A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users

Krishnapriyaa Kovalan[1], Siti Zobidah Omar[2]*, Lian Tang[3], Jusang Bolong[4]
Rusli Abdullah[5], Akmar Hayati Ahmad Ghazali[6], Muhammad Adnan Pitchan[7]
Institute for Social Science Studies (IPSAS), Universiti Putra Malaysia[1, 2, 6]
Department of Communication, Faculty of Modern Languages and Communication, Universiti Putra Malaysia[1, 2, 3, 4]
Baoji University of Arts and Sciences[3]
Department of Software Engineering and Information System[5]
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia[5]
Department of Media and Communication Studies, Faculty of Social Science and Humanities, Universiti Kebangsaan Malaysia[7]

***Abstract*—The authentication system is one of the most important methods for maintaining information security in smart devices. There are many authentication methods, such as password authentication, biometric authentication, signature authentication, and so on, to protect cloud users' data. However, online information is not yet effectively authenticated. The purpose of this systematic literature review is to examine the current types of authentication methods as a safety practices for information security among Internet users. The PRISMA method was adopted to present a systematic literature review of 28 articles from three main databases (20 articles from Scopus, one article from Google Scholar, and seven articles from Dimension). This study used the Prediction Study Risk of Bias Assessment Tool to appraise the quality of the included studies. From the findings of the study, a total of three main themes were identified: password authentication, biometric authentication, and multiple-factor authentication. Multiple-factor authentication was found to be the most secure and most frequently recommended authentication method. It is highly recommended to implement three-factor authentication and multi-biometric model in the future, as it provides a higher surveillance level in terms of information security among cloud computing users.**

Keywords*—Password authentication; biometric authentication; multi-factor authentication; information security; safety practices

I. Introduction

Smart telecommunication devices have become a fundamental element in most of our lives, and for many have become a trusted companion. It is where we store almost all our data and information. However, in Malaysia, the statistics for denial of service, malicious attacks, intrusion, and fraud indicated 6898 cases in 2016, 6686 cases in 2017, 7993 cases in 2018, 9890 cases in 2019, and 9646 cases in 2020 respectively [1]. The statistics show that information security incident reports increased from 2017 through 2019 and decreased slightly in 2020. The expanding number of smart devices and increasing availability of Internet access have changed the lives of many individuals. People began to use the Internet for different purposes, such as obtaining information, communicating, banking, entertainment, and many more [2]. The Internet also plays an important role as a teaching aid in universities [3]. Cloud computing allows users to save data online and access it from anywhere at any time via an Internet connection, instead of using a hard drive or other storage devices [4]. The development of cloud storage, however, has its own negative aspects, such as information security attacks. Data transmittal in the cloud environment can require a huge amount of bandwidth, which may allow hackers to retrieve the information [5] and the insufficiency of authentication is the cause of information attacks in cloud computing [6]. Data transparency and unauthorized information usage are the reasons behind these attacks [7]. With safe Internet usage awareness, being vulnerable to cyber threats and becoming a cyber victim can be avoided [8].

Authentication is a method for estimating the level of trust one can have that the source of information is who it is stated to be [9]. The authentication process happens when information is entered into the login system with a database. Then, the system checks whether the information entered matches the database information. If it matches, the user can access the system [10]. Social environment factors such as parents, friends, work colleagues, social media, and government policies play a vital role in educating Internet users about cybersecurity [11]. The public and organizations have to realize that cybercrime is highly risky, and that they have to take safety precautions to protect their information from being shared online [12]. An effective way to protect storage and authorization of data in the cloud environment is by having an appropriate authentication [13]. The general objective of this study is to examine the authentication methods used as a safety-enhancing practice for information security among Internet users. This study will benefit the Internet user society acknowledging that authentication plays an important role in enhancing a greater cloud environment. The higher the demand of Internet of Things (IoT) justifies the usefulness of safe authentication method. Further, research gap was noticed in the types of authentications used in the last five years. Hence, this paper intends to develop a systematic literature review by focusing on the types of authentications used in the last five years.

*Corresponding Author

The authors would like to thank the Ministry of Higher Education (MOHE) Malaysia for Funding this project under Fundamental Research Grants Scheme, Project Code 05-01-18-2036FR and FRGS/1/2018/SS09/UPM/02/1/5540161.

II. Method

Using a systematic literature review, an exhaustive exploration of the research topic was made to provide the objective summary of current studies related to the research topic. Systematic literature described as a qualitatively and quantitatively identifying, merging, and assessing all available data to produce results related to a specific research question [14]. It is also a study to analyse research problems by recognizing, evaluating, and integrating results of all related studies acknowledging one or more research objectives [15]. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method was used to study authentication method as a safety practice for information security among Internet users. Studies related to the authentication method for the 5 years from 2016 through 2020 were reviewed. Figure 1 displayed the flow diagram of this systematic review process.

A. *Systematic Review Process*

The systematic review process can be classified into three stages which are identification, screening and included [36]. This process is in accordance with PRISMA 2020 Flow Diagram (as shown in Figure 1).

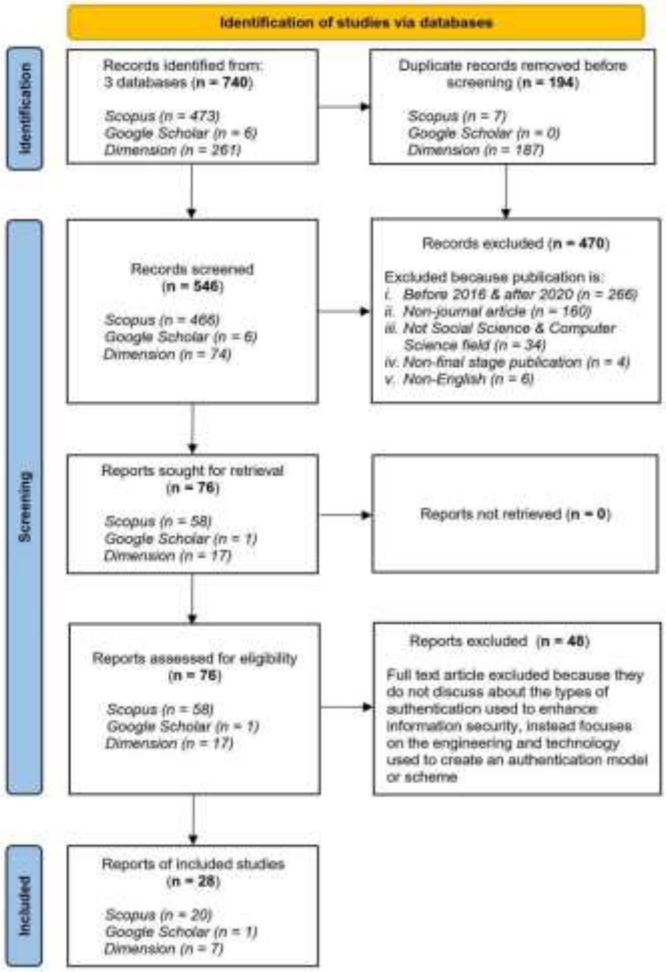
Identification of studies via databases
Identification
Records identified from:
3 databases (n = 740)
Scopus (n = 473)
Google Scholar (n = 6)
Dimension (n = 261)
Duplicate records removed before screening (n = 194)
Scopus (n = 7)
Google Scholar (n = 0)
Dimension (n = 187)
Screening
Records screened
(n = 546)
Scopus (n = 466)
Google Scholar (n = 6)
Dimension (n = 74)
Records excluded (n = 470)
Excluded because publication is:
i. Before 2016 & after 2020 (n = 266)
ii. Non-journal article (n = 160)
iii. Not Social Science & Computer Science field (n = 34)
iv. Non-final stage publication (n = 4)
v. Non-English (n = 6)
Reports sought for retrieval
(n = 76)
Scopus (n = 58)
Google Scholar (n = 1)
Dimension (n = 17)
Reports not retrieved (n = 0)
Reports assessed for eligibility
(n = 76)
Scopus (n = 58)
Google Scholar (n = 1)
Dimension (n = 17)
Reports excluded (n = 48)
Full text article excluded because they do not discuss about the types of authentication used to enhance information security, instead focuses on the engineering and technology used to create an authentication model or scheme
Included
Reports of included studies
(n = 28)
Scopus (n = 20)
Google Scholar (n = 1)
Dimension (n = 7)

Fig. 1. The Flow Diagram of this Systematic Review Process Source: Page et al. [45].

B. *Identification*

The systematic review process can be categorized into three stages. The first is the identification of keywords of a specific study, a process to enrich keywords in a search string. Keyword searching related to this study was based on synonym searching in thesauruses, dictionaries, and past research. Sa'di et al. [16] found that, in Merriam Webster's dictionary, "authentic" means "original, actual, or truthful" as well as "true" (http://www.merriam-webster.com/dictionary/authentic). However, in this study, the theme was mostly about the types of authentications. "Authentication" is defined as "verification" and "certification" in the thesaurus. The dictionary also defines authentication as verification, certification, and validation.

The terms 'certification' and 'validation' were removed from the search string as use of these terms did not return the expected theme of study from the databases. The search strategy was developed in March 2021, as shown in Table 1. below. This process retrieved a total of 740 papers (473 from Scopus, six from Google Scholar and 261 from Dimension). Before moving to the screening process, 194 duplicate papers obtained from all three main databases were manually removed (as shown in Figure 1).

C. *Screening*

The second stage of the systematic review is screening. From the three main databases, a total of 546 papers were screened based on inclusion and exclusion criteria as determined by the researchers (Scopus = 466 papers; Google Scholar = 6 papers; Dimension = 74 papers; as shown in Table 1). The first criterion was that the timeline of this review was only focused on papers published during a five-year period from 2016 to 2020. Second, only research articles in journals were included. Then, only articles published in the fields of computer science and social science were retrieved. In addition, only articles that had reached final publication stage are reviewed in this study. Last, only English-language articles were included. A total of 470 articles were excluded based on the inclusion and exclusion criteria (as shown in Table 2).

Seventy-six articles were retrieved from the inclusion and exclusion criteria process. All 76 articles were successfully moved into the next stage of the screening process, eligibility. Eligibility is a manual process of document exclusion, the purpose of which is to filter the articles based on their respective abstract, method, results, or findings section to ensure that the articles match the objective of the systematic review. A total of 48 articles were excluded in this process because their contents were mostly about pure engineering and science that did not address the objective of this review.

D. *Inclusion*

A total of 28 articles were eligible for inclusion in this systematic review [17 - 44].

E. *Selection and Data Collection*

The main review process in this paper consisted of coding the themes, known as thematic analysis. A panel of five researchers from the field of cybersecurity, analysed the selected articles one by one. They independently reviewed titles and abstracts of 76 screened articles and discussed all the inconsistencies found. The themes were then generated by the panel for validation, individually and in pairs. This is to ensure that there is no bias toward the themes discussed. The themes were then double-checked and renamed, if necessary, after several discussions among the panel of researchers. The researchers came up with several themes once the article reviewing process was completed. This process was repeated three times before the themes were finalized. The panel later auto generated a standardized data, extraction form to abstract the characteristics of a study, which included type of authentication, research objectives, research design, findings, contribution, and limitation. Reviewers worked independently and simultaneously to extract article data. Data extraction was completed only when conflicts of idea were resolved, and reviewers were assured that their view of the topic was neutral.

TABLE I. KEYWORDS AND SEARCH STRATEGY

Database	Keywords and Search String
Scopus	TITLE-ABS-KEY ((“password authentication” OR “two factor authentication” OR “multi-factor authentication” OR “token authentication” OR “biometric authentication” OR "transaction authentication" OR "computer recognition authentication" OR "single sign-on authentication” OR "email authentication” OR "laptop recognition authentication” OR "gadget recognition authentication" OR “fingerprint authentication” OR "fac* authentication" OR "device authentication" OR “mobile authentication” OR "android authentication" OR “ios authentication” OR “password verification” OR “two-factor verification” OR “multi-factor verification" OR “token verification” OR “biometric verification" OR “transaction verification” OR "computer recognition verification" OR "single sign-on verification” OR "email verification” OR "laptop recognition verification” OR "gadget recognition verification" OR “fingerprint verification” OR "fac* verification" OR "device verification" OR “mobile verification” OR “android verification" OR “ios verification”) AND ("information security" OR " information protection” OR "information safety" OR "data security" OR "data protection" OR "data safety”))
Google Scholar	Phase 1: allintitle: “authentication” OR “verification”, “security” Phase 2: allintitle: “password authentication” OR “two factor authentication” OR “multi-factor authentication” OR “token authentication” OR “biometric authentication” OR "transaction authentication" OR "computer recognition authentication" OR "single sign-on authentication” OR "email authentication” OR "laptop recognition authentication” OR "gadget recognition authentication" OR “fingerprint authentication” OR "facial authentication" OR "device authentication" OR “mobile authentication” OR "android authentication" OR “ios authentication” OR “password verification” OR “two-factor verification” OR “multi-factor verification" OR “token verification” OR “biometric verification" OR “transaction verification” OR "computer recognition verification" OR "single sign-on verification” OR "email verification” OR "laptop recognition verification” OR "gadget recognition verification" OR “fingerprint verification” OR "facial verification" OR "device verification" OR “mobile verification” OR “android verification" OR “ios verification” "information security" OR " information protection” OR "information safety" OR "data security" OR "data protection" OR "data safety”
Dimension	Phase 1: ("authentication" OR "verification") AND (security) Phase 2: (“password authentication” OR “two factor authentication” OR “multi-factor authentication” OR “token authentication” OR “biometric authentication” OR "transaction authentication" OR "computer recognition authentication" OR "single sign-on authentication” OR "email authentication” OR "laptop recognition authentication” OR "gadget recognition authentication" OR “fingerprint authentication” OR "facial authentication" OR "device authentication" OR “mobile authentication” OR "android authentication" OR “ios authentication” OR “password verification” OR “two-factor verification” OR “multi-factor verification" OR “token verification” OR “biometric verification" OR “transaction verification” OR "computer recognition verification" OR "single sign-on verification” OR "email verification” OR "laptop recognition verification” OR "gadget recognition verification" OR “fingerprint verification” OR "facial verification" OR "device verification" OR “mobile verification” OR “android verification") AND ("information security" OR " information protection” OR "information safety" OR "data security" OR "data protection" OR "data safety”)

TABLE II. THE INCLUSION AND EXCLUSION CRITERIA

Criterion	Inclusion	Exclusion
Timeline	From 2016 to 2020	Before 2016 and after 2020
Literature type	Journals (research articles)	Journals (review papers), books, preprints, book chapters, series, conference proceedings, trade journal
Subject area	Computer science and social science	Other than computer science and social science
Publication stage	Final	Other than final
Language	English	Non-English

F. *Quality Appraisal*

This present study used the Prediction Study Risk of Bias Assessment Tool (PROBAST) to appraise the quality of the included articles. Based on PROBAST, five experts in this research group assessed the risk of bias by means of 22 multiple-choice questions with the responses No (N), Yes (Y), Unclear (U), and Not Applicable (X). The answer of “Y” for each signalling question was assigned 1 point, and that of “N,” “U,” or “X” was assigned 0 points. The total score ranged from 0 to 22. The five reviewers gave an overall score for each included study. An average score of 0–7 for each article is considered low quality, 8–14 is considered medium quality, and 15–22 is considered high quality [46][47]. All 28 articles were retained in the final review, as they met the standard of medium quality.

G. *Data Analytic Strategy (Synthesis Methods)*

Twenty-eight articles were reviewed, evaluated, and analysed after the eligibility process in this study. The search was thoroughly done according to the objective of this review, which is to study the current types of authentication methods as safe practice for information security among Internet users. The studies were classified into relevant themes by using qualitative synthesis. This was done by reading the title, abstract, and keywords of each study. Furthermore, a thematic analysis was performed to classify themes related to type of authentication method. Through an article review process, relevant groups were identified. Finally, a total of three main themes including password authentication, biometric authentication, and multifactor authentication methods emerged. Password-based methods were grouped into textual and graphical authentication. Biometric methods were classified into fingerprint, facial, retina or iris, voice, and digital signature authentication. Several review processes were done by the authors to finalize the themes and sub-themes.

III. Results

Seven hundred forty papers were identified based on the search strings. Later, 28 articles were found to be eligible for the review process by using qualitative synthesis. The results of the systematic literature review are further summarized in Table 3. The table shows the title of article, layer(s) of authentication applied, authors and, subject of the study. Of the 28 articles reviewed, 20 were about biometric authentication [18 - 21], [23 - 33], [35], [37], [40], [42], [44]. There were 17 studies about textual password authentication [17], [21], [23], [25 - 27], [30], [32 - 38], [41 - 43] and three studies about graphical password authentication [22], [34], [39]. Seventeen studies discussed multifactor authentication [17], [19], [21], [23 - 28], [30], [32 - 37], [42] (as shown in Figure.2.). The review found that most scholars had chosen to focus on biometric authentication. There were some studies excluded from this review [48 - 52] as they did not focus on types of authentication methods as a safety practice for information security. Of the 28 articles reviewed, 13 were based in India [20 - 26], [30], [34 - 37], [42]; four were from China [32], [33], [38], [44]; two from Saudi Arabia [18], [19] one from Poland [27]; one from the Czech Republic [31]; one from the United Arab Emirates [28]; one from Turkey [43]; one from Ukraine [40]; 1 from Jordan [17]; and one each from Zambia [29]; Philippines [39]; and the United States [41] (as shown in Figure 2).

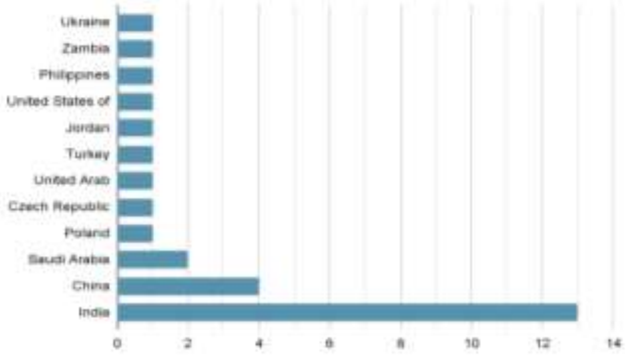

Fig. 2. Countries of Origin.

IV. Discussion

A. Types of Authentication

Based on the analysis, this section discusses types of authentications, such as password authentication (textual and graphical authentication), biometric authentication (fingerprint, facial, retina, voice, and digital signature), and multifactor authentication.

- Password authentication

Password has been used to protect online information since the early existence of the Internet. Passwords often do not expire, and users tend to use the same password for a long period, which leads to cyberattacks [53]. Passwords are one of the most significant risk factors because they are vulnerable to threats and attacks. Thus, a well-formulated and structured password should be “easy to remember but hard to hack” [54]. In this paper, the review has found two sub-themes under password authentication: textual and graphical.

1) Textual password authentication: Textual password authentication is knowledge based. Only four studies have focused on textual authentication [17] [38][41][43], whereas 12 other studies considered textual password as a part of multifactor authentication [23] [25-27] [30] [32-37] [42]. Furthermore, textual password authentication was studied by Akingbade [4]. Their study aimed to construct a protected login interface that could avoid cybersecurity attacks by using the 6 × 6 sized alpha numeric characters. The keyboard used in this experimental study was divided into letters, numbers, and symbols. Besides, users were allowed to select different of password lengths and different characters according to their preference. In fact, textual password method has been used in traditional bank environments, such as keying in the six-digit ATM personal identification number (PIN) [17]. In another experimental study that involved two groups: a control group and an experimental group; aimed to enhance the security of text-based passwords and to examine the effectiveness of creating a text-based password [43]. It was found that the experimental group experienced a more successful method of creating strong passwords that were also easy to remember. Another study, using a qualitative methodology aimed to understand the practice of mobile authentication user’s security awareness [41]. Twenty mobile device users made up the sample study, 19 of whom were aware of risk management in authentication. Additionally, used dynamic password technology, also known as One-Time Password (OTP) [38]. Each password is generated using the current time and can be only used once based on the function of the SM3 Hash Algorithm. This proposed scheme can be further improved to enhance network security. Moreover, applied multifactor authentication by using textual password authentication from server to user, then from user to server [36]. This approach provides users with anonymous identity, mutual authentication, surveillance against cyberattacks, and session key compliance in a multi-server environment.

2) Graphical password authentication: Graphical password authentication is more difficult to circumvent than biometric authentication, is more user-friendly, has easy-to-remember passwords, and provides high-level security [34][55]. The image-based authentication system is the main type of graphical password authentication [56]. This authentication method is based on recognition and recall approaches. Although this authentication method is highly secure, the ability to remember the password plays an important role. Songcuan et al. further mentioned that used graphical password authentication in an experimental study measuring students' memory ability, speed of registration, and speed of authentication [39]. The results recorded 100% successful password memory in the first session and 90.90% in the second session. There is a decrease in memory percentage because the second session took place after two weeks of delay. Hence, these findings prove that memorability plays a huge role in this type of authentication. A survey on graphical password authentication using images as passwords was conducted [22] and found that the memorability of graphical passwords was better than that of textual passwords. The authors noted that graphical password technology was still immature; hence more research is needed to achieve a higher level of usefulness.

- Biometric authentication

The security of biometric identification depends on body patterns such as fingerprints or facial features [57]. This type of authentication has the uniqueness derived from a human body [58]. Biometric authentication has been increasingly used as it provides a more secured process of identifying users [44]. Biometric authentication methods are more likely to be convenient, secure, and strong used compared with traditional authentication methods [59]. This section discusses fingerprint, facial feature, retina/iris, voice, and digital signature authentication.

3) *Fingerprint authentication:* In the protocol proposed by Zhu et al. [44], the first two modules of this scheme can be classified into enrolment and authentication phases. These two phases enable data to be protected better rather than in a one-step login phase and provides higher resistance against some possible threats. Moreover, ArunPrakash et al. [20] said that personal data stored in cloud computing can be protected because authentication can be completed only when the fingerprint encryption matches the enrolment phase data. This way, it is impossible for any harmful cyber threats to occur. Besides, they proposed a scheme for mobile banking application users to apply an efficient and privacy-preserving biometric identification outsourcing scheme in mobile banking applications [31]. This study suggested using a multibiometric system for a more significant variability.

4) *Facial authentication:* Musambo and Phiri [29] have proposed a facial authentication scheme for university students. It was found that the system only obtained 66% detection rate. This was due to the lighting conditions when the images are captured and the complexion of students' face. Another researcher also proposed a facial authentication scheme to be used in online banking services [18]. The proposed scheme can deny access for unauthorized usage and determines ways to identify different testing images. Ten different images were taken from the same user. The results of authentication accuracy were 97.50% from the first image. In the second image, a result of 100% successful authentication was achieved.

5) *Iris/Retina authentication:* Retina authentication provides unique biometric structure, shape, and specified image specification, and it has one of the longest lifespans of biometric data. A user who authenticates by this method even with glasses or contact lens will still be able to effectively use this process. However, this authentication method may not be well received by cloud computing users. This is because this form of authentication has not been widely practiced and expensive [29]. A multifactor authentication combining fingerprint and iris was formulated [24]. They used a qualitative methodology to enhance the authenticating system for cloud computing users by using finger vein and iris authentication. Their results showed that the finger vein's biometric template cannot be duplicated; hence, this methodology can strengthen security systems compared with other authentication methods.

TABLE III. LAYER(S) OF AUTHENTICATION OF THE ARTICLES SELECTED TO BE REVIEWED

No	Title of article	Layer(s) of authentication	References	Subject
1	A Smooth Textual Password Authentication Scheme Against Shoulder Surfing Attack	*Password authentication* Textual-based	[17]	Textual password users
2	Research And Implementation of Time Synchronous Dynamic Password Based on Sm3 Hash Algorithm	*Password authentication* Textual-based	[38]	Internet users
3	An Empirical Study Examining the Perceptions and Behaviours of Security-Conscious Users of Mobile Authentication	*Password authentication* Textual-based	[41]	20 IT mobile users
4	Encouraging Users to Improve Password Security And Memorability	*Password authentication* Textual-based	[43]	Text-based password users
5	Graphical Password Authentication – Survey	*Password authentication* Graphical	[22]	Computer users
6	Towards Usability Evaluation of Jumbled PassSteps	*Password authentication* Graphical	[39]	30 students from Don Mariano Marcos Memorial State University
7	Biometric Encoding and Biometric Authentication (Beba) Protocol For Secure Cloud in M-Commerce Environment	*Biometric authentication* Fingerprint	[20]	Cloud users

8	Hand-Based Biometric Recognition Technique – Survey	*Biometric authentication* Hand-based	[31]	Mobile banking application users
9	An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing	*Biometric authentication* Fingerprint	[44]	Cloud computing users
10	Edge-Centric Multimodal Authentication System Using Encrypted Biometric Templates	*Biometric authentication* Facial	[18]	Cloud computing users
11	Student Facial Authentication Model Based on Open Cv's Object Detection Method and Qr Code For Zambian Higher Institutions of Learning	*Biometric authentication* Facial	[43]	3000 students in University of Zambia
12	A Method For User Authenticating to Critical infrastructure Objects Based on Voice Message Identification	*Biometric authentication* Voice	[40]	Cloud computing users
13	Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data	*Multifactor authentication* Biometric (digital signature & fingerprint)	[19]	Patients in medical sector
14	Accomplishment of New Protocol for Stupendous Security in Cloud Environment	*Multifactor authentication* Biometric (fingerprint) & password (textual)	[21]	Cloud computing users (30 different fingerprint with eight different repetitive to compare results)
15	Multi-Biometric Authentication System Using Finger Vein and Iris in Cloud Computing	*Multifactor authentication* Biometric (fingerprint & iris)	[24]	Cloud computing users
16	Cloud Service Security Using Two-Factor or Multi Factor Authentication	*Multifactor authentication* Biometric (digital signature) & password)	[25]	Smartphone users
17	Multifactor Authentication Protocol in a Mobile Environment	*Multifactor authentication* Biometric (fingerprint) & password (login key)	[27]	200 Android users
18	Securing Personal Health Records Using Advanced Multi-Factor Authentication in Cloud Computing	*Multifactor authentication* Password (textual) & biometric (digital signature & iris)	[35]	Patients in hospital
19	Multi-Layered Multimodal Biometric Authentication for Smartphone Devices	*Multifactor authentication* Biometric (fingerprint, facial & voice)	[42]	Smartphone users
20	Access Control Framework Using Multi-Factor Authentication in Cloud Computing	*Multifactor authentication* Biometric (fingerprint) & password (textual & login key)	[30]	Cloud computing users
21	New Robust Biometrics-Based Mutual Authentication Scheme With Key Agreement Using Elliptic Curve Cryptography	*Multifactor authentication* Biometric (fingerprint) & password (login key)	[33]	Single-client server application in mobile environment
22	Anonymous Biometrics-Based Authentication With Key Agreement Scheme for Multi-Server Environment Using Ecc	*Multifactor authentication* Biometric (fingerprint) & password (login key)	[32]	Multi-server environment using ECC
23	Research and Development of User Authentication Using Graphical Passwords: A Prospective Methodology	*Multifactor authentication* Password (Textual & graphical)	[34]	Cloud computing users
24	An Improved and Secure Two-Factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment	*Multifactor authentication* Password (server to user & user to server)	[36]	Multi-server environment
25	I-Voting on Cloud Framework	*Multifactor authentication* Biometric (fingerprint & facial) & password (login key)	[23]	Internet voting platform users
26	Analysis of information Security Service for Internet Application	*Multifactor authentication* Biometric (fingerprint) & password (login key)	[37]	Internet application users
27	A Highly Secure Multi- Factor Authentication System Using Biometrics to Enhance Privacy in Internet of Things (IoT)	*Multifactor authentication* Password (textual & login key) & biometric (palm print)	[26]	Internet users
28	Privacy Preserving Biometric Authentication and Identification in Cloud Computing	*Multifactor authentication* Password (login key) & biometric (fingerprint)	[42]	Cloud computing users

6) Voice authentication: Voice authentication is a conversion of a human voice into an electrical signal that can be digitally coded to recognize a user from the coded voice data [60]. People usually speak faster than they write; hence, voice authentication can be considered a time-preserving method. Memon [28] proposed a multifactor biometric authentication including fingerprint, face, and voice for smartphone users. He found that this biometric used in smartphones is more robust and secure compared with single-layered biometric. Additionally, Trysnyuk et. al. [40] proposed a voice message identification method to improve the standard password authentication. It was found that the security of this method can be enhanced by applying another layer of password or biometric authentication.

7) Digital signature authentication: Digital signature is a behavioral biometric which has high acceptance rate and ease in data collection [28]. Digital signature is less cumbersome compared with handwritten signature. It was suggested that a multifactor authentication model was used based on digital signature and password [25]. However, this study found the scheme can only be applied for a small proportion of users. In addition, digital signature was also implemented in a health care system with fingerprint verification [19]. As proposed, the signature verification process has several steps. The main purpose of this signature authentication is to protect patients' health record and to avoid misplacing of their personal data. It was found that the patient's information was highly secured as it increases the system performance rate compared to single-factor authentication. Moreover, combined password, iris verification, and digital signature in their authentication scheme is needed to secure health care records [35]. This scheme comprises key generation and signature encryption stage. The key generation stage creates random number combinations to be used as a private key. Iris features are used because of clear-cut texture of the cornea. This study results show that the multifactor authentication method provides security and confidentiality to health care records. The authors suggested the use of hybrid technologies in the future to enhance health care data security.

- Multiple-factor authentication

Multiple-factor authentication involves two or more phases of authentication and is widely used because it increases the mechanism of data protection compared with single factor authentication. The authors in [27] [37] used two-factor authentication in their proposed scheme combining password verification and fingerprint authentication. Password identification comprises of OTP and secret question, whereas fingerprint authentication is required as a second factor to verify the user's identity. The system will accept or reject authentication based on the fingerprint received during each authentication process. Besides, a scheme using two-factor authentication for the password change process is also proposed [36]. This verification process is a two-way; server to user and user to server. This two-way authentication gives a protected multi-server environment. Another researcher proposed a three-factor authentication (3FA) scheme to be used in a mobile banking environment among 200 Android users [37]. The OTP received must be typed correctly in the provided field and biometric authentication is then used to activate the account with fingerprint access. The authors found that two-factor authentication makes a cloud environment more robust. The concept of mutual authentication scheme key agreement in a single-server environment has been implemented to improve the security [33] [61]. Qi and Chen [32] then introduced an approach through implementation of BAN logic. This project aimed to provide a new method based on mutual authentication that allows use of the same session key. Both studies involve multifactor authentication of fingerprint and textual authentication. Furthermore, Reshma and Shivaprasad [34] combined textual and graphical authentication to provide a better authentication system for cloud computing users and to avoid data breaches. Besides, Balaji and Saravanakumar [21] presented a biometric method using thirty different fingerprints with eight different repetitions along with textual authentication. The results show that the scheme reduces false rejection rate and false acceptance rate.

Then, Yellamma et al. [42] proposed a biometric scheme with registration and verification processes by designing a new coding rule to prevent hackers from attacking the cloud environment. The findings show that the scheme provides higher security from malicious attacks. Moreover, Patel et. al. [30] suggested an authentication model consisting of fingerprint, facial, PIN, and OTP. The results of study were disrupted due to the delay in OTP receiving. This study later suggested improving the method of biometric collection for future studies and the availability of mobile network to effectively receive the OTP. Additionally, Sathishkumar et al. [23] designed an authentication model for online voting. The authentication mode involves fingerprint, facial, and OTP. The advantages of using this proposed voting framework are that the frequency of voting is higher but fewer personnel are required. It is hoped to facilitate a fairer voting system that allows more people to practice their voting rights. Besides, Qi and Chen [33] proposed an authentication consisting of palm print, four-digit user password, and OTP. The results show that this method functions well and provides a lower false rejection ratio. The study aims to work more on the combination of multi-biometric scheme.

V. Conclusion

Based on the discussion above, the summary of the types of authentications reviewed in this paper is presented below (as shown in Figure 3.) Previously, much of the authentication was created based on traditional password i.e. using textual. With the advances in technology, a value can be added to the password authentication by using biometric data, which led to multifactor authentication and a more secure cloud environment. Thus, with the multilayer authentication, it is difficult for hackers to attack the system, especially related to the use of passwords. Further, more awareness on authentication is needed among Internet users to help create a secure online environment. In future, different biometric authentication methods can be combined for greater key encryption, which improves information security. Biometric authentication should also be used whenever there is in need for higher security. OTP can be used to increase surveillance and safety templates, as it changes on the device with each use. In addition, information security awareness should be taught to users so that they know how to safely access the Internet. Future research should combine authentication methods in large-scale studies and increase the sample size for better results. It is also recommended that future studies evolve in a multi-server environment. This systematic review also concluded that no study was done to examine the types of authentication methods being used in Malaysia among Internet users. Most of the studies were found to be in India, China, countries from Middle East, and Europe. Research about authentication method used in Malaysia is highly recommended. This is because Malaysia is one of the leading communication technology countries with almost 89% of its population which is equivalent to 25.4 million Internet users. Future research can propose a secure authentication scheme according to the suitability of subjects of study. We hope this study can provide cloud users with increased awareness of the types and importance of authentication.

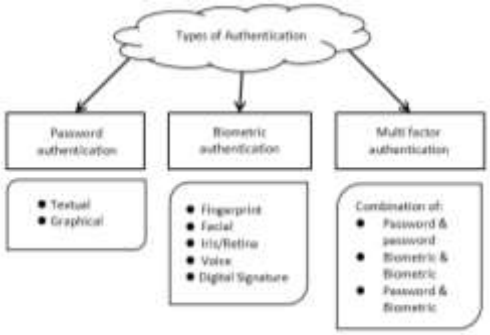

Fig. 3. Summary of Authentication Types.

ACKNOWLEDGMENT

This research was supported by Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2018/SS09/UPM/02/1/5540161), Project Code 05-01-18-2036FR.

REFERENCES

[1] MyCERT, *Incident Statistics. Reported Incidents Based on General Incident Classification Statistics*, 2021. Available online: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228 (accessed on 24 March 2021).

[2] Omar, Siti Zobidah, Raidah Mazuki, Jusang Bolong, Jeffrey Lawrence D'Silva, and Hayrol Azril Mohamed Shaffril, "Pattern of Internet Usage at the Rural Library among Rural Youth in Malaysia," *Mediterranean Journal of Social Sciences*, vol. 7, 2016.

[3] Segura-Robles, Adrián, Antonio-José Moreno-Guerrero, María-Elena Parra-González, and Jesús López-Belmonte, "Review of Research Trends in Learning and the Internet in Higher Education," *Social Sciences*, vol. 9, no. 6, pp. 101, 2020.

[4] Akingbade, Luisa, "Cloud storage problems, benefits and solutions provided by data de-duplication," *International Journal of Engineering and Innovative Technology*, vol. 5, no. 6, pp. 70-77, 2016.

[5] Ungurean, Ioan, and Nicoleta Cristina Gaitan, "Software Architecture of a Fog Computing Node for Industrial Internet of Things," *Sensors*, vol. 21, no. 11, pp. 3715, 2021.

[6] Jain, Anil, Arun Ross, and Salil Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, pp. 4-20, 2004.

[7] Kadam, Yashpal, "Security Issues in Cloud Computing A Transparent View," *International Journal of Computer Science Emerging Technology*, vol. 2, pp. 316-322, 2011.

[8] Pitchan, Muhammad Adnan, Siti Zobidah Omar, Jusang Bolong, and Akmar Hayati Ahmad Ghazali, "Amalan Keselamatan Siber Pengguna Internet Terhadap Buli Siber, Pornografi, E-Mel Phishing Dan Pembelian Dalam Talian," *Jurnal Komunikasi: Malaysian Journal of Communication*, vol. 35, pp. 212–227, 2019.

[9] Bishop, Matt, Essay. *In Computer Security: Art and Science*. Boston: Addison-Wesley, 2012.

[10] Lal, Nilesh A, Salendra Prasad, and Mohammed Farik, "A review of authentication methods," *International Journal of Scientific & Technology Research*, vol. 5, pp. 246-249, 2016.

[11] Pitchan, Muhammad Adnan, Siti Zobidah Omar, Jusang Bolong, and Akmar Hayati Ahmad Ghazali, "Analysis of Cyber Security from the Perspective of Social Environment: A Study of Internet Users in Klang Valley," *Journal of Social Sciences and Humanities*, vol. 12, pp. 16-29, 2017.

[12] Brandao, Pedro Ramos, "The Importance of Authentication and Encryption in Cloud Computing Framework Security," *International Journal on Data Science and Technology*, vol. 4, no. 1, pp. 1-5, 2018.

[13] Vouk, Mladen A, "Cloud Computing - Issues, Research and Implementations," *Journal of Computing and Information Technology*, vol. 16, no. 4, pp. 235-246, 2008.

[14] Petrosino, Anthony, Robert F. Boruch, Haluk Soydan, Lorna Duggan, and Julio Sanchez-Meca, "Meeting the Challenges of Evidence-Based Policy: The Campbell Collaboration," *The ANNALS of the American Academy of Political and Social Science*, vol.578, no. 1, pp. 14-34, 2001.

[15] Baumeister, Roy F, "*Writing a Literature Review*," In The portable mentor: Expert guide to a successful career in psychology. Edited by Mitchell J Prinstein. North Carolina, USA: Springer, pp. 119-132, 2013.

[16] Sa'di, Mustapa Mursilalaili, Abdul Rani Kamarudin, Duryana Mohamed, and Zulfakar Ramlee, "Authentication of electronic evidence in cybercrime cases based on Malaysian laws," *Pertanika Journal of Social Science and Humanities*, vol. 23, pp. 153-168, 2015.

[17] Al-Husainy, Mohammed A. Fadhil, and Diaa M. Uliyan, "A Smooth Textual Password Authentication Scheme Against Shoulder Surfing Attack," *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 9, pp. 2546-2556, 2018.

[18] Ali, Zulfiqar, M. Shamim Hossain, Ghulam Muhammad, Ihsan Ullah, Hamid Abachi, and Atif Alamri, "Edge-Centric Multimodal Authentication System Using Encrypted Biometric Templates," *Future Generation Computer Systems*, vol. 85, pp. 76-87, 2018.

[19] Amirthalingam, Gandhimathi, and Harrin Thangavel, "Multi-Biometric Authentication Using Deep Learning Classifier for Securing of Healthcare Data," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, pp. 1340–1347, 2019.

[20] ArunPrakash, R., T. Jayasankar, and K. Vinothkumar, "Biometric Encoding and Biometric Authentication (Beba) Protocol for Secure Cloud in M-Commerce Environment," *Applied Mathematics & Information Sciences*, vol. 12, no. 1, pp. 255-263, 2018.

[21] Balaji, S, and S Saravanakumar, "Accomplishment of New Protocol for Stupendous Security in Cloud Environment," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 2616-2619, 2019.

[22] Bhootwala, Jasmin P., and Pravin H. Bhathawala, "Graphical Password Authentication - Survey," *Global Journal For Research Analysis*, vol. 9, no. 2, pp. 31-35, 2020.

[23] D, Sathishkumar, SureshAnand M, JeganAmarnath J, SangeeraniDevi A, and Gurusubramani S. "I-Voting on Cloud Framework," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1S, pp. 61-64, 2019.

[24] Ilankumaran, S., and C. Deisy, "Multi-Biometric Authentication System Using Finger Vein and Iris in Cloud Computing," *Cluster Computing*, vol. 22, no. S1, pp. 103-117, 2018.

[25] Luckose, Jubin, Sameer Chindarkar, and Dhanamma Jagli, "Cloud Service Security using Two-factor or Multi factor Authentication," *International Research Journal of Engineering and Technology*, vol. 4, pp. 2066-2070, 2017.

[26] M, Vijay, and Indumathi G, “A Highly Secure Multi- Factor Authentication System Using Biometrics to Enhance Privacy in Internet of Things (IOT),” *International Research Journal of Multidisciplinary Technovation*, vol. 1, no. 6, pp. 26-34, 2019.

[27] Maciej, Bartlomiejczyk, El Fray Imed, and Miroslaw Kurkowski, “Multifactor Authentication Protocol in a Mobile Environment,” *IEEE Access*, vol. 7, pp. 157185–157199, 2019.

[28] Memon, Qurban A, “Multi-Layered Multimodal Biometric Authentication for Smartphone Devices,” *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 15, pp. 222, 2020.

[29] Musambo, Lubasi Kakwete, and Jackson Phiri, “Student Facial Authentication Model Based on OpenCV’s Object Detection Method and QR Code for Zambian Higher Institutions of Learning,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, pp. 88-94, 2018.

[30] Patel, Subhash Chandra, Sumit Jaiswal, Ravi Shankar Singh, and Jyoti Chauhan, “Access Control Framework Using Multi-Factor Authentication in Cloud Computing,” *International Journal of Green Computing*, vol. 9, no. 2, pp. 1-15, 2018.

[31] Prihodova, Katerina, and Miloslav Hub, “Hand-Based Biometric Recognition Technique – Survey,” *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 6, pp. 689–698, 2020.

[32] Qi, Mingping, and Jianhua Chen, “Anonymous Biometrics-Based Authentication with Key Agreement Scheme for Multi-Server Environment Using ECC,” *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27553–27568, 2019.

[33] Qi, Mingping, and Jianhua Chen, “New Robust Biometrics-Based Mutual Authentication Scheme with Key Agreement Using Elliptic Curve Cryptography,” *Multimedia Tools and Applications*, vol. 77, no. 18, pp. 23335–23351, 2018.

[34] Reshma, and Shivaprasad G., “Research and Development of User Authentication Using Graphical Passwords: A Prospective Methodology,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9S3, pp. 385–390, 2019.

[35] S, Meena, and Gayathri V., “Securing Personal Health Records Using Advanced Multi-Factor Authentication in Cloud Computing,” *International Journal of Recent Technology and Engineering*, vol. 8, no. 6, pp. 5133–5140, 2020.

[36] Sahoo, Shreeya Swagatika, Sujata Mohanty, and Banshidhar Majhi, “An Improved and Secure Two-Factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment,” *Wireless Personal Communications*, vol. 101, no. 3, pp. 1307–1333, 2018.

[37] Shanker, Ravi, Sahil Verma, and Kavita, “Analysis of Information Security Service for Internet Application,” *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 58-62, 2018.

[38] Silue, Dognery Sinaly, Wanggen Wan, and Muhammad Rizwan, “Research and Implementation of Time Synchronous Dynamic Password Based on SM3 Hash Algorithm,” *Open Journal of Applied Sciences*, vol. 6, no. 13, pp. 893–902, 2016.

[39] Songcuan, Jerome P., Ariel M Sison, Ruji Medina, “Towards Usability Evaluation of Jumbled PassSteps,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, pp. 1032–1037, 2019.

[40] Trysnyuk, Vasyl, Yevhen Nagornyi, Kirill Smetanin, Igor Humeniuk, and Tetyana Uvarova, “A Method For User Authenticating To Critical Infrastructure Objects Based On Voice Message Identification,” *Advanced Information Systems*, vol. 4, no. 3, pp. 11-16, 2020.

[41] Wolf, Flynn, Ravi Kuber, and Adam J Aviv, “An Empirical Study Examining the Perceptions and Behaviours of Security-Conscious Users of Mobile Authentication,” *Behaviour & Information Technology*, vol. 37, no. 4, pp. 320-334, 2018.

[42] Yellamma, Pachipala, Rajesh P.S.S., Pradeep V.V.S.M., Manishankar Y.B., “Privacy Preserving Biometric Authentication and Identification in Cloud Computing,” *International Journal of Advanced Science and Technology*, vol. 29, pp. 3087-3096, 2020.

[43] Yildirim, M., and I. Mackie, “Encouraging Users to Improve Password Security and Memorability,” *International Journal of Information Security*, vol. 18, no. 6, pp. 741–759, 2019.

[44] Zhu, Liehuang, Chuan Zhang, Chang Xu, Ximeng Liu, and Cheng Huang, “An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing,” *IEEE Access*, vol. 6, pp. 19025–19033, 2018.

[45] Page, Matthew, Joanne McKenzie, Patrick Bossuyt, Isabelle Boutron, Tammy Hoffmann, Cynthia Mulrow, Larissa Shamseer, et al., “The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews,” *PLOS Medicine*, vol. 18, no. 3, pp. e1003583, 2021.

[46] Meier, Kennedy, Jacqueline Parrish, and Rohan D'Souza, “Prediction Models for Determining the Success of Labor Induction: A Systematic Review,” *Acta Obstetricia et Gynecologica Scandinavica*, vol. 98, no. 9, pp. 1100–1112, 2019.

[47] Wolff, Robert F., Karel G.M. Moons, Richard D. Riley, Penny F. Whiting, Marie Westwood, Gary S. Collins, Johannes B. Reitsma, Jos Kleijnen, and Sue Mallett, “PROBAST: A Tool to Assess the Risk of Bias and Applicability of Prediction Model Studies,” *Annals of Internal Medicine*, vol. 170, no. 1, pp. 51-58, 2019.

[48] Abuarqoub, Abdelrahman, “D-FAP: Dual-Factor Authentication Protocol for Mobile Cloud Connected Devices,” *Journal of Sensor and Actuator Networks*, vol. 9, no. 1, pp. 1-23, 2019.

[49] Lalitha, Krishnan, Subramanian Vaithyasubramanian., K Vengatakrishnan, A Christy, and M Metilda, “A Novel Authentication Procedure for Secured Web Login Using Coloured Petri Net,” *International Journal of Simulation: Systems, Science & Technology*, vol. 19, 2019.

[50] Shin, Sanggyu, and Yoichi Seto, “Security improvement of biometric authentication systems at cancelable biometrics,” *Information (Japan)*, vol. 19, pp. 505-513, 2016.

[51] Thakur Priyanka, Ravishanker, and Ashish K Luhach, “Personal data access control based on trust and reputation in cloud computing,” *International Journal of Control Theory and Applications*, vol. 9, pp. 5263-5270, 2016.

[52] Yoshida, Atsumasa, “The measures applied internally by the NEC Group to forestall and prevent cybersecurity incidents,” *NEC Technical Journal*, vol. 12, pp. 29-33, 2018.

[53] Curran, Kevin, Jonathan Doherty, Ayleen McCann, and Gary Turkington, “Good Practice for Strong Passwords,” *The EDP Audit, Control, and Security Newsletter*, vol. 44, no. 5, pp. 1-13, 2011.

[54] Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon, “Authentication Using Graphical Passwords,” in *Proceedings of the 2005 symposium on Usable privacy and security - SOUPS '05*, vol. 93, pp. 1-12, 2005.

[55] Fong, Teoh Joo, Azween Abdullah, N. Z. Jhanjhi, and Mahadevan Supramaniam, “The Coin Passcode: A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices,” *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 1, pp. 302-308, 2019.

[56] Al-Husainy, Mohammed A. Fadhil, and Raghda Ahmed Malih, “Using Emoji Pictures to Strengthen the Immunity of Passwords against attackers,” *European Scientific Journal*, vol. 11, no. 30, pp. 153-165, 2015.

[57] Hodge, Edwin, Helga Hallgrimsdottir, and Marianne Much, “Performing Borders: Queer and Trans Experiences at the Canadian Border,” *Social Sciences*, vol. 8, no. 7, 2019.

[58] Bharadi, Vinayak Ashok, “Texture Feature Extraction For Biometric Authentication using Partitioned Complex Planes in Transform Domain,” *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 2, no. 1, pp. 39-46, 2012.

[59] Jain, Anil, Lin Hong, and Sharath Pankanti, “Biometric identification,” *Communications of the ACM*, vol. 43, pp. 90-98, 2000.

[60] Tripathi, K P., “A Comparative Study of Biometric Technologies with Reference to Human Interface,” *International Journal of Computer Applications*, vol. 14, no. 5, pp. 10-15, 2011.

[61] Chaudhry, Shehzad Ashraf, Husnain Naqvi, and Muhammad Khurram Khan, “An Enhanced Lightweight Anonymous Biometric Based Authentication Scheme for TMIS,” *Multimedia Tools and Applications*, vol. 77, no. 5, pp. 5503–5524, 2018.