack have become more serious, designing a high-security mechanism for information security becomes crucial [2]. In web-based services and applications, users decide whether the applications or services they are accessing are safe. Therefore, the inherent need for robust security encouraging the developer to ensure higher safety is a prime design factor. Over the years, computing assets have transformed from a centralized system to a distributed system and more often to cloud-based virtual centralization. Cloud computing and web-based services are emerging as the de facto technological systems in the past few years. Cloud computing plays a crucial role in all aspects of human life, such as

The associate editor coordinating the review of this manuscript and approving it for publication was Binit Lukose.

healthcare, businesses, e-commerce, and online services [3], [4]. It is estimated that in the next few years, web applications will amount to a market transaction volume of over 1 trillion U.S. dollars [5]. Many big organizations and private enterprises facilitate their services on web applications and leverage the advantage and scalable features of the internet like simplicity and cost-efficiency. Unfortunately, most cyber-attacks are launched via the internet, and because of the weak security implementations, users are more susceptible to viruses, password thefts, and privacy attacks. All this leads to facing challenges in retaining applications and service security [6], [7].

User authentication and authorization are essential security layers to offer a wide range of protection over online services and web applications [8], [9]. Over the years, many efforts have been made by researchers towards enabling secure environments using authentication mechanisms based on username, passwords, one-time-password (OTP), biometrics (fingerprinting and facial recognition), and token-based security [10]. Conventional identity verification mechanism offers a good user authentication approach enabling users to access secure web applications. However, traditional authentication approaches are associated with limitations. They do not ask users to validate their uniqueness during their active login session, making computing devices vulnerable to invite security threats and illegal activity when they log in [11]. These studies have also emphasized improving privacy when accessing sensitive context information, which is a significant challenge. A multi-factor security mechanism is required to verify user identity uniqueness and communication transaction identity [12]. There are different variants of the existing research-based solution towards securing web applications reported viz. security assessment using fuzzy logic and analytical hierarchy process [13], [14], usage of filter for identifying injection attacks [15], detection of intrusion using machine learning [16], adoption of hybrid constraint solving for detection of attacks [17], and visualization-based tools for security monitoring [18]. Irrespective of different variants of the research-based solution towards securing web applications, the commercial web applications used in enterprises still encounter vulnerability issues. This is clear evidence that security issues connected to web applications are still an open-ended problem.

Therefore, this paper proposes a secure user authentication scheme with a frictionless experience for web-based applications. It allows users to use their devices to authenticate themselves without performing any additional authentication-related tasks while accessing web-based services. Frictionless user authentication adopts a risk-based strategy to evaluate the degree of threat followed by an appropriate amount of protection to be offered. The proposed solution addresses the issues associated with privacy concerns by implementing a multi-factor authentication process, which facilitates multiple processes for authentication from self-opting modules of credentials to validate user identity uniqueness for secure log in to web applications. The study brings the following contributions from work reported in this paper:

- A model is introduced to automatically select login options, which improves user experience based on the user behavior profile.
- An analytical methodology is adopted towards modelling Frictionless and Secure User Authentication (FSUA) in web applications, which offers a new perspective for the user identity authentication for secure log in to web applications.
- A logic-based behavior profiling is constructed that follows an analytical module that enables users to select an authentication method of their choice based on what the user has and what he knows.

The rest of this paper is organized as follows. Section II briefs existing approaches to accessing web-based applications and highlights the problem description. This is followed by a discussion on the frictionless authentication system in Section III. Section IV discusses the proposed system and methodology adopted. Section V presents a performance analysis of the proposed system. The overall contribution of this paper is concluded in Section VI.

II. BACKGROUND

This section provides a brief technical background on the security terminologies related to web applications and services. Further, a review of the state of practice in authentication is carried out to analyze the current pattern and research trend.

A web application is a software application or computer program that operates on web technology accessed through a web browser to perform a task over an open network channel like the internet. Web-based applications are extremely popular because of the universality of web browsers as clients. Another interesting fact is that maintaining a web application is independent of installing software programs on several client devices. Web applications offer various low-cost and premium services, including web-mail services, E-banking, E-commerce, various business applications, and many more [19]. Since the internet is a global network-connected system, the increasing usage of web applications to facilitate critical services to their users makes it an essential target for attackers. The web application supports a highly interactive interface and facilitates a communication platform to exchange information, including sensitive data such as financial and health. Therefore, ensuring higher security in the web application is a critical concern to every internet user.

A. WHY ARE WEB APPLICATIONS VULNERABLE TO CYBER ATTACKS?

Most enterprises attempt to secure their network systems using firewalls and Secure Sockets Layer (SSL), which cannot prevent web applications from being hacked; thus, the website and web application services are designed to be publicly accessible. The user or consumer database in web applications can often be directly accessed. If web

applications are attacked, an adversary or malicious user has complete access to the user database even if its firewall is configured appropriately. As a result, issues of data security like data integrity and availability become key factors. Besides, the network security system does not protect against web application attacks. They are initiated on port 80, which must be open to allow the consistent process of data transactions. Therefore, it is essential to maintain adequate authentication and access control mechanisms to ensure data and services are protected from unauthorized access.

B. WHY IS AUTHENTICATION NECESSARY IN WEB APPLICATIONS?

Web application security is one of the neglected aspects of corporate security today. Authentication acts as the primary layer of security towards securing users against identity theft or fraud and permits only authorized users to access web application services. If web applications are not implemented with an authentication mechanism, then the entire system, including network premium services and databases, may become vulnerable to severe attacks. The attackers increasingly focus on premium web-based applications and services like social networking sites, payment web apps login pages, shopping carts, dynamic content, and many more. Unsafe web applications are accessible twenty-four hours globally, providing laidback access to the backend of corporate databases, and allow attackers to commit illegal activities. A Web Application Security Consortium report stated that about 49% of the web services being analyzed are vulnerable to a high-security risk, and about 13% of web applications might be attacked [20]. The targeted web applications can be further used to initiate illegal activities such as sensitive data exposer, missing function level access control, transferring illegal content, misusing the website's bandwidth, and holding its owner responsible for the illegal actions. The study conducted by researchers [21] disclosed that about 75% of cyberattacks target web applications. Cybercriminals have also maintained a comprehensive database of attacks, which they frequently launch, such as cross-site scripting, security misconfiguration, authentication attacks, dictionary attacks, and parameters attacks.

C. CURRENT STATE-OF-PRACTICES ON FSUA

This section reviews state-of-art trends in secure and user-friendly authentication systems to access web-based applications and services:

1) COLLABORATIVE AUTHENTICATION SCHEMES

Authentication refers to the process of validating user identity. If the strength of the authentication system is weakened, then it means that authentication can be compromised. That may cause serious loss to the user or organization. An efficient authentication that can support user-friendly mechanisms could be designed based on PINs or passwords considering typical adversarial scenarios. However, an alternative solution can be developed based on the collaborative approach of multiple computing devices to facilitate a secure login process to a remote server and web applications. A combination of wearable units and smartphone devices would be a cost-effective approach in this context. Such a cooperative approach can offer a better form of security during the authentication process. For an attacker, it isn't easy to compromise authentication mechanisms to impersonate an authentic user. The ideology behind collaborative authentication mechanisms is to replace a password-authentication via a single authenticator and validator with multiple collaborative authenticators and a single validator. A threshold-based cryptography mechanism is adopted to reduce the wearable unit's risk of being lost using the conventional secret sharing method discussed by Shamir [21]. This idea was further followed up by Pedersen [22] to design Distributed Key Generation (DKG) scheme. Although the study offers decentralized security, it also induces significant time consumption to generate a secret key. In the same line of research, the DKG protocol was improved by Simoens *et al.* [23], who have shown that wearable devices are not much capable of storing secret shares to be united. However, the implementation doesn't ensure data security against device-capture attacks. The work of Bonneau *et al.* [24] carried a comprehensive study to provide an effective insight into the challenges in replacing passwords. Grosse and Upadhyay [25] focused on privacy and usability issues and suggested significant points for a better solution irrespective of the password-based authentication mechanism. In a similar research direction, Guidorizzi [26] presented their work in the context of moving beyond passwords. The author has suggested an authentication process based on personal information systems like biometrics sensors. However, the study didn't emphasize protecting the biometric template, which has a higher possibility of becoming compromised in public networks. Preuveneers and Joosen [27] designed a flexible context-aware authentication mechanism based on the fingerprint to check whether a user's identity is authentic continuously. Although the study offers a faster authentication scheme, it lacks a multi-level security system essential when considering an identity factor to strengthen user privacy. The study carried out by Corella and Lewison [28] analyzes the basic factors of the security requirements in frictionless authentication like usability, privacy, and security. The authors have introduced a frictionless scheme for web payments using a fingerprinting-based authentication scheme where the uniqueness of the cardholder is validated with a cryptographic credential in the cardholder's browser with a frictionless experience. However, the cryptographic credentials must be authenticated over the web-based application, where there is no further layer of security once the security token has been issued. Further, there is no resilience against man-in-middle attacks. Rimmer *et al.* [29] carried a review study to explore recent trends and challenges with frictionless authentication systems. The authors have discussed the significance of authentication and authorization in web-based and cloud-based applications and several challenges associated

with frictionless authentication technology while highlighting future research work opportunities. Liu *et al.* [30] developed 2-factor access control and authentication mechanism for web-based cloud applications. The author introduces an attribute-oriented access control system integrated with user secret key and lightweight hardware security devices. However, the scalability of this approach when the devices are exposed to potential attacks, e.g., distributed denial of service attacks or cross-scripting attacks, which is common in web applications is not validated. Besides, the approach needs storing the secret key, which is another level of security concern. Khandre and Shikalpure [31] tried to find an effective mechanism based on biometric conferencing without user interaction to ensure better service. The approach offers autonomous utilization, but there is a vulnerability due to unprotected storage of biometric templates in the server. The work carried out by Rahman *et al.* [32] designed a secure online transaction algorithm based on 2-factor authentication. The presented technique mandates a specialized hardware device to login into card accounts via an application to analyze the security tokens. This approach demands possession of hardware devices during authentication, which restricts portability and mobility factor.

The collaborative authentication scheme discussed above does have its security benefits while having serious usability impediments. Any solution developed based on such schemes need to consider limitations associated with this scheme.

2) RISK-BASED ACCESS CONTROL AND AUTHENTICATIONS

Risk-oriented access control and authentication mechanisms are fundamental blocks of commercial security models. As mobile and wearable units continue to increase, fundamental changes can be seen in people's access to services and web content. Also, there are related security risks because these devices are small, light, and configured with low-security protocol, threatening to be compromised. The recent progress in access control mechanisms is Risk-Adaptive-Access-Control, where the decision for access relies on dynamic assessment. There is a lot of knowledge on this subject in the existing research literature [33], [34]. Moreover, risk-oriented access control solutions and authentication processes are considered in the access management policies. Contextual information like device fingerprint, device location, I.P. address, date, etc., is used to assess users' risk of accessing web resources. However, this method is usually based on a weighted score function. Bilal *et al.* [35] evaluated the performance of their security technique, namely Reverse Authentication Authorizing and Accounting, with the existing Single Sign-On (SSO) mechanism. The outcome and performance analysis suggested that the presented work is always better towards facilitating efficient authentication and robustness to prevent web attacks. However, this approach depends on its password to be extra strong and dependent on server operation. In case the server is down, all the users are affected. The work carried out by Rahman *et al.* [32] used the concept of keystroke dynamics to provide a strong layer of authentication in web applications. The authors have designed a web-based platform to assess the performance of the presented authentication approach. The study outcome proves the efficiency of the proposed system with an equal error rate corresponding to approx. 10.5%. This technique can protect users from stopping mechanical keystroke captures but renders them helpless against any concerning phishing attacks. The authors in the study of Chang and Choi [33] discussed access control and user authentication and tried to explore a significant problem and research challenges associated with it. The authors have studied the research gap and many directions for future research work.

Access control is one of the essential security management scheme. With the evolution of various approaches, as discussed above, there is more scope for improvement. Developing access control based on different types of risk for web applications is not a simplified task and requires more in-depth exploration.

3) BEHAVIOMETRICS AUTHENTICATION

A recent trend in authentication is the use of behavioral biometrics that comprises specific attributes used to measure patterns to identify the identity of a user. Various research approaches have been introduced in the existing literature to explore feasibility in continuous authentication throughout the user login session and the non-intrusive authentication process to analyze frequent user interaction with the system. Recent trends in the existing literature have shown that user identities can be validated through multiple Behaviometrics, such as keystroke dynamics, CPU and RAM usage [36], mouse movements [37], accelerometers [38] fingerprints [39], and browsing behavior [40]. A detailed description of such an authentication process based on Behaviometrics can be found in the existing literature [41]–[43]. However, despite the significant advantage of Behaviometrics authentication, a key challenge is determining the appropriate combination of behavioral biometrics to achieve an adequate level of security and higher user experience. The study conducted by Haron *et al.* [11] presented an extensive discussion on the user behavior for multimodal authentication systems for web application access and login. The authors have highlighted the efficiency of a multimodal authentication scheme considering high-level user experience in this study. One of the downsides of this approach is its iterative operation to perform increasing steps of the process. Besides, the process is not implemented in a decentralized manner, which will eventually make all users vulnerable to attacks when compromised. Vassallo *et al.* [44] presented a security system based on behavioral authentication using keystroke dynamics. In this security approach, the authors have implemented multi-level privacy schemes, i.e., permutation, substitution, and suppression. The model improves security aspects but at the cost of computational burden due to increasing mathematical operations and memory dependency to store the values. Garg *et al.* [45] presented a brief survey on the multimodal authentication system. In this

survey, the authors have studied various biometric modalities depended upon using a single human characteristic. This study has highlighted the disadvantages of such a system and discussed the different methods for authentication towards achieving better security in the authentication process.

Although the literature mentioned above has dedicated attempts towards behavior-based biometric usage for security, adoption of dynamics involves biometric attributes that always invite security breaches. Apart from this, the adoption of biometrics also involves cost factors; although biometrics offer potential security in many cases, they are practically significantly less effective in web applications. What is required is to strengthen the security system to include various external attributes (e.g., biometric templates) while working on web application.

4) MULTI-FACTOR AUTHENTICATION

The weak login credential is one of the significantly prone areas of security attacks. The simple credential-(password) can be easily cracked with dictionary attacks and customized credential-cracking tools, particularly if the user has kept the same credential for different web services [46]. Also, it is always difficult to remember the complex form of credentials. It becomes hectic when entering such complex credentials on a wearable device or small computing devices such as mobile phones. This shows the commonly accepted conception that complex credentials are inconvenient. In this regard, several types of research are underway to transform the authentication process based on password credentials [26], [47]. With the adoption of multi-factor authentication, the users can perform identity verification with multiple authentication factors, namely, knowledge, biometrics, OTP token, and certificate. Biometric traits such as voice, fingerprints, and retinal scans cannot be forgotten, but security mechanisms based on biometric traits may not be cost-effective. Such a mechanism requires biometric features, which are usually troublesome to revoke and may be compromised. The multi-factor authentication process designed using public key encryption and digital certificates can be a robust solution, making it very difficult to launch common attacks on passwords. The work carried out by Osman *et al.* [48] presented a security model for web applications and internet-based services based on cryptographic approaches, access control, and session management schemes. The authors have adopted a hardware-based authentication mechanism with an MD5 hashing scheme. This paper also provides a threat analysis to analyze and evaluate their proposed security solution. However, the study didn't address the downsides of using MD5 due to the larger size of the dictionary table and the incapability to resist brute-force attacks. The work of Rama and Raja [49] has presented an OTP-based security analysis for user authentication to a web service based on the mobile application. However, the study's dependency on a long-term password is needed to perform user login on different websites. Seak *et al.* [50] designed a centralized approach for user authentication to access web services using security assertion markup language with SSO. Esfahani *et al.* [51] designed an effective web authentication mechanism to resist man-in-middle attacks in Industry 4.0. In this approach, the authors have used the TLS protocol to enable secure internet-based communications. However, the study cannot withstand common DDoS attacks. Moreover, TLS protocol cannot be used for a full-proof security system for identifying and stopping dynamic attackers. The study conducted by Swedha and Dubey [52] analyzed web authentication mechanisms using Amazon Web Services over the OpenStack platform. However, this scheme demands the storage of secret keys and a virtual handshaking mechanism. Although it offers security, its security effectiveness is not rigorously assessed with respect to various major threats in the cloud environment. The study of Herrera-Cubides *et al.* [34] introduced a security scheme based on a service-oriented architecture that enables the business system and authentication authority to separate services. Irrespective of the explicit security definition of this model, it still couldn't perceive the dynamics involved in unknown adversary identification and authentication. The study presented by Chandrakar and Om [53] used Rabin cryptosystem to design remote user authentication and session-key agreement mechanism. The presented scheme is robust against various attacks and efficient in smart card storage costs and processing time. Kaminsky *et al.* [54] tried to address the challenges associated with authentication in a global file system. In this work, an authentication server is adapted to validate user identity by considering local information. However, the lack of global attributes would further result in a vulnerable situation to get security updates. Zhang *et al.* [55] have developed an implicit authentication mechanism to recognize a user's past behavior to provide a secure login to mobile devices. However, the approach is associated with the limitation that it cannot monitor a user's behavior continuously. Many biometric-based authentication mechanisms require different hardware systems to capture data. However, biometric attributes are not emphasized to be protected much in existing approaches. The adversary can observe a unique feature of the user and may attempt to perform illegal activities. Altinok and Turk [56] presented a continuous authentication scheme based on biometric features to estimate authentication certainty over a certain time. The downside of the study is the decrease in system usability. Moral-Garcia *et al.* [57] suggested a security scheme based on model-driven architecture to offer guidelines for enabling a unified authentication mechanism. Trnka *et al.* [58] have carried out survey work on existing authentication and authorization for internet-of-Things-oriented applications. The authors have explored significant open research issues and highlighted critical points for future research work. In the study of Ndibanje *et al.* [59], the authors have presented an improvised version of the authentication mechanism presented by Jing *et al.* [60], which suffers from weak authentication factors and a complex message exchange process.

All the above approaches have a unique way to implement multi-factor authentication where the emphasis is mainly on

generating a secret key for authentication and authorization. The existing methods are also normally iterative in their operation and depend on its execution environment while working on web application. Hence, such limitations must be addressed to optimize security features while using such approaches in web applications.

D. PROBLEM DESCRIPTION

Based on literature analysis, it is determined that the authentication mechanism is necessary, but existing mechanisms have certain limitations. If the user's password is stolen and subsequently used by a malicious user, it leads to a single point of failure [23]. The existing authentication methods do not provide a comprehensive solution to address issues associated with various factors like (i) users prefer a single credential-based authentication mechanism [25], (ii) entering a complex password in wearable devices is very probabilistic, as they do not offer convenient user interactive interface [26], (iii) biometric solutions are not adequately suitable for carrying out continuous authentication process with minimal interaction with the user [27], (iv) specific risk-based techniques work well for desktop and laptops but fall short on mobile devices, [28]. Hence, most studies have been carried out considering either cookies, tokens, or third parties. Also, very few works have been carried out concerning the actual implementation of all the authentication mentioned above approaches. Utilizing these recent initiatives, multi-factor, collaborative authentication, and Behaviometrics-based authentication can further improve the requirement of adequate balance between security level and frictionless user experience. Several research challenges and opportunities remain to explore. Significant research problems are identified as follows:

- It has been identified that only a few research studies aimed towards frictionless user authentication in web applications and services.
- The existing works of literature on authentication systems do not offer a comprehensive solution [26], [34], [47]–[63]. Most of the existing solutions are not focused on determining that most wearable devices do not provide a suitable interface for password-based authentication [22]–[25].
- Most studies have not focused on the practical implementation of frictionless authentication techniques in web-based applications [32], [33], [35], [36].
- Existing surveys are more application-specific and do not cover the entire range of security and privacy in cloud computing systems and web services networks.

III. FRICTIONLESS USER AUTHENTICATION SYSTEM

From the previous section, it can be seen that the existing authentication solutions are based on the usage of a simplified form of credentials, e.g., usernames, PINs, and passwords that cannot be easily remembered and fed into wearable units and mobile devices. Such a process hinders user-friendly authentication from accessing privileged contents. As a result, there is ongoing research towards facilitating alternative forms of authentication to improve user experience. In this regard, a frictionless mechanism comes into the picture to enhance the user experience by reducing delays during the authentication process. Therefore, as a contribution, the proposed system introduces a novel FSUA to perform the authentication process. Users on their computing devices carry out this mechanism (e.g., smartphone, laptop, etc.) to a web content service provider on a larger scale of interactivity and user-friendly interface. Figure 1 depicts the frictionless user authentication scenario.

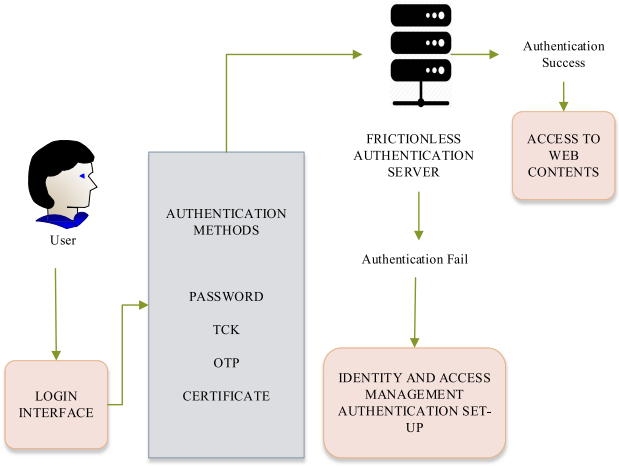

FIGURE 1. A typical scenario of the FSUA.

A user seeking access to web content provides different web applications. A login interface module is a user-computing device (mobile or laptop) that s/he uses to access the webserver. The user access will be successful upon the completion of authentication. The authentication methods in the proposed system comprise different ways provided via the analytics engine configured inside the authentication module. In contrast to the existing security system, the proposed analytics engine maintains a user profile based on their browsing pattern. One authentication method will be available to the user in a frictionless manner. It is a timesaving approach as it doesn't have to undergo many authentication steps. Once the authentication of user identity is successful, they are authorized to access web content. The contribution of this authentication system is that it has an analytical engine that offers different user options to undergo the authentication process giving more rounds of flexibility. In case of failed authentication, the user needs to go through the authentication setup process, or an alternate authentication mechanism is available to him. The proposed system introduces an analytical framework to offer a secure authentication scheme with a frictionless experience for safe user access into web-based applications. The prime objective of the proposed scheme is to provide an automated mechanism of authentication based on historical data and user behavioral profiles. The schematic

internal process flow of the proposed framework is described in Figure 1. The internal process flow of authentication in FSUA is presented in Figure 2, and it comprises the following entities:

i) *user*- an entity who wants to access services provided by the web application. The user may also carry personal or wearable computing devices to authenticate in a frictionless manner.

ii) *profiler*- this module maintains the user profile based on their behavior, the existing web access mechanism, and past login sessions. The profiler includes device location, login timestamp, and web application service, provider.

iii) *authenticator*- this module performs an automated authentication process.

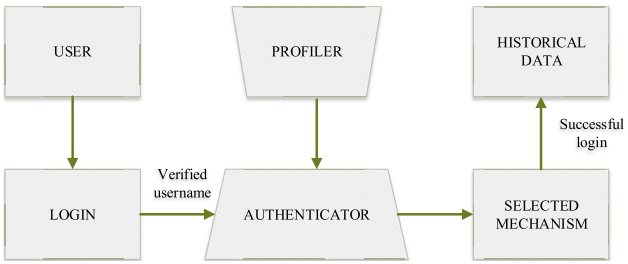

FIGURE 2. Internal process flow of authentication in FSUA.

Once the user is verified, the analytics engine selects the authentication mechanism for the user and forwards the authentication request to the authentication server. Apart from this, an additional layer of security is added in the proposed system viz. i) password-based authentication, ii) time-constrained key-based authentication, iii) one-time password token-based authentication, and iv) secure certificate-based authentication mechanism to user access into web-based applications. As the proposed system is designed using the frictionless methodology, hence there is the absence of any occurrences of overhead cost. The following section describes the methods adopted and the core implementation of the proposed system.

IV. IMPLEMENTATION STRATEGY

The proposed system uses an authentication gateway for initiating the process of accessing resources to the web application. The authentication server will ask the user to provide their credentials (username). After delivering its credential and verifying the username, the proposed system automatically selects authentication mechanisms. The analytical engine automatically displays a login mechanism for the user based on past events of the login method and historical profiles maintained in the database. If the user selected the suggested login option and completed its authentication, the successful login attempt is maintained to the historical database and profiler. However, the user can skip suggested login mechanisms and be allowed to select another authentication or login mechanism. In this process, the proposed system again initiates the user credential (username) verification process and suggests another login mechanism by excluding the skipped one. However, in some cases, multiple authentication methods may have the same login attempts in past login events and are maintained in the profiler and historical database. However, the proposed system in this scenario will select recent login mechanisms identified based on the timestamp carried by the profiler module. The overall process of the proposed system depends on the two core modules, namely the profiling module and the authenticator.

A. PAST EVENTS RECORDS AND HISTORICAL PROFILE

The past event and historical profiles refer to the data-gathering process to analyze the user's behavior and profiling in the analytics module. The entire information related to past events and user behavior is stored in three different contexts:

1) Event Storage: The event storage records information about events associated with previous access attempts, specifically contextual information about the user login pattern.

2) Pattern Constructor: This module is responsible for constructing patterns associated with past events records and historical profiles for the pattern construction process. It also evaluates the reference information inside the access record stored in event storage. The study considers access records in the predefined time only and does not consider entire access records. Any access records beyond a given timeline are regarded as outdated and will be ignored for adequate security.

3) Pattern Storage: Converting the context information of the attribute factor such as last session login time and device location into a vector, which is meaningful to the system, and then store the output record and the number of occurrences in the pattern storage. This information will then be fed to the analytics engine configured inside the authenticator module for the trust evaluating process via profiler. Each attribute factor is allocated with a unique identifier, and a profiler score is computed. The profiler consists of all these attribute records. The pattern construction procedure evaluates all recent records for all users in the system. However, this process will demand higher computational resources due to the large amount of data required to be processed. Therefore, the proposed system optimizes this process by allocating pattern construction at midnight within the scheduled timeline or when the system is ideal.

B. TRUST EVALUATING PROCESS

The trust evaluation process is the second process in the proposed FSUA scheme. The trust evaluation process is responsible for analyzing each user's login request, deciding and taking measures. The trust evaluation process consists of multiple modules viz. historical data storage, profile score calculator, and authentication method selection (Fig.2). From historical data storage, the reference collector processes data collection reflecting the current user access attempt parameters. All data is passed to the authenticator except the time access that uses the time clock of the authenticator. The device location is identified based on the I.P. address sent by

the authenticator. The pattern store contains the user attribute profile generated from the first procedure mentioned earlier. The profile score calculator is an integral part of the trust evaluation process. The trust calculator equivalences the current context processed with the user attribute profile to determine the user's total profile score. The empirical evaluation of trust score is computed as follows,

$$\text{Trust}_{\text{score}} = f(\text{C}|\text{U}_{\text{pa}}) \tag{1}$$

The expression (eq.1) shows a mechanism of computation of trust by an explicit function $f(x)$, which checks the successful score for each user profile attribute, U_{pa}. The variable C represents context that records the number of successful or failed authentication processes in historical rounds. The proposed system allocates the successful operation of authentication as one and unsuccessful attempts as 0. Hence based on the added score of the current user profile score, trust value is evaluated. The recent user profile scores are retained with [0 1]. It will mean that the outcome of the trust score will be a real-valued number between 0 to 1. If the trust score is more than 0.05, the authentication is further carried out, while the trust score less than that value is aborted. Hence, unlike any existing approach, the proposed system offers computation of dynamic trust value, which is highly adaptable for any form of the dynamic environment. The authenticator module determines the system's response based on the user's final profile score calculated by the analysis component and the level of the application to be accessed by the user. The response may be to grant the user access or require the user to provide additional credentials in complex cases. This is done to prevent the user from logging into the system, event storage stores data from the event collector and decisions from the authenticator. The stored information of events is used by a pattern constructor process that complements the closed-loop mechanism for authentication processes.

C. USER ATTRIBUTES

While accessing any form of the application over a web browser, different transactional features can be captured for analysis. This extraction of components can be carried out based on cached information from a prior session of access by the user. The proposed system performs extraction of a particular set of information associated with user access viz. time to access the content of website/portal, information about the source of the website being accessed, geographic location of the user attempting to access, the name of the browser that was used to access, and finally the operating system used over the machine to access. The primary information about accessing web-based content is an essential identifier to evaluate the maximized threat of access attempts. A similar time pattern is usually seen for each user to be active or inactive while accessing web-based content. The proposed system can also determine the behavior of a specific user based on geographical location to triangulate the origination point of access attempts. The malicious intention of any user can be determined by identifying the frequent variations in user location from the prior historical data. Usage of Global Positioning System integrated with the machines can capture the user's precise position. However, this approach includes costs due to additional hardware and the management process of tracking location. One cost-effective method for monitoring location will also be to monitor the I.P. address of the system from where access to the contents is carried out. At present, there is the availability of various services that can provide the user's precise location based on its I.P. address. The proposed system uses *IP2Location* [64] that offers solutions towards tracking I.P. address geographically with higher precision.

Further, the proposed system also analyzes accessibility towards various web contents without any dependencies towards using multiple identities of the user. The system offers users convenience and freedom to feed the credential multiple times while accessing different web contents. Owing to the usage of a singular authentication process, it provides user-friendliness and convenience. For a better tracking system, the proposed system indexes different applications with a unique identity that further analyzes user's behavior. The user's unusual behavior can be easily captured when the system finds users to access new applications that are rarely found in historical data of access. Finally, the client browser and operating system also assist in furnishing significant information about the user access activity.

D. AUTHENTICATION METHODS

The proposed FSUA system supports multiple types of authentication methods, but in this case, the following three authentication methods are being studied:

- *Username/Password:* A password is a secret text commonly used to verify the identity of a user. The authentication server only checks whether the person who claims to be the legitimate user is submitting a valid password. The significant issue with passwords is that they are usually static, thus vulnerable to a wide range of authentication attacks. Static passwords are still the most popular credentials used for authentication. However, users tend to set up easy-to-remember passwords with low entropy to minimize their hassle, thus making their applications susceptible to security threats. The proposed authentication framework is a pragmatic solution for countering the tedious task of creating and managing passwords.
- *OTP Token:* One-time passwords are dynamic in nature and hence can additionally be alluded to as passwords of single usage, i.e., upon each utilization, they are disposed of. OTPs are the most grounded variation of passwords and give a convincing answer to many security concerns. An OTP token is supported with a hardware computing device that displays a secure one-time password, which can only be used once and changed every two minutes. The password is generated based on a The time based one-time password (TOTP), the extension of HOTP (HMAC based OTP), from RFC 6238 using the current time and the activated key.

- *Digital Certificate:* Certificate-based authentication involves the usage of digital certificates issued by trusted entities to validate a user or a device before granting access. A digital certificate is an electronic document that utilizes a digital signature to bind a public key with an identity. The certificate usually comprises the certificate holder's name, a sequential number, certificate's expiration date, holder's public key, and the digital signature of the certificate-issuing authority (CA). Usually, digital certificates are kept locally on the device through which access is being sought and are often deployed in coordination with static passwords.

E. OPTIONAL AUTHENTICATION SELECTION

In Fig. 3, a flow process is described for the system assessment process after one authentication mechanism suggested by the system is skipped. Also, it has already been mentioned that some cases may be associated with the same number of Highest Profiler Score (HPS). The proposed system will then go with the method used in the last login session. Since the user can skip the authentication method, another case can be encountered where the user has only one login method; then, the proposed system will show a related message. While a user has used a different access/login method previously, the proposed system will discard that skipped mechanism and execute the re-assessment process to provide another login mechanism that the user has used chiefly. After a successful login, the information associated with the current session is stored in the historical database and profiler module.

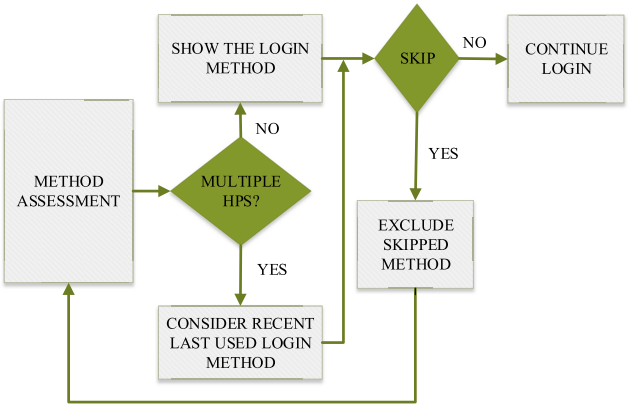

FIGURE 3. The assessment process after the selected mechanism is skipped.

The algorithm descriptions of the adopted methodology for automated authentication to web-based applications with frictionless experience are mentioned as follows:

Algorithm 1 mentioned above is designed for secure authentication of web services with a frictionless experience. The initial step of the algorithm is subjected to system configuration, where the user will first begin the enrolment process. The user will register themselves in the web service

Algorithm 1 Intelligent Attacks Recognition System

The proposed algorithm takes input values as traffic data-(T_D). After execution, the algorithm generates output as threat level identification-(T_L), which refers to particular kinds of attacks and any forms of threats identified in the system. The significant steps of the algorithm are as follows:

Input: Username (U)
Output: Authentication mechanism
Start
// System Configuration
Step1- User enrolment → Web services
Step2-Configure → Profiler
Step3-Profiler ←{browser, geo-location, login time, web service}
Step4 Configure → Authenticator
Step4a- Create → historical database
// System Deployment
Step5-User initiates the login process
Step6- User enter credential → U
Step7. User verification ← Authentication server
Step8- *Check: U is valid*
Step9- Initiate System assessment
Step10- Select authentication mechanism → login page
Step11- *Check: U is authenticated*
Step12- if successful → historical update profile.
End

or application using the browser as a user agent (step 1). Once the system profiler module is configured, the next step takes information associated with all login sessions to generate the user profile and profiler score for each authentication or login mechanism (step 2). An authenticator module is then designed as an explicit function that acts as an analytics engine to carry out further assessment tasks to provide an automated login option to the user for the verification process (step 3). A historical database is constructed to store all information related to successful login attempts. Both profiler and historical databases capture user behavior and session login details. In the system deployment phase, the user opens a login page and provides a credential in the form of a username (U) to validate its uniqueness via the authentication server (step 5-7). The system checks whether the username U is verified (step 8). If it is unique, the authenticator initiates an assessment process to select the login mechanism for the user authentication (step 9). In the next step, the system forwards the mechanism chosen to the login page (step 10). Then the request is sent to the authentication server to perform user authentication (step 11). If the user is authenticated, the system flags login successfully, and details of current login attempts are added to the historical database (step 12). The following section discusses the performance analysis of the proposed system.

V. RESULT AND PERFORMANCE ANALYSIS

The proposed implementation used a specific form of the experimental setting. The design and development of the complete model have been carried out in Java environment considering enterprise architecture system. The database structure is designed over Oracle, while the full application after development is hosted over Amazon Elastic cloud. To perform the initial level of authentication, the proposed system considers a single host machine (physical) with 15 virtualized environments. Virtual machines use the Ubuntu platform, while the host machine is standard systems with i5 Core of 9th generation intel processor and with 4 G.B. of RAM. The URL of this cloud-based application, guarded by SSL and the Secured HTTP protocol (HTTS), is now shared with multiple users to investigate its security performance. A network protocol analyzer is also used to capture the information associated with data flow, number of accesses, latency patterns, client application used, number of events, memory utilization, etc.

The observation carried out in this stage is as follows: The information used for the analysis is collected from the 114817 I.P. address of the user's device used for accessing their web-based resources. Among the others, 2662 access records from external networks, 2515 were from Malaysia. Among them, Kuala Lumpur has 2116 access records. The remaining login records are from Sweden. (3), the Philippines (2), Thailand (3), Netherlands (2), and United States (37). The login admissions saved in the log table refer to server machine time when login requests were received from the authenticator. The data are collected from three timeslots viz. i) first timeslot (7:00PM-12:00AM), ii) second timeslot (8:00AM-7:00PM), and iii) third timeslot (12:00AM-8:00AM). Hence, the term timeslot refers to the duration of time where the observation has been carried out, anticipating three different traffic load possibilities. The login record demonstrates that 94.4% of login requests were received for the scheduled timeline refers to the second time slot, and 3% of the total record came from the first time slot (i.e., 7 pm to 12 am). In the third time slot (i.e., 12 am to 8 am), only 1.6% of login events were recorded.

The observed data confirms the presence of a more extensive user base required to verify while assessing the security performance of the proposed system. Owing to the massive size of recorded data associated with the proposed model, the result analysis is carried out using qualitative and quantitative mechanisms. The qualitative mechanism offers information about the individual performance of the model. In contrast, the quantitative mechanism provides more insight about performance effectiveness concerning standard security performance parameters followed by security analysis.

A. QUALITATIVE METHOD ANALYSIS

A profiler and authentication module is used primarily to access the security strength of the proposed authentication system. However, unlike conventional authentication scheme analysis, the proposed system performs an extensive analysis via qualitative mechanisms. In this method, all the primary attributes of authentication obtained from a test client application, timestamp (date and time), and selection of authentication mechanism are assessed. For this purpose, the proposed system considers four alternatives of authentication, i.e., password-based, Time-Constrained Key (TCK), OTP, and certificate-based password. The prime justification behind the above authentication is based on their frequent adoption in the majority of existing authentication.

TABLE 1. User distribution based on browser and profiler score.

Browser	Authentication Mechanism			
	Password	TCK	OTP	Certificate
Firefox	0.22807	0.105263	0.157895	0.508772
Chrome	0.258621	0.051724	0.172414	0.517241

The *profiler module* maintains a user profile based on user behavioral information such as login sessions, device location, browser type, and web applications. A user profile is generated in a profiler-based on the data provided by the analytics engine and authentication server after the user credential is verified. In particular, the user profile is generated after successful login attempts and user-related parameters like a web application, browser, and device location. The proposed system uses the probability concept to evaluate the probability score P_{score} associated with successful authentication. The first dependable variable for P_{score} is *password login* which signifies a number of only successful authentication.

In contrast, *total login* represents number of overall passwords fed to the system for authentication purposes. It will eventually mean that probability P_{score} is computed by favorable outcome to total outcome of providing a password. The selection of logging methods via analytics engine is based on the username profiler score computed from the following equation:

$$P_{score} = \frac{password\ login}{total\ login} \tag{2}$$

The total access in Firefox for password ($n_1 = 13$), TCK ($n_2 = 6$), OTP ($n_3 = 9$), and certificate-based ($n_{14} = 29$). Similarly, the access in Chrome for password ($m_1 = 15$), TCK ($m_2 = 3$), OTP ($m_3 = 10$), and certificate-based ($m_{14} = 30$). The probability score for Firefox is calculated as P_{score} (Password) $= n_1/(n_1 + n_2 + n_3 + n_4)$, P_{score} (TCK) $= n_2/(n_1 + n_2 + n_3 + n_4)$, P_{score} (OTP) $= n_3/(n_1 + n_2 + n_3 + n_4)$, and P_{score} (Certificate) $= n_4/(n_1 + n_2 + n_3 + n_4)$. A similar method is also carried out for Chrome to obtain the numerical outcome shown in Table 1. On the other hand, the profiler also maintains a timestamp for each authentication method. Table 1 and Table 2 illustrate the profiler score and timestamp format concerning each authentication/login method, respectively. The next operation towards qualitative analysis is the *authenticator module* implemented with an

TABLE 2. Timestamp for an authentication mechanism.

Timestamp	Password	TCK	OTP Token	Certificate
Date	12/03/2021	18/03/2021	22/03/2021	29/03/2021
Time (sec)	1600 Hrs	1645 Hrs	2000 Hrs	0800 Hrs

TABLE 3. Authentication mechanism selection.

User-Related Parameter	Authentication Mechanism with Profiler Score			
	Password	TCK	OTP Token	Certificate
Browser	1	1	2	1
Web application	2	3	1	1
Device location	3	5	1	2
Timestamp	4	2	3	2
Accumulated profiler score	10	11	7	6

analytics engine to assess user profiles to select an authentication mechanism based on the accumulated profiler score. In this process, the authentication mechanism with the HPS is preferred for user login. Table 3 demonstrates a sample representation for the authentication mechanism based on the highest accumulated profiler score.

Table 3 shows the profiler score concerning browser, web application, device location, and the timestamp for authentication mechanism selection for secure user login. After username verification, an accumulated profiler score is computed. This outcome infers that the timestamp for password-based authentication is comparatively higher than the OTP-token-based authentication system. It is also seen that TCK-based and certificate-based authentication system offers similar timestamp. On the other hand, the TCK-based approach has more dependency on device location than OTP-based and certificate-based authentication. A similar pattern is also seen for the dependence of web application parameter dependency for TCK. For example, in Table 3 HPS is 11. Therefore, the TCK authentication mechanism is chosen to log in to the web application.

Qualitative analysis is also carried out further to assess the number of access attempted with increasing time of entry. The graphical analysis of events login based on a timeline is presented in Figure 4. This is essentially carried out to understand the user's pattern for performing access considering the account of access time. Unlike any existing system, the proposed method, therefore, offers an extraction of patterns to identify the anomaly behavior of the user.

A network protocol analyzer and the proposed experimental model are operated simultaneously to confirm the same number of tracked unique logins at different instantaneous times. The numerical data exhibited in Table 4 are observation values for 24 Hours carried out on 16th February 2021. From an experiment viewpoint, Java Socket Clients are used to

TABLE 4. Frequencies of access observed.

Observation Time	Number of Login
00:00 Hours	149
03:00 Hours	268
06:00 Hours	785
09:00 Hours	24,432
10:00 Hours	20,650
11:00 Hours	10,000
12:00 Hours	6789
13:00 Hours	16,521
14:00 Hours	16,987
15:00 Hours	16710
16:00 Hours	5423
18:00 Hours	1671
21:00 Hours	325
00:00 Hours	96

confirm unique access identities, while the Wireshark protocol analyzer is used to confirm the same. The graphical trend of the same data is exhibited in Figure 4.

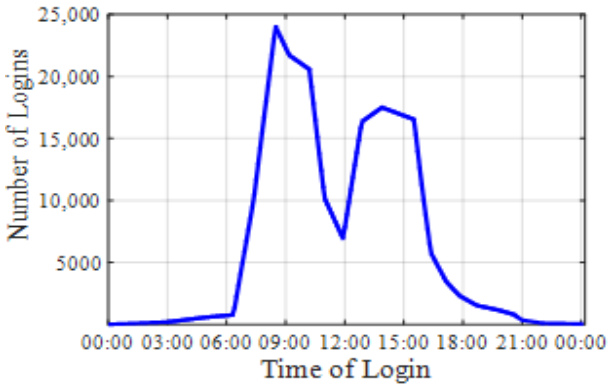

FIGURE 4. Analysis of access pattern.

The prime objective of capturing the numerical values in Fig.4 is to capture the access pattern to realize the peak and off hours of network traffic load. This provides an opportunity to execute the proposed algorithm in different time samples to assess its performance. The idea is also to see if the algorithm introduces any significant delay with increased traffic load. The proposed study assumes the possibility of an attack in both off and peak hours, and hence this data was essential to capture. Figure 4 demonstrates the graphical analysis for the number of logins concerning time log in (hours). From the results, it can be ascertained that the user's login increases from 7 am onwards. After 7:00 pm, the rate of the number of logins tends to be low (i.e., decreasing). The login trend shows the normal distribution in the login events since the standard working hours are between 9:30 am to 6:30 pm.

In the afternoon, the number of logins declines approximately for 2 hours.

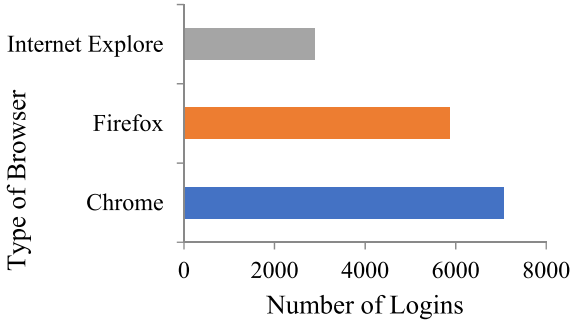

FIGURE 5. Logins Vs. Browser type.

Figure 5 highlights the graphical presentation for the number of login records concerning browser types. The graph trend shows that Chrome and Firefox are the top two most favorite web browsers. In those, the most prevalent web browsers are Chrome, followed by Firefox and internet Explorer. Figure 6 provides a graphical analysis of user attribute values versus login times based on different threshold ratios. The value given to the threshold-ratio is the condition for calculating the mutual context of each user attribute. The higher the assigned weight, the more stringent the requirements for making an entry for an ordinary user. Each user may have different behavior patterns. Similar data stored in data logs were used as input parameters for analysis. The analysis provides a ratio-limit effect on the number of active user attributes concerning all login accesses. Record and analyze the number of events when the attribute factor is activated. In each of these events, the respected attribute factor affects the attribute score result, thereby reducing the trust established by the user. The study used different threshold-ratio values (i.e., 10, 30, and 50) to analyze their impact on each user attribute.

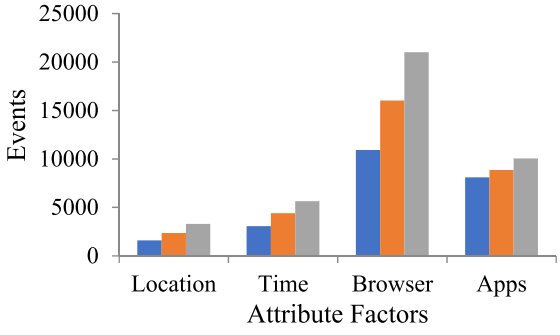

FIGURE 6. A number of events for each attribute.

It can be analyzed from the graph trend that for each user attribute, the higher the threshold-ratio value, the more events. When a higher threshold-ratio percentage is used, the number of events that do not activate the attribute decreases. Browser type contributed the most significant number of occasions, followed by application, login time, and location. It can be concluded that individual users are more inclined to use various types of browsers compared with other factors. Location is a minor factor.

B. QUANTITATIVE METHOD ANALYSIS

To carry out quantitative analysis, it is necessary to showcase a measurable value of the performance parameters. As the proposed system targets authentication mechanism, the performance parameters selected are delay, response time, and memory utilization. The rationale behind selecting the approaches mentioned above is that they are frequently used in existing authentication over web-based applications. A secure system should reduce delays in data transmission before getting authorization and getting authorization by a service provider to the user. An efficient, secure system also demands faster response time to reduce any chances of a man-in-middle attack. In contrast, memory utilization is used to showcase computational efficiency, especially for the client machine. For this purpose of quantitative outcome analysis, a similar test bench compares the proposed system and the existing systems. The study considers the existing authentication systems utilizing Cookie-based approach (CBA) [61], Token-based approach (TBA) [62], and Third-party based approach (TPA) [63]. The outcome of quantitative analysis for opted performance parameters are discussed as follows:

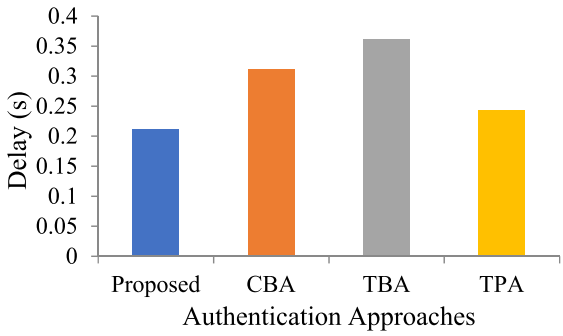

FIGURE 7. Comparison of delay analysis.

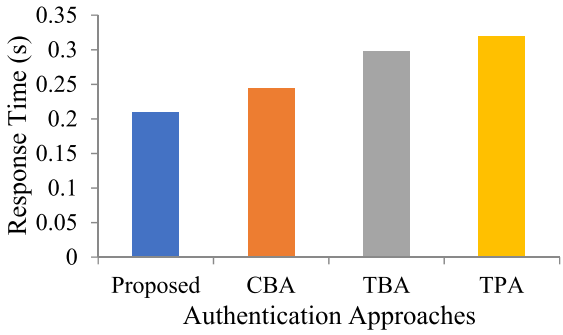

FIGURE 8. Comparison of response time analysis.

Before discussing the outcomes, it should be noted that CBA, TBA, and TPA are majorly the existing and frequently adopted authentication approaches in present times, as witnessed in Section II of this paper. Figure 7 showcases that

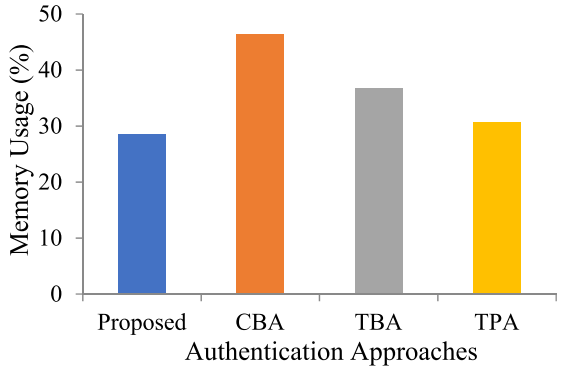

FIGURE 9. Comparison of memory utilization.

the proposed system offers reduced delay compared to the existing system. The cookie-based system has a dependency towards accessing login credentials from the server, where further verification is carried out, followed by the generation of unique identification of a session. This information may sometimes be so vast that it can over-saturate the server, too, resulting in increased response time as shown in Figure 8 and increasing memory utilization shown in Figure 9. It should be noted that the proposed system has been analyzed over 4GB RAM. On the other hand, it is seen that the existing token-based authentication system results in the generation of a web token specific to each unique client resulting in increased delay if the system deals with a stream of data. Furthermore, the memory utilization is relaxed in TBA compared to CBA as all the user information is within this web token (Figure 9). Moreover, this token is not permitted to be stored in the server, and this results in quite an iterative operation, causing an increase in response time (Figure 9). The lower memory utilization for TBA also owes to the management of this web token with the client-side. The usage of third-party access offers various benefits of the supportive services resulting in reduced delay than CBA and TBA (Figure 8). However, its response time is comparatively higher than CBA and TBA due to the long process of sharing user information (Figure 9). However, this does not significantly affect memory utilization. This is the key contribution of the proposed system, where without adopting any complex structure of encryption like the existing scheme, the proposed method offers better performance.

C. SECURITY ANALYSIS

It is seen that the proposed authentication system called FSUA offers a secure and automated user authentication mechanism with a frictionless experience. The discussion of the security analysis is carried out based on the threats it offers resistivity as follows:

- *Illegitimate Access*: As the proposed system is hosted over a cloud environment, an intruder has a fair possibility of illegitimate access. This could only happen when the attacker knows the authentication score. It should be noted that the proposed system has an internal analytical engine that performs the computation of P_{score} based on the threat environment and not based on user choice. Hence, if an intruder attempts to select an optional access system, then the numerical score of P_{score} for the favorable outcomes will never match with its past access pattern. Therefore, the authentication eventually fails for them. The possibility of having an appropriate P_{score} for an intruder is one successful attempt out of 1000 attempts which could be an expensive aspect for an intruder. Hence, the proposed system offers significant security from any form of illegitimate access.
- *Resistivity from attacks*: The proposed system is highly resistive from attacks viz. denial of service, information disclosure, repudiation, and data tampering attacks. The prime justification is that the proposed method offers an intellectual recognition of attacks within a faster response time based on dynamic parameters. Hence, irrespective of the presence of any such attackers in different forms, the proposed system can identify and stop them without depending on maximum resources.

The underlying scheme offers the user to select the authentication mechanism of their own choice, based on their past events of the login session. Therefore, FSUA provides resistance to any forms of attacks that compromise data integrity. Apart from this, the proposed system offers its total user rights on its intellectual property, which also supports data ownership if hosted on a cloud environment. FSUA also provides resistance to any malicious codes, which tampers the trust value as it maintains a historical profile based on user behavior. FSUA facilitates a multimodal authentication system based on the user's behavior profile without any friction in the user experience. It will mean that an attacker cannot compromise trust value without knowing the behavior profile. It is unlikely that malicious nodes can access information of behavior profiles as they are dynamic and encoded to a higher level. The analytical function of the proposed system is based on user-related parameters like location, timing, and browser. These parameters are highly associated with user behavior, as each user has their behavior of web service access such as browser and authentication mechanism. This means that the proposed system offers an automated authentication process in which the user's desired login mechanism is selected in a different environment without creating any confusion. The proposed study provides a lightweight, cost-efficient, and faster responsive mechanism without using any complex cryptographic mechanism.

VI. CONCLUSION

This article explores the feasibility of implementing a frictionless mechanism in user authentication to access web services and applications. The authentication setup utilizes profiler-based user behavior information to generate a login method for user authentication. FSUA setup is lightweight and reduces the time-consuming process in real-time systems. It is secure and flexible, offering a multi-model authentication process, where users can select a login mechanism of their

own choice. FSUA can also prevent unauthorized access and secure user authentication to premium web applications with frictionless experience by using their devices to authenticate them without deliberately performing any authentication tasks. The outcome of the study shows that the proposed authentication scheme offers reduced delay, lower processing time, and lower dependencies of memory compared to frequently used authentication for web applications, i.e., CBA, TBA, and TPA. The study contribution, as well as novelty set by the proposed system, are:

- Existing methods emphasize using claimed robust authentication primitives where there is also a possibility that such solutions do not consider dynamic threat and attack strategies when clients are exposed to unidentified attack environments. Unlike the existing system, the proposed method offers multiple options to access web content while increasing convenience and improving security features towards monitoring precise behavioral patterns.
- The prior mechanism towards frictionless authentication system mechanism involves complex and iterative evaluation of risk before authenticating and authorizing a user, whereas the proposed system offers progressive risk evaluation based on identity and access management attributes, while utilizing prior historical information about profile to evaluate the threat landscape in few straightforward steps.
- Existing authentication approaches have potential usage of complex and sophisticated encryption primitives with a dependency on resources. However, the proposed system implements a novel profiling mechanism that can permit a better form of trust evaluation within a multiple user access environment evaluated in both peaks and off hours.

The future work will be further continued towards applying an optimization approach of the proposed frictionless authentication scheme. The idea is to make the system more robust by exploring more appropriate dynamic environmental attributes additionally.

ACKNOWLEDGMENT

The authors are thankful to the three anonymous reviewers for their careful reading of the initial manuscript, as their many insightful comments and suggestions have helped improve and clarify the contents of the paper.

The authors express their personal appreciation for the effort of Gousia Nissar, Md Moktarul Alam, and Abdul Mobeen Khan in proofreading, editing, and formatting the paper.

REFERENCES

[1] P. Muthukrishnan, V. Sakthivel, B. Ramachandran, and K. Srihari, "Technical analysis on security realization in web services for e-business management," *Inf. Syst. e-Bus. Manage.*, vol. 18, no. 3, pp. 427–438, Sep. 2020, doi: 10.1007/s10257-019-00423-w.

[2] B. U. I. Khan, R. F. Olanrewaju, and F. Anwar, "Rehashing system security solutions in e-banking," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 4905–4910, 2018.

[3] M. S. Mir, M. A. B. Suhaimi, B. U. I. Khan, M. M. U. I. Mattoo, and R. F. Olanrewaju, "Critical security challenges in cloud computing environment: An appraisal," *J. Theory Appl Inf. Technol*, vol. 95, no. 10, pp. 2234–2248, 2017.

[4] R. F. Olanrewaju, B. U. I. Khan, M. M. U. I. Mattoo, F. Anwar, A. N. B. Nordin, R. N. Mir, and Z. Noor, "Adoption of cloud comput in higher learning institutions: A systematic review," *Indian J. Sci. Technol.*, vol. 10, no. 36, pp. 1–19, 2017, doi: 10.17485/ijst/2017/v10i36/117641.

[5] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2013, doi: 10.1016/j.jcss.2014.02.005.

[6] S. Z. Sajal, I. Jahan, and K. E. Nygard, "A survey on cyber security threats and challenges in modem society," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, Brookings, SD, USA, May 2019, pp. 525–528, doi: 10.1109/EIT.2019.8833829.

[7] P. Padma and S. Srinivasan, "A survey on biometric based authentication in cloud computing," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Coimbatore, India, Aug. 2016, pp. 1–5, doi: 10.1109/INVENTIVE.2016.7823273.

[8] T. Midhun, K. Prasanth, and J. Anoop, "A survey on authorization systems for web applications," *J. Comput. Eng.*, vol. 17, no. 3, pp. 1–5, 2015.

[9] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and M. Yaacob, "Offline OTP based solution for secure internet banking access," in *Proc. IEEE Conf. e-Learn., e-Manage. e-Services (IC e)*, Nov. 2018, pp. 167–172, doi: 10.1109/IC3e.2018.8632643.

[10] K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," *Proc. SPIE*, vol. 7667, Apr. 2010, Art. no. 76670L, doi: 10.1117/12.847886.

[11] G. R. Haron, D. Maniam, L. M. Nen, and N. I. Daud, "User behaviour and interactions for multimodal authentication," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Auckland, New Zealand, Dec. 2016, pp. 309–316, doi: 10.1109/PST.2016.7906979.

[12] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, R. N. Mir, and M. Yaacob, "Scrutinising internet banking security solutions," *Int. J. Inf. Comput. Secur.*, vol. 12, nos. 2–3, pp. 269–302, 2020, doi: 10.1504/IJICS.2020.105180.

[13] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, pp. 48870–48885, 2020, doi: 10.1109/ACCESS.2020.2978038.

[14] M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective," *IEEE Access*, vol. 8, pp. 25543–25556, 2020, doi: 10.1109/ACCESS.2020.2970784.

[15] S. Ibarra-Fiallos, J. B. Higuera, M. Intriago-Pazmino, J. R. B. Higuera, J. A. S. Montalvo, and J. Cubo, "Effective filter for common injection attacks in online web applications," *IEEE Access*, vol. 9, pp. 10378–10391, 2021, doi: 10.1109/ACCESS.2021.3050566.

[16] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of deep learning to real-time web intrusion detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.

[17] J. Thome, L. K. Shar, D. Bianculli, and L. Briand, "An integrated approach for effective injection vulnerability analysis of web applications through security slicing and hybrid constraint solving," *IEEE Trans. Softw. Eng.*, vol. 46, no. 2, pp. 163–195, Feb. 2020, doi: 10.1109/TSE.2018.2844343.

[18] F. O. Sonmez and B. G. Kilic, "Holistic web application security visualization for multi-project and multi-phase dynamic application security test results," *IEEE Access*, vol. 9, pp. 25858–25884, 2021, doi: 10.1109/ACCESS.2021.3057044.

[19] S. Gordeychik, J. Grossman, M. Khera, M. Lantinga, C. Wysopal, S. Shah, L. Lee, C. Murray, and D. Evteev, "Web application security statistics," *Web Appl. Secur Consortium.*, pp. 1–172, Jan. 2010.

[20] *Gartner*. Accessed: Apr. 21, 2021. [Online]. Available: http://www.gartner.com

[21] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[22] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Annu. Int Cryptol. Conf.*, Santa Barbara, CA, USA, 1991, pp. 129–140, doi: 10.1007/3-540-46766-1_9.

[23] K. Simoens, R. Peeters, and B. Preneel, "Increased resilience in threshold cryptography: Sharing a secret with devices that cannot store shares," in *Proc. Int Conf Pairing-Cryptogr.*, Yamanaka Hot Spring, Japan, 2010, pp. 116–135, doi: 10.1007/978-3-642-17455-1_8.
[24] J. Bonneau, C. Herley, P. C. V. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Secur. Privacy*, San Francisco, CA, USA, May 2012, pp. 553–567, doi: 10.1109/SP.2012.44.
[25] E. Grosse and M. Upadhyay, "Authentication at scale," *IEEE Security Privacy*, vol. 11, no. 1, pp. 15–22, Jan. 2013, doi: 10.1109/msp.2012.162.
[26] R. P. Guidorizzi, "Security: Active authentication," *IT Prof.*, vol. 15, no. 4, pp. 4–7, Jul. 2013, doi: 10.1109/mitp.2013.73.
[27] D. Preuveneers and W. Joosen, "SmartAuth: Dynamic context fingerprinting for continuous user authentication," in *Proc. 30th Annu. ACM Symp. Appl. Comput.*, Salamanca, Spain, Apr. 2015, pp. 2185–2191, doi: 10.1145/2695664.2695908.
[28] F. Corella and K. P. Lewison, "Frictionless web payments with cryptographic cardholder authentication," in *Proc. Int. Conf. Hum.-Comput. Interact.*, Orlando, FL, USA, 2019, pp. 468–483, doi: 10.1007/978-3-030-30033-3_36.
[29] T. Van hamme, V. Rimmer, D. Preuveneers, W. Joosen, M. A. Mustafa, A. Abidin, and E. A. Rúa, "Frictionless authentication systems: Emerging trends, research challenges and opportunities," 2018, *arXiv:1802.07233*. [Online]. Available: http://arxiv.org/abs/1802.07233
[30] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two-factor access control for web-based cloud computing services," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 484–497, Mar. 2016, doi: 10.1109/TIFS.2015.2493983.
[31] A. A. Khandre and S. Shikalpure, "WAAM web & Android authentication model using improvised user identification and verification technique using biometric and digital certificate," in *Proc. 2nd Int Conf I-SMAC (IoT Social, Mobile, Anal., Cloud)*, Palladam, India, 2018, pp. 536–541, doi: 10.1109/I-SMAC.2018.8653703.
[32] K. A. Rahman, D. Neupane, A. Zaiter, and M. S. Hossain, "Web user authentication using chosen word keystroke dynamics," in *Proc. 18th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Boca Raton, FL, USA, Dec. 2019, pp. 1130–1135, doi: 10.1109/ICMLA.2019.00188.
[33] H. Chang and E. Choi, "User authentication in cloud computing," in *Proc. Int. Conf. Ubiquitous Comput. Multimedia Appl.*, Daejeon, South Korea, 2011, pp. 338–342, doi: 10.1007/978-3-642-20998-7_42.
[34] J. F. Herrera-Cubides, P. A. Gaona-García, and G. A. Salcedo-Salgado, "Towards the construction of a user unique authentication mechanism on LMS platforms through model-driven engineering (MDE)," *Sci. Program.*, vol. 2019, pp. 1–16, Mar. 2019, doi: 10.1155/2019/9313571.
[35] M. Bilal, C. Wang, Z. Yu, and A. Bashir, "Evaluation of secure OpenID-based RAAA user authentication protocol for preventing specific web attacks in web apps," in *Proc. IEEE 11th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Beijing, China, Oct. 2020, pp. 82–90, doi: 10.1109/ICSESS49938.2020.9237635.
[36] N. A. Hamid, S. Safei, S. D. M. Satar, S. Chuprat, and R. Ahmad, "Mouse movement behavioral biometric systems," in *Proc. Int. Conf. User Sci. Eng. (I-USEr)*, Selangor, Malaysia, Nov. 2011, pp. 206–211, doi: 10.1109/iUSEr.2011.6150566.
[37] I. Deutschmann, P. Nordstrom, and L. Nilsson, "Continuous authentication using behavioral biometrics," *IT Prof.*, vol. 15, no. 4, pp. 12–15, Jul./Aug. 2013, doi: 10.1109/MITP.2013.50.
[38] T. Van Goethem, W. Scheepers, D. Preuveneers, and W. Joosen, "Accelerometer-based device fingerprinting for multi-factor mobile authentication," in *Proc. Symp. Eng Secure Softw. Syst.* Cham, Switzerland: Springer, 2016, pp. 106–121, doi: 10.1007/978-3-319-30806-7_7.
[39] J. Spooren, D. Preuveneers, and W. Joosen, "Leveraging battery usage from mobile devices for active authentication," *Mobile Inf. Syst.*, vol. 2017, pp. 1–14, Mar. 2017, doi: 10.1155/2017/1367064.
[40] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1565–1573, Mar. 2011, doi: 10.1016/j.asoc.2010.08.003.
[41] M. Abramson and D. W. Aha, "User authentication from web browsing behavior," Nav. Res. Lab., Washington, DC, USA, 2013.
[42] H. Saevanee, N. L. Clarke, and S. M. Furnell, "Multimodal behavioural biometric authentication for mobile devices," in *Proc. IFIP Int Inf. Secur Conf.* Berlin, Germany: Springer, 2012, pp. 465–474, doi: 10.1007/978-3-642-30436-1_38.
[43] L. Wang and X. Geng, *Behavioral Biometrics for Human Identification: Intelligent Applications*. Hershey, PA, USA: IGI Global, 2009, p. 530.
[44] G. Vassallo, T. Van Hamme, D. Preuveneers, and W. Joosen, "Privacy-preserving behavioral authentication on smartphones," in *Proc. 1st Int. Workshop Hum.-Centered Sens., Netw., Syst.*, Nov. 2017, pp. 1–6, doi: 10.1145/3144730.3144731.
[45] S. Garg, R. Vig, and S. Gupta, "Multimodal authentication system: An overview," *Int. J. Control Theory Appl.*, vol. 10, no. 13, pp. 111–119, 2017.
[46] M. Jakobsson and M. Dhiman, "The benefits of understanding passwords," in *Mobile Authentication*. New York, NY, USA: Springer, 2013, pp. 5–24, doi: 10.1007/978-1-4614-4878-5_2.
[47] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *J. Comput. Secur.*, vol. 15, no. 5, pp. 529–560, Jul. 2007, doi: 10.3233/jcs-2007-15503.
[48] A. M. Osman, A. Dafa-Allah, and A. A. M. Elhag, "Proposed security model for web based applications and services," in *Proc. Int. Conf. Commun., Control, Comput. Electron. Eng. (ICCCCEE)*, Khartoum, Sudan, Jan. 2017, pp. 1–6, doi: 10.1109/ICCCCEE.2017.7866696.
[49] M. Rama and S. S. Raja, "Web based security analysis of OPASS authentication schemes using mobile application," in *Proc. Int. Conf. Emerg. Trends VLSI, Embedded Syst., Nano Electron. Telecommun. Syst. (ICEVENT)*, Tiruvannamalai, India, Jan. 2013, pp. 1–3, doi: 10.1109/ICEVENT.2013.6496552.
[50] S. C. Seak, N. K. Siong, W. H. Loon, and G. R. Haron, "A centralized multimodal unified authentication platform for web-based application," in *Proc World Congr. Eng. Comput. Sci.*, San Francisco, CA, USA, vol. 1, 2014, pp. 1–6.
[51] A. Esfahani, G. Mantas, J. Ribeiro, J. Bastos, S. Mumtaz, M. A. Violas, A. M. D. O. Duarte, and J. Rodriguez, "An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain," *IEEE Access*, vol. 7, pp. 58981–58989, 2019, doi: 10.1109/access.2019.2914454.
[52] K. Swedha and T. Dubey, "Analysis of web authentication methods using Amazon web services," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–6, doi: 10.1109/ICCCNT.2018.8494054.
[53] P. Chandrakar and H. Om, "An efficient two-factor remote user authentication and session key agreement scheme using rabin cryptosystem," *Arabian J. Sci. Eng.*, vol. 43, no. 2, pp. 661–673, Feb. 2017, doi: 10.1007/s13369-017-2709-6.
[54] M. Kaminsky, G. Savvides, D. Mazieres, and M. F. Kaashoek, "Decentralized user authentication in a global file system," in *Proc. 19th ACM Symp. Operating Syst. Princ. (SOSP)*, Bolton Landing, NY, USA, 2003, pp. 60–73, doi: 10.1145/945445.945452.
[55] D. Zhang, F. Song, Y. Xu and Z. Liang, *Advanced Pattern Recognition Technol With Applications to Biometrics*. Hershey, PA, USA: IGI Global, 2009, p. 384.
[56] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," in *Proc. Workshop Multimodal User Authentication*, 2003, pp. 1–7.
[57] S. Moral-García, S. Moral-Rubio, E. B. Fernández, and E. Fernández-Medina, "Enterprise security pattern: A model-driven architecture instance," *Comput. Standards Interfaces*, vol. 36, no. 4, pp. 748–758, Jun. 2014, doi: 10.1016/j.csi.2013.12.009.
[58] M. Trnka, T. Cerny, and N. Stickney, "Survey of authentication and authorization for the Internet of Things," *Secur. Commun. Netw.*, vol. 2018, pp. 1–17, Jun. 2018, doi: 10.1155/2018/4351603.
[59] B. Ndibanje, K. Kim, Y. Kang, H. Kim, T. Kim, and H. Lee, "A secure and efficient mutual authentication hand-off protocol for sensors devices support in Internet of Things," *Sensors Mater.*, vol. 29, no. 7, pp. 953–960, 2017, doi: 10.18494/sam.2017.1603.
[60] X. Jing, J. Zhao, Q. Zheng, Z. Yan, and W. Pedrycz, "A reversible sketch-based method for detecting and mitigating amplification attacks," *J. Netw. Comput. Appl.*, vol. 142, pp. 15–24, Sep. 2019, doi: 10.1016/j.jnca.2019.06.007.
[61] M. Bugliesi, S. Calzavara, R. Focardi, and W. Khan, "Automatic and robust client-side protection for cookie-based sessions," in *Proc. Int Symp. Eng. Secur Soft Syst.*, Munich, Germany, 2014, pp. 161–178, doi: 10.1007/978-3-319-04897-0_11.

[62] J. Kubovy, C. Huber, M. Jäger, and J. Küng, "A secure token-based communication for authentication and authorization servers," in *Proc. Int Conf Future Data Secur Eng.*, Can Tho City, Vietnam, 2016, pp. 237–250, doi: 10.1007/978-3-319-48057-2_17.
[63] A. Vapen, N. Carlsson, A. Mahanti, and N. Shahmehri, "Third-party identity management usage on the web," in *Proc. Int Conf Passive Act. Netw Meas.*, Los Angeles, CA, USA, 2014, pp. 151–162, doi: 10.1007/978-3-319-04918-2_15.
[64] *Identify Geographical Location and Proxy by IP Address*. Accessed: Jul. 14, 2021. [Online]. Available: https://www.ip2location.com/

RASHIDAH F. OLANREWAJU (Senior Member, IEEE) was born in Kaduna, Nigeria. She received the B.Sc. degree (Hons.) in software engineering from University Putra Malaysia, in 2002, and the M.Sc. and Ph.D. degrees in computer and information engineering from the International Islamic University Malaysia (IIUM), Kuala Lumpur, in 2007 and 2011, respectively. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, IIUM, where she is leading the Software Engineering Research Group (SERG). She is an Executive Committee Member of technical associations, like IEEE Women in Engineering and Arab Research Institute of Science and Engineers. She represents her university, IIUM, at the Malaysian Society for Cryptology Research. Her current research interests include mapreduce optimization techniques, compromising secure authentication and authorization mechanisms, secure routing for *ad-hoc* networks, and formulating bio-inspired optimization techniques.

BURHAN UL ISLAM KHAN is associated as a Postdoctoral Fellow with the Computer Network Research Group at International Islamic University Malaysia. He holds a Ph.D. degree in engineering from the same university. Before commencing his doctoral degree, he has been involved in varying roles as that of a Software Engineer, a Research Analyst, and an Assistant Professor. He has published over 60 refereed articles in a wide range of highly recognized international journals and conferences (Springer, IEEE, ACM, etc.). His current research interests include designing one time password schemes, employing mechanism design, and game theory to protect *ad-hoc* networks.

MALIK ARMAN MORSHIDI received the B.Sc. degree in computer science from Western Michigan University, USA, in 1999, the M.Sc. degree in computer systems engineering from Universiti Putra Malaysia, in 2007, with a focus on the vision and navigation system for an autonomous mobile robot for plant watering, and the Ph.D. degree in engineering from the University of Warwick, U.K., in 2013, with a focus on image processing and augmented reality. Upon graduation, he started his career as a System Engineer at MacroHard AUM Sdn. Bhd. Later, he joined Office Equipment & Communication Sdn Bhd (OEC), in 2000, as a System Analyst, where he worked directly under the supervision of the Software Team, Unit Bisnes Fasiliti (UBF), Tenaga Nasional Berhad (TNB), and Petaling Jaya. In 2001, he joined as a Chief Software Engineer at Irhamna IT Sdn Bhd (IIT). During his tenure at both OEC and IIT (where both are TNB vendors), he was responsible for developing and managing many software development projects for TNB and a recipient for Certificate of Excellence for this achievement. In 2003, he joined academic profession as an Assistant Lecturer at the Faculty of Engineering, International Islamic University Malaysia (IIUM).

FARHAT ANWAR (Member, IEEE) received the Ph.D. degree in electronic and electrical engineering from the University of Strathclyde, U.K., in 1996. Since 1999, he has been with IIUM and currently working as a Professor with the Department of Electrical and Computer Engineering. He has published extensively in international journals and conferences. His research interests include QoS in IP networks, routing in *ad-hoc* and sensor networks, computer and network security, network simulation and performance analysis, the IoT, and biometrics.

MISS LAIHA BINTI MAT KIAH (Senior Member, IEEE) received the Ph.D. degree in information security from Royal Holloway, University of London, U.K., in 2007. Since then, she has been an Active Researcher with the Faculty of Computer Science and Information Technology, UM, in the computer science field, particularly in security. She was promoted to a Professorship, in 2015. Her main research interest will always be in the security aspect of computing and technology fields with variation of applications in multi and/or transdisciplinary projects. This is evidenced by her publications and research projects in which she is/was the Principal Investigator (PI) as well as a Co-PI. As a Professional Technologist (Ts.), keeping up with the current trend and demand of ever evolving computing technology field is crucial to ensure the quality and the impact of her research work. Her current research interests include cyber security, blockchain technology, the IoT, and health information exchange. She is an Active Member of EC Council, Malaysian Society for Cryptology Research (MSCR), and Malaysia Board of Technologists (Ts.).