SOCIAL MEDIA USER AUTHENTICATION TECHNIQUES

Pratheep V, Dhanush S R, Jayanth Kumar

Dept of Computer Science Engineering(Btech)

School of Computer Science Engineering(SCOPE VIT)

ABSTRACT:

In the digital age of social media, user authentication has emerged as a critical concern due to the widespread adoption of online platforms and the increasing threat of security breaches. Traditional authentication methods, such as passwords and two-factor authentication (2FA), suffer from vulnerabilities such as weak passwords, phishing risks, and social engineering attacks. This research paper addresses these pressing issues and proposes a novel solution to enhance social media user authentication. By integrating biometric authentication, leveraging unique physical and behavioral characteristics like fingerprints and facial features, alongside multifactor authentication (MFA) that combines multiple verification methods, the proposed approach strengthens the security and reliability of user authentication. Additionally, this paper explores the significance of safeguarding against social engineering attacks, as they pose a significant risk to user authenticity and privacy on social media platforms.

KEYWORDS:

Social Media, User Authentication, Biometric Authentication, Multifactor Authentication, Security, Social Engineering, Online Platforms.

INTRODUCTION

In the era of digital connectivity, social media platforms have become an integral part of our daily lives, transforming the way we communicate, share information, and build relationships. However, with the widespread adoption of social media comes the increasing concern over user authenticity and security. Authenticity refers to the trustworthiness and genuineness of social media users, ensuring that they are who they claim to be, while security entails protecting users from various threats such as identity theft, hacking, and unauthorized access to personal information. Celebrities and causal user's social media accounts were hacked and many dubious activites has been done using their name .User verification is a critical aspect of ensuring the authenticity and security of online platforms.

Multi-modal biometric authentication systems combine two or more biometric traits for user identification and verification.

Enhanced Security: Multi-modal biometrics improve security by combining multiple biometric traits, making it much more difficult for attackers to forge or spoof the authentication process. This reduces the risk of false positives and ensures a higher level of confidence in the user's identity.

- Accuracy and Reliability: Each biometric trait has its strengths and weaknesses. By using multiple biometric modalities, the system can compensate for the limitations of individual traits, resulting in increased accuracy and reliability.
- Lower False Rejection Rate (FRR): Utilizing multiple biometric factors can reduce the chances of false rejections. If one biometric fails to be recognized due to external factors (e.g., poor lighting for facial recognition), the system can fall back on another modality (e.g., fingerprint) to authenticate the user.
- User Convenience: Multi-modal biometrics can offer a more seamless user experience by allowing individuals to choose from several authentication methods. Users may find it more convenient to authenticate using a combination of modalities they are comfortable with.

This research aims to explore the significance of user authenticity on social media and proposes a novel user verification system that combines cutting-edge technologies such as Facial recognition and Hand gesture to create a robust and user-friendly muti-modal biometric system solution.

LITERATURE REVIEW

1.In the modern internet era, concerns about third-party involvement in data management have increased, particularly with the prevalence ofcloud environments. Anonymity, data maintenance, and confidentiality issues have become critical. To addressthese challenges, Searchable Encryption (SE) has emerged as a promising solution, allowing secure browsing ofencrypted data. However,

existing SE schemes often lack multi-factor authentication and verification, posingsecurity risks. In response, researchers proposed the Time-Based One-Time Password and Verification inKey-Aggregate Searchable Encryption (TOTPV-KASE) scheme. This innovative approach incorporatestime-based one-time passwords generated by the data owner and validates them using the Inter Planetary FileSystem (IPFS) for enhanced security. The TOTPV-KASE scheme aims to safeguard confidential data, providingefficient and secure data access through searchable encryption, thus advancing data security in the era ofthird-party involvement and cloud-based management.

2.An authentication protocol for secure remotereal-time monitoring of patients in healthcare using Cloud-IoT networks. The protocol incorporates three-factor MP authentication (password, biometrics, and smartcard verification), mutual authentication between the MP and cloud server, and the establishment of a secure shared session key.Key freshness is maintained to prevent replay attacks. The protocol achieves high security levels while minimizing computation and communication costs, requiring only two message exchanges between the MP and cloud server. Formal analysis, security assessment, and performance evaluationusing AVISPA web tool confirm its effectiveness against potential attacks. The research highlights the protocol's viability for efficient and secure healthcare services in a centralized system, leveraging the benefits of cloud computing and IoT in the healthcare sector.

3.Haider Mehraj(2021) explores the security challenges and privacy concerns associated with the widespread use of Social Networking Sites (SNS). The research identifies various security risks, including account hacking, identity theft, and data breaches, as cyber attackers exploit the vast amount of personal information shared on these platforms. The application of the Protective Motivation Theory (PMT) in understanding users' online safety intentions has been studied, emphasizing the importance of factors such as behavioral strength and individual responsibility. Multi-Factor Authentication (MFA) is proposed as a robust alternative to traditional password-based methods to enhance SNS security. User privacy behavior is also examined, as many users unwittingly share personal information, necessitating better security controls and user education. The popularity of SNS and their vulnerabilities require ongoing research and education to safeguard users' digital identities effectively. The review concludes with the importance of enhanced authentication methods for account recovery, utilizing trusted friends for secure confirmation processes.

4.Muhammad Sajjad's (2019) hybrid biometric recognition and anti-spoofing system combines fingerprint, palm vein print, and face recognition modalities with CNN-based anti-spoofing models. While related research has explored individual aspects of this system, the specific combination described in the abstract appears to be a unique contribution. Such multi-modal biometric systems have been studied to enhance security and accuracy, utilizing fusion techniques from different sources for reliable authentication. This novel approach may lead to more robust and secure biometric authentication systems, surpassing traditional single-modal methods

5. Arunava Roy & Dipankar Dasgupta (2017) propose a novel framework for active authentication, aiming to improve user identification and security. The approach includes various authentication modalities, such as stylometry, web-browsing behavior, screen fingerprints, and behavioral biometrics (keystroke and mousedynamics). By intelligently selecting multiple modalities based on the operating environment, application types, and communication modes, the framework enhances device and online application security effectively. It addresses potential drawbacks and aims to achieve scalable and robust authentication accuracy. This approach allows continuous monitoring and validation of users through diverse means, including physical aspects, user behavior with systems, context analysis, and expert data usage. The ultimate goal is to identify malicious users and detect deceptive writing while ensuring a seamless and secure user experience

6. Bhawna Narwal, Amar Kumar Mohapatra proposed that Wireless Body Area Networks (WBAN) have revolutionized the healthcare industry, enabling remote monitoring of patients through wearable or implantable sensors. However, the sensitive nature of patient data poses security threats. To ensure widespread adoption,robust security and authentication mechanisms are vital. A systematic review examines WBAN security essentials, threats, attackers, and existing solutions, providing a comprehensive understanding. Authentication schemes are explored in detail, including their design, strengths, limitations, and verification techniques. WBAN applications span medical and non-medical fields, with advantages such as real-time health monitoring andpersonalized treatment options. Nonetheless, privacy and security challenges persist, necessitating future research to develop secure and privacy-preserving authentication solutions.

7. Wong et al. (2006) introduced a lightweight user authentication protocol for wireless sensor networks (WSNs),but it suffered from security issues. Subsequent

researchers proposed various improvements, each facingvulnerabilities. To address these shortcomings, the proposed scheme by Wong et al. uses the Rabin cryptosystemfor public-key technology, achieving multi-factor security, forward secrecy, and user anonymity in IndustrialInternet of Things (IIoT) systems. The authors conducted both formal and heuristic security analyses to validateits robustness compared to existing schemes. The proposed solution seeks to strike a balance between securityand efficiency, presenting a practical approach for IIoT authentication and privacy challenges.

8. The Internet of Things (IoT) has transformed object connectivity, leading to intelligent identification and management. Wireless Sensor Networks (WSNs) play a crucial role in various fields like smart healthcare and transportation. However, ensuring data security in WSNs, particularly in Wireless Medical Sensor Networks (WMSNs), has become vital. Existing authentication protocols for WMSNs suffer from limitations, leaving them vulnerable to attacks. To address this, a new ECC-based secure three-factor authentication protocol is proposed. It utilizes a fuzzy commitment scheme for secure biometric handling and integrates fuzzy verifier and honey_list techniques to enhance user verification. The protocol's effectiveness is evaluated using provable security, Proverif tool, and information analysis, showing promising results and establishing its robustness against existing protocols. This innovative approach enhances WMSN security, making future systems more secure and reliable

9. Obi Ogbanufe a, Dan J. Kim b aims to compare and understand individuals' perceptions and beliefs regarding different electronic payment authentication methods in an e-commerce context. The methods being comparedare credit card, credit card with PIN, and fingerprint biometrics authentication. The study uses the valenceframework to assess the individual's evaluation of benefit and risk concerning these payment methods. Throughexperiments, the study finds that biometrics authentication significantly influences individuals' securityconcerns, perceived usefulness, and trust in online stores. It highlights the importance of considering users' perceptions, concerns, and beliefs when implementing biometrics for electronic payments, as it is perceived as a safer and more convenient option compared to traditional methods. The paper provides valuable insights for promoting the use of biometrics authentication in electronic payment applications.

10. Hasini Gunasinghe and Elisa Bertino has presented a cutting-edge biometrics-based authentication system thatprioritizes user privacy, enabling seamless authentication with various service providers using mobile phones.Our solution operates without the need for identity providers' involvement in the transaction process. Theauthentication method leverages zero-knowledge proof of knowledge, combining a cryptographic identity tokenwith the user's biometric identifier and a secret for robust three-factor authentication. To achieve a unique, repeatable, and revocable biometric identifier from the user's biometric image, we utilize a state-of-the-art machine learning-based classification technique. This involves extracting essential features from the user's biometric image, ensuring a secure and reliable identifier generation process. Our implementation has resulted in a fully functional prototype of the proposed authentication solution. Through extensive evaluation on a public data set of face images, we have thoroughly examined its performance, security, and privacy aspects. The outcomes demonstrate the efficacy and reliability of our solution, solidifying its position as an innovative and privacy-conscious approach to biometrics-based authentication.

11. The migration from local to web applications has been a significant advancement in application software, supporting multi-user scenarios and resource sharing. Security is a vital aspect of web application development, including authentication, authorization, and data protection. Cloud computing, particularly the Software as a Service (SaaS) model, offers advantages in flexibility and scalability but introduces new security challenges. Cloud-based systems face risks related to data isolation, network communication, and loss of control over data. To safeguard data and infrastructures, remote user authentication plays a crucial role. Biometric authentication is considered reliable and can enhance security compared to traditional methods like passwords and tokens. However, privacy concerns arise from storing biometric data in the authentication server's database. To address this, various techniques like fuzzy templates and biometric encryption are used. The chapter presents a cloud system utilizing biometric authentication based on fingerprints and introduces a unique data fragmentation technique for enhanced data security on the cloud architecture. Future improvements include multimodal biometric access and the development of a web server application for user-side access without local software installation.

12. For a long time, user authentication relied on knowledge-based methods like PINs and passwords, but these have proven to be inadequate and vulnerable, especially on mobile devices. Mobile devices are susceptible to smudge attacks, and stolen devices can compromise critical applications and personal data. To address these security

concerns, novel authentication methods based on biometrics have been proposed, utilizing unique morphological features like fingerprints and iris. Continuous Authentication (CA) technology, in conjunction with Behavioral Biometrics (BB), has gained interest for its ability to continuously re-authenticate users during a session, providing additional security. This survey aims to comprehensively explore BB and CA technologies on mobile devices, including data collection methodologies, machine learning models, attack vectors, and defense techniques. The adoption of multimodal authentication and the balance between security and usability are crucial challenges to address. Additionally, the evaluation of biometric features' usability and end-users' technology acceptance determinants will contribute to improving the effectiveness and adoption of BB and CA technologies.

13.Identity theft rates have surged, with identity thieves leveraging advanced software and hardware to their advantage. The use of affordable crime tools makes it easier for them to commit identity theft and evade punishment. According to statistics, millions of individuals have become victims of identity theft, resulting in financial losses and reputational damage. Traditional prevention methods like password-based authentication have proven inadequate, leading to the development of new technologies, such as RFID blocking cards, to combat theft attempts. However, identity thieves quickly adapt to these technologies, necessitating the creation of a novel protection method. The main problem lies in people's lack of control over their bank accounts, leaving them vulnerable to large-scale theft once their identity is stolen. To address this, a proposed Biometric Lock Application aims to add an extra layer of security to banking apps using biometric authentication, allowing users to set spending limits and approve purchases with biometric confirmation. Despite some downsides like false negatives, this solution could provide better protection against identity theft.

14. The Internet of Things (IoT) encompasses various devices, including wearables, smartphones, and computers, equipped with embedded sensors and processors. These devices have become essential in people's lives due to their decreasing costs and increasing computational capabilities. The IoT offers numerous benefits and applications, revolutionizing various fields like smart homes, healthcare, and industry. However, the limited computing capacity of IoT devices hinders the implementation of sophisticated security measures, making them vulnerable to attacks from adversaries. Biometric recognition, which uses physical traits for identification, has emerged as an alternative to password-based authentication. Integrating biometrics into IoT systems can enhance security, but it also raises concerns about protecting biometric template data from being compromised. Existing research has explored biometric applications in IoT but lacks comprehensive coverage of biometric data protection and biometric-cryptography. This review paper addresses this gap, presenting a comprehensive overview of contemporary biometric-based systems that focus on authentication and encryption for IoT security. The paper identifies challenges, provides potential solutions, and discusses future research directions for improving biometric authentication and encryption in IoT applications.

15. Biometric recognition involves automatically identifying individuals based on their unique physical or behavioral traits. These traits can be categorized into physiological (e.g., fingerprint, face, iris) and behavioral (e.g., keystroke dynamics, voice, gait) characteristics. Biometrics provides a more secure and reliable way to authenticate individuals compared to traditional methods like passwords or PINs. The paper discusses various biometric techniques and their applications, including desktop PCs, smartphones, ATMs, computer networks, workstations, and smart cards. While no biometric system is entirely foolproof, each method has its advantages and limitations. The paper aims to explore different biometric technologies and algorithms for future development and to offer security researchers a comprehensive understanding of these systems. However, further research is needed to analyze multiple techniques and conduct a comparative study for more in-depth analysis and improvement in the security sector.

16. This article addresses the issue of algorithmic bias and fairness in biometric systems. Biometric technologies, which identify individuals based on unique physical or behavioral traits, have seen significant growth in various domains like border control, law enforcement, and national identity management. However, concerns have been raised about bias in these systems, particularly regarding demographic attributes. Algorithmic bias refers to significant differences in system operation for different demographic groups, resulting in privilege or disadvantage for certain individuals. The article provides an overview of biased biometric algorithms, surveys

existing approaches for bias estimation and mitigation, and discusses the potential social impact of biased systems. It emphasizes the need for large-scale studies and highlights the challenges in achieving fairness and transparency in algorithmic decision-making. The article suggests that proper assessment, transparency, accountability, and fairness definitions are essential for these systems, with potential legal provisions to regulate their use

17. In recent years, the rapid advancement of technology, particularly in cloud and network computing, has profoundly impacted the world. Users have embraced these technological developments to streamline operations, enhance efficiency, and conveniently store their confidential data in cloud-based applications and web programs. Unfortunately, this progress has also led to a surge in network attacks, weakening the security environment and making users more susceptible to viruses, Trojans, and password theft. As a response, user authentication has become a crucial requirement for safeguarding web-based applications. Traditional methods like passwords, fingerprints, and ID cards have limitations, prompting the need for multifactor authentication. To address this, the authors have introduced the MIMOS Unified Authentication Platform (Mi-UAP), a multimodal authentication system that offers users multiple login options for a frictionless and secure experience. The paper outlines the background, experimental environment, and analysis of user historical data to develop an automated selection of login methods for users. While the proposed approach demonstrates positive results in facilitating the authentication process, it does have limitations for new users without historical data and users who change their behavior over time. The team plans to deploy and experiment with the protocol in real-world scenarios and work on refining its complexity while enhancing the end-user experience.

18. Biometrics has become essential in security systems, employing image-based and signal-based methods to distinguish individuals based on behavioral or physical traits. Image-based systems encompass various biometric methods like iris recognition, face, and hand geometry, while signal-based systems include ECG and speaker identification. Iris recognition, finger vein, and ear recognition are considered reliable modalities. The paper proposes a multimodal biometric system using a score-level fusion method called CEWA. The system achieved high accuracy in authentication and plans to enhance security by adding speaker verification in the future. Challenges include data leakage and image quality degradation.

19. The digital world's complexity has made it challenging for institutions to balance user-friendly security solutions with high quality. Face recognition has emerged as a major player in cybersecurity, providing both convenience and accuracy. This technique utilizes computerized images or videos to identify and authenticate individuals. The process involves storing facial patterns in a database and matching them during subsequent attempts. Various face recognition techniques, such as Eigenfaces, Fisher faces, and Local Binary Pattern Histogram (LBPH), have been developed.

Eigenfaces relies on Principle Component Analysis (PCA) and uses pre-defined sample images (eigenfaces) for prediction. Fisher faces, based on Linear Discriminant Analysis (LDA), outperforms Eigenfaces in different environments and expressions. LBPH, a combination of histogram and local binary pattern, is highly efficient in texture and image labeling. Among the techniques, LBPH shows the highest accuracy of 80%, followed by Fisher Faces with 78% and Eigenfaces with 70%.

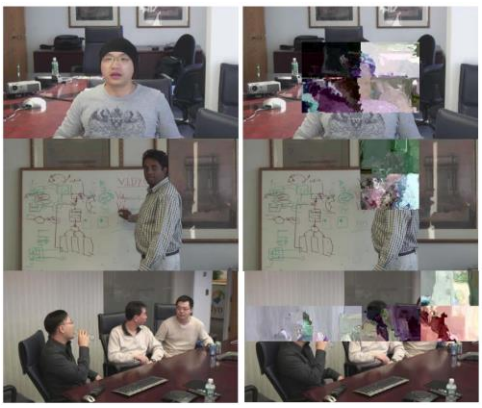
For secure communication between hosts, authentication and authorization are essential elements. Authentication involves verifying user credentials to determine if they are authorized to access the system. Authorization, on the other hand, grants access based on the user's position, determined after authentication. Geo-location is an efficient technique for both authentication and authorization. It associates geographical information, such as longitude and latitude, with data and restricts access based on the recipient's location. Combining face recognition and geo-location can create a robust algorithm for efficient authentication and authorization of data. The future of Geo-location in the security field appears promising.

20. The paper proposes a location-based authentication and authorization mechanism utilizing smart phones with GPS technology. Currently, passwords are commonly used for authentication, but their security is often compromised due to weak choices and reuse across services. To address this, multi-factor authentication, including what you know, what you have, and what you are (biometrics), has been implemented. The paper suggests incorporating user location as an additional factor. While existing location-based systems require specialized infrastructure and devices, smart phones with built-in GPS offer a feasible solution without

such constraints. They can accurately detect a user's location, making it suitable for authentication and authorization purposes. The advantages of this approach include utilizing existing mobile network infrastructure, not requiring specific devices, easy integration with existing systems, stable platforms for secure applications, and multiple location sensing technologies for better services.The proposed solution uses GPS technology for location-based authentication and authorization. It incorporates a hybrid approach for location verification, combining various technologies to enhance security. However, the paper acknowledges the potential to further improve security mechanisms by leveraging other contextual information from smartphones, such as proximity sensors and NFC technology.

21. In the modern age of information technology, ensuring secure identity verification has become crucial. Traditional methods like PINs and patterns have vulnerabilities, prompting the use of biometric techniques on smartphones for more reliable identification based on unique human traits. Iris recognition is considered one of the most dependable biometric methods for protecting sensitive data and applications. However, unimodal biometric systems like iris recognition have limitations, such as noisy sensor data and susceptibility to spoof attacks.To address these limitations, multimodal biometric systems are utilized, which combine more than one physiological or behavioral characteristic for enrollment, verification, or identification, improving system performance and reliability. This paper focuses on a multimodal eye biometric system that combines iris, pupil, and sclera features. Various multimodal biometric systems and their fusion methods were compared based on accuracy and equal error rate, with feature level fusion being proposed as the most suitable for the multimodal eye biometric system.The proposed eye biometric system utilizes entropy-based CNN for segmentation and features extracted through the color histogram algorithm and log Gabor filter. The fusion method chosen is feature level-based fusion, as it is expected to outperform score level and decision level fusion. By combining multiple biometric traits, the proposed system aims to enhance authentication accuracy and security in various environments.

22. This article shows a live HEVC video coding demonstration setup with Region of Interest (ROI) encryption. The highlighted The method divides video frames into separate HEVC tiles and encrypts those that relate to the ROI. This end-to-end content protection strategy is implemented by incorporating selected encryption techniques into the Kvazaar HEVC encoder and decryption methods into the openHEVC decoder. The demonstrated approach secures the ROI in real time while maintaining a low bit rate and complexity overhead.



23. Email has grown into one of the most used communication methods throughout the years most extensively utilised communication mediums for both individuals and organisations. Despite its near universal use in parts of the globe, existing information technology standards do not prioritise email security. Only lately have webmail providers like Yahoo Mail and Google Gmail begun to encrypt emails for privacy protection. The encrypted emails, on the other hand, will be decoded and kept on the service provider's servers. All saved emails can be read, copied, and edited if the servers are hostile or exploited. As a result, end-to-end (E2E) email encryption is critical for protecting email users' privacy.We provide a certificateless one-way group key agreement mechanism with the following features in this work.End-to-end email encryption, where only the email sender and receiver can decrypt the communications, is essential to ensure email privacy. We suggested a certificateless one-way group key agreement protocol with attractive characteristics that is appropriate for building end-to-end email encryption systems in this work

24. The Internet of Things (IoT) provides services by connecting various platform devices. They are limited in their ability to provide intelligent service. IoT devices are diverse, ranging from wireless sensors to less resource-constrained gadgets. These devices are vulnerable to hardware/software as well as network assaults. It may result in security risks such as privacy and confidentiality if not adequately guarded. This study proposes an Intelligent Security Framework for IoT Devices to address the aforementioned issue. The suggested technique consists of (1) light weight Asymmetric cryptography for

protecting End-To-End devices that secure the IoT service gateway and low power sensor nodes and (2) Lattice-based cryptography for safeguarding Broker devices/Gateway and cloud services. We presented mutual and double authentication techniques in this work, which minimise traffic by removing fault and bogus packets. This system protects against quantum attacks, enhances performance, and minimises bandwidth usage.

25. Cyber security and data science are two of the most rapidly expanding topics in computer science, and they have lately been merged for a variety of applications. This position paper will examine the latest breakthroughs in applying data science to cyber security and cyber security to data science, followed by a discussion of the applications in social media. This study has examined the application of data science to cyber security as well as the application of cyber security to data science. There are several avenues for further investigation. We require new data science tools that can manage enormous volumes of data in a timely manner. We also need stronger adversarial machine learning models that incorporate a broader spectrum of approaches. Finally, we must keep trying to integrate cyber security and data science into social media apps. This includes addressing the difficult issue of distributing fake news. We need engineers, policymakers, social and political scientists, and legal experts to collaborate to discover viable answers to this challenge, just as we did with data privacy over the last decade.

26. A function that returns a feature vector from a dataset.A perceptual content is the perceived contents of the input video.The perceptual video hash is the product of the video hashing function and the output feature vector that characterises the perceptual contents of the input video. This hash must be resistant to changes that retain the perceptual contents of the video while also being vulnerable to adjustments that change the perceived contents of the video. The widespread use of perceptual hash in the field of multimedia, such as video authentication, copyright protection, and video retrieval, emphasises its significance. This study constructs a perceptual hash from a movie using 3D-radial pixel projection and evaluates the distinguishing capabilities and perceptual resilience of the hash obtained.

27. Getting daily news through social media is currently a regular practise among individuals. Untrustworthy information sources expose people to hoaxes, rumours, conspiracy theories, and false news. The mixing of legitimate and untrustworthy information on social media has made determining the truth difficult. According to academic study, online users are increasingly relying on social media as their primary source of news.Researchers discovered that young users, in particular, are more likely to accept what they read on social media if proper verification is not provided. In prior work, we presented the notion of 'Right-click Authenticate,' in which we recommended creating an accessible tool for authenticating and verifying material online before sharing it.

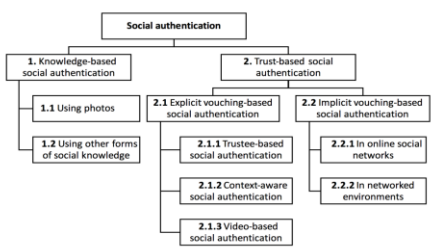
TABLE I. Information Quality Categories and Dimensions

Information Quality	Intrinsic IQ	Accuracy
		Believability
		Objectivity
		Reputation
	Contextual IQ	Value added
		Relevancy
		Timeliness
		Completeness
		Amount of data
	Representational IQ	Interpretability
		Ease of understanding
		Representation & consistency
		Conciseness of representation
		Manipulability
	Accessibility IQ	Access
		Security

In the era of information and social media, managing information quality has presented new issues. Whereas early study considered social media as an ancillary source of news, research reveals that this is no longer the case for many web users.This, in turn, has had a significant influence on intelligence. This research demonstrated how the dimensions of Information Quality may be utilised to organise the inherent complexity. Furthermore, giving methods for validating news and information may considerably increase the quality of information available to users.

38. Researchers have been motivated to develop socially-aware authentication schemes by the ever-increasing volumes of social knowledge shared in OSNs, the establishment of trustworthy social relationships over these platforms, and the emergence of technologies that allow friendship networks to be inferred from data exchanged in communication networks. We conduct the first survey of the literature on social authentication. We not only created a taxonomy classifying all social authentication schemes deployed in online or physical social contexts and extensively analysed their authentication features in this study, but we also built a novel framework for evaluating the effectiveness of all social authentication schemes, identified all practical and theoretical attacks that could be mounted against such schemes, addressed possible defence strategies, and identified challenges, open questions, and A complete comparative assessment of the security, usability, and deployability was undertaken

to quantify their accuracy, strengths, flaws, and limits, as well as to highlight the potential of knowledge-based and trust-based social authentication techniques. We think that by laying a strong basis for getting a comprehensive understanding of how users' social interactions have been used in user authentication systems and their security consequences, we may lead future research in this subject.



29 Mobile message sharing apps like WhatsApp, Hike messenger, and others have made it possible to communicate text and video messages on an unprecedented scale.These tools, however, allow the transmission of erroneous or even malicious information, which can generate widespread fear or manipulate public opinion. This study presents a method that allows users to validate the authenticity of messages received via message sharing apps. The Message Authentication System (MAS) creates a hierarchical library of legitimate information by mining a wide range of reliable internet and social media feeds. The user is subsequently given an authenticity index for the communication under review. Fake news is becoming a serious issue on all social media and message-sharing apps, with a number of adverse side effects as a result of the large volume and quick dissemination of information that they enable. Although Facebook is attempting to fix the problem, no solution for mobile message sharing applications exists, necessitating further study in this area. The Message Authentication System (MAS) is one of the first solutions to solve this issue by developing a third-party fact-checking tool.

30. The engineering faculty's major objective is to train qualified engineers for the local industry. Universities, in addition to providing engineering information, play an important and significant role in the construction and refining of an engineer's personality. This includes interpersonal social skills, which are especially important for industrial engineers (IEs), who deal with people more frequently than engineers in other professions. Recent research and ideas have revealed that students' Social Intelligence (SQ) consists of various abilities or competency areas. We invited IE students to fill out questionnaires assessing their own SQ across those skill categories. We discovered that the three skill categories with the lowest ratings are maybe the most significant for the workplace: Teamwork, conflict resolution, and social adaptability are all important. We also discovered that these three competency domains are connected, but not to other social competency areas.

We ended by looking at specific abilities within each competence area where IE students struggled the most. This paper presents a theoretical research to improve IE students' social intelligence in terms of appearance, importance, and abilities required to improve social intelligence.

31. Informally, "social debt" in software engineering refers to unplanned project costs associated with a "suboptimal" development community. Suboptimal development communities can be caused by a variety of factors, ranging from global distance to organisational hurdles to incorrect or ignorant socio-technical decisions (i.e., decisions that effect both social and technical components of software development). Social debt, like technical debt, has a significant influence on software development success. To ensure excellent software engineering, we believe that practitioners should be equipped with ways to recognise and manage social debt associated with their development communities. This study outlines and elaborates on social debt, pointing forth potential research directions. We compare social debt to technical debt and examine frequent real-life instances involving "sub-optimal" development communities.

32. We define social computing as a paradigm based on abstractions that describe how social actors—humans and organizations—interact in order to do business. These abstractions are part of a social layer that sits above the technical layers that make up software systems. This social layer is built on notions like agent, role, commitment, delegation, trust, and reputation. Many of the challenges we effectively manage in our daily lives influence social computing: business transactions with unknown parties, unpredictable settings, the establishment and enforcement of standards that control the marketplace, hostile actors, and so on. These dangers provide new issues for Requirements

Engineering (RE), which must specify artefacts capable of dealing with these hazards. We presented our viewpoint on social computing, identified a set of new risks introduced by this paradigm, and outlined some problems that Requirements Engineering would need to solve in order to properly tackle these threats.

33. Researchers have extensively studied extremists' use of online forums and social media platforms for recruiting and radicalising individuals. Meanwhile, the social engineering strategies used by these radicals to entice underprivileged persons to become radicalised have gone unnoticed. The social engineering components of internet radicalization will be discussed in this essay.The five Principles of Persuasion in Social Engineering (PPSE) will be specifically mapped onto the internet radicalization strategies used by extremists. Analysing these strategies can help you obtain a better understanding of the brainwashing process as well as the psychology of both the attacker and the target of such attacks.

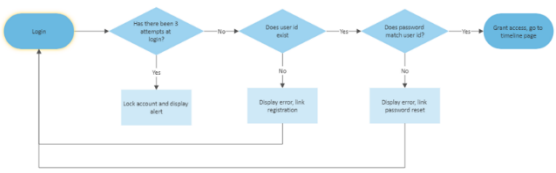


Fig 3.1.1: Flowchart for login page

PROPOSED SOLUTION:

This research paper elucidates one of the fine measures to verify user in online platforms.Our proposed technology will protect user's profile from unauthorized users in very safety way.A pseudo online platform was created and few accounts for testing was signed in to validate the accuracy and performance of our technology our technology. This paper is for protecting already existing users in the online platform.

3.1) Logging in

Logging in procedure consist of accepting user's phone number, user's password which later on clicking login will generate a OTP of 6 digits to the user's phone number which is made up number , so there are 1,000,000 possiblities for OTP.One-time passwords (OTP) are generally considered more secure than traditional static passwords because they are valid for only a short period and can be used only once.The login page is designed and implemented using React application along with phone number authentication using Firebase's authentication API.

Fig 3.1.2

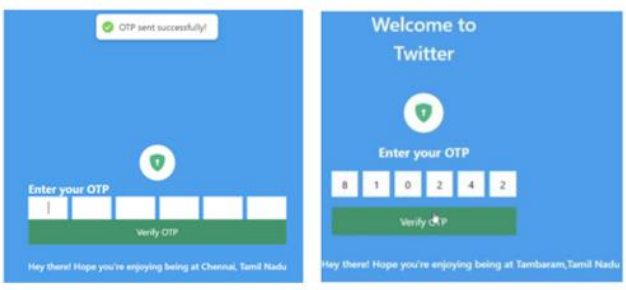


Fig 3.1.3

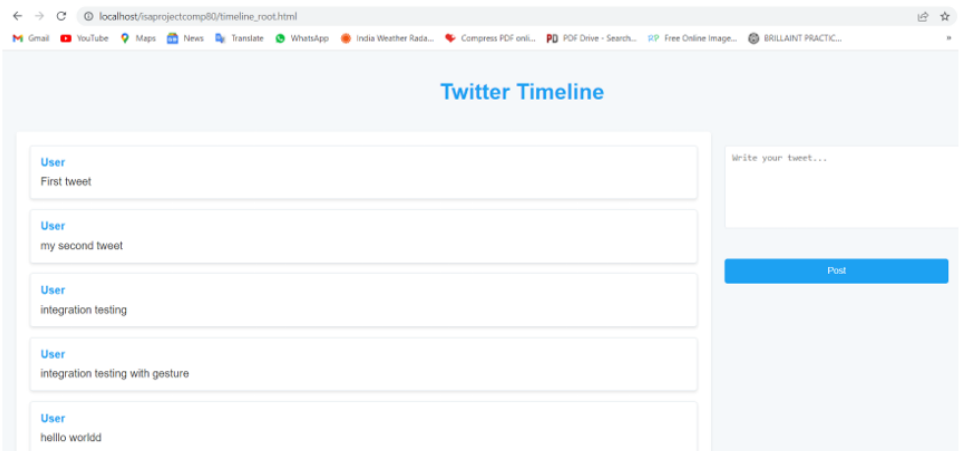


Fig: 3.1.4: Post verification

This Logging in technique using OTP is used because , we want to create a method that also compatiable with older devices , logging in using fingerprints needs fingerprint scanner which does not come in default with older mobilephones and since many still uses older mobilephone, so inorder to not exclude them we went with the conventional OTP system.

But still OTP based security systems can be compromised through several means phishing attack,Social engineering , sim swapping , Man-in-the-Middle.

However, despite these potential vulnerabilities, OTPs remain an effective additional security layer when compared to traditional passwords. To increase the difficulty of hacking OTPs, it is essential to implement best practices, such as:

- Using time-based OTPs instead of event-based ones.
- Encouraging users to use dedicated authentication apps instead of receiving OTPs via SMS.
- Implementing multi-factor authentication (MFA) with multiple authentication factors, such as something the user knows (password), something the user has (OTP token or authentication app), and something the user is (biometrics).

3.1) Allowing Activities

Securing the user profile is important , but securing what the user does and what the user can do with his/her account is even more important. We created a social media platform where we can post something (primarly text in our case). Inorder to post something the user has to undergo various verfication layers / protocols to conclude whether is it actually the user who is ready to post.

We created a post timeline (refer figure 3.1.4) which displays all the previous post posted by the user after logging in , if the user wants to post something new , the user has to type in the text and click the post button.Then user is again verified using multi-modal biometric system

1. Face-Recognition
2. Hand Gesture-Recognition

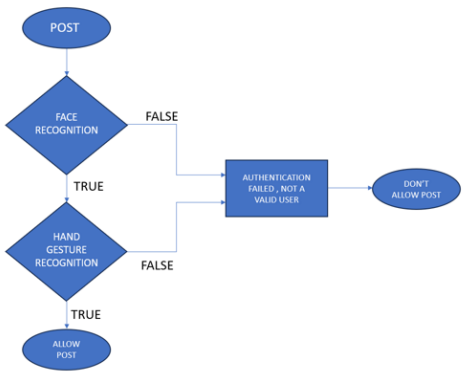


Fig:3.2.1

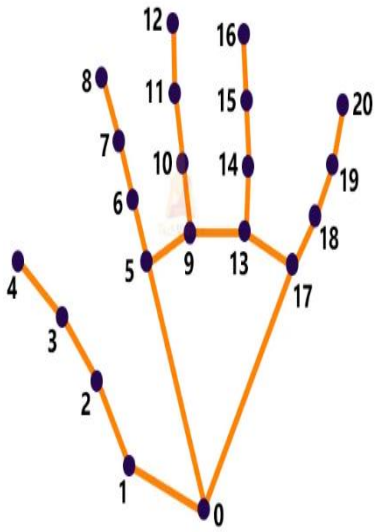
For face-recognition : the Face recognition is implemented using python programming language, opencv library and the model is taken from dlib which is consist of face-landmark mapping , image processing , and various face-recognition methods and function that are very handy.For Hand-Gesture recognition : is implemented using the MediaPipe framework and Tensorflow in OpenCV and Python.

The user has to pass both the layers , first Face-recognition system followed by Hand Gesture recognition. If the user fails either one in these layer , the user will not be able to perform any activities (post in this case)

Algorithms Used: OpenCV (Open Source Computer Vision Library) is a widely used open-source computer vision and machine learning library that includes functions for face detection and recognition. It utilizes pre-trained models and algorithms to detect faces in images and videos, and it can also be used to recognize faces by matching them against known faces or face encodings.

The face recognition functionality in OpenCV often relies on Haar cascades or deep learning models like Single Shot Multibox Detector (SSD) or You Only Look Once (YOLO) for face detection. For face recognition, it may use various algorithms, such as Eigenfaces, Fisherfaces, or Local Binary Patterns Histograms (LBPH).

In addition to OpenCV, Python also offers other powerful face recognition libraries like dlib and face_recognition. Dlib is a C++ library with Python bindings that includes facial landmark detection and various face recognition algorithms, such as Histogram of Oriented Gradients (HOG) and deep learning-based face embeddings using Residual Networks (ResNet).



0. WRIST
1. THUMB_CMC
2. THUMB_MCP
3. THUMB_IP
4. THUMB_TIP
5. INDEX_FINGER_MCP
6. INDEX_FINGER_PIP
7. INDEX_FINGER_DIP
8. INDEX_FINGER_TIP
9. MIDDLE_FINGER_MCP
10. MIDDLE_FINGER_PIP
11. MIDDLE_FINGER_DIP
12. MIDDLE_FINGER_TIP
13. RING_FINGER_MCP
14. RING_FINGER_PIP
15. RING_FINGER_DIP
16. RING_FINGER_TIP
17. PINKY_MCP
18. PINKY_PIP
19. PINKY_DIP
20. PINKY_TIP

Case 1 : The user is a verified user

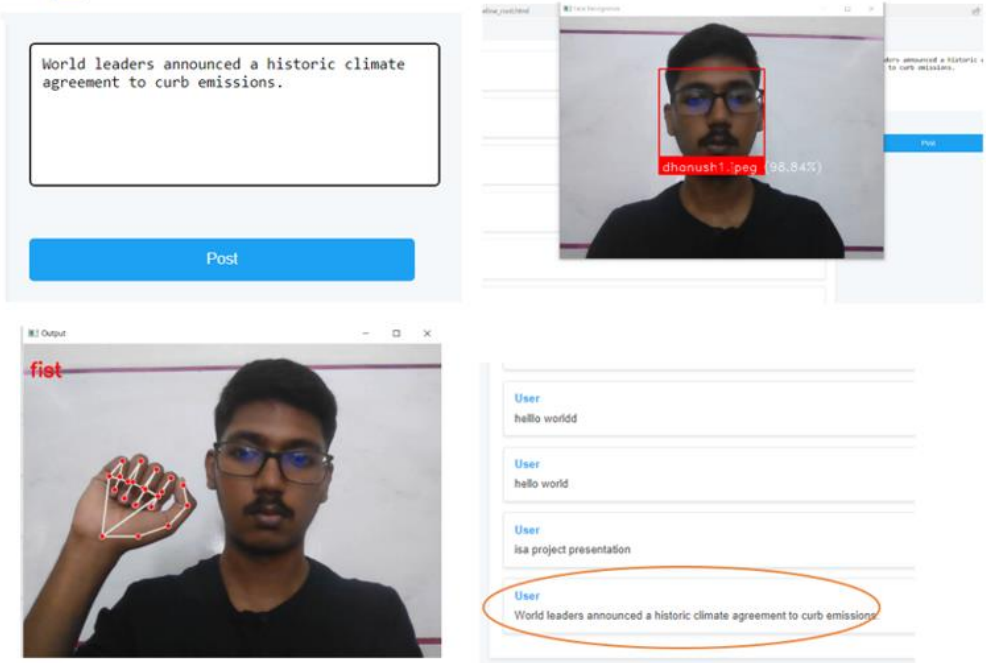


Fig 3.2.2 : the user is a verified user

In this case , the system user was able to clear all the security level because that person is the actual user for the account .

Case 2: not a valid user

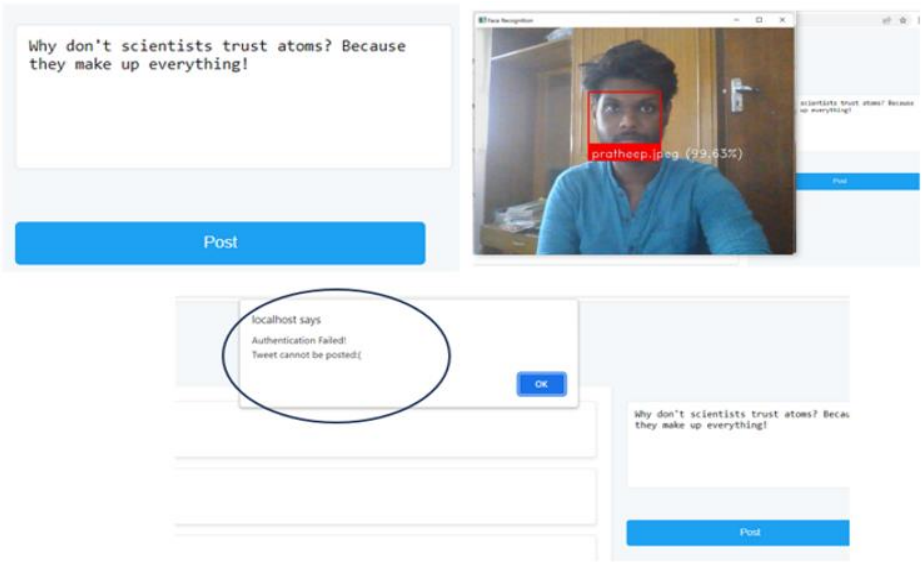


Fig:3.2.3: User is not valid user for the account (a)

The unauthorized user trying to post something on other person's account , got stopped at the facial recognition level.

Case 3: User is not valid user , bypassed face-recognition level , but caught in Hand gesture level

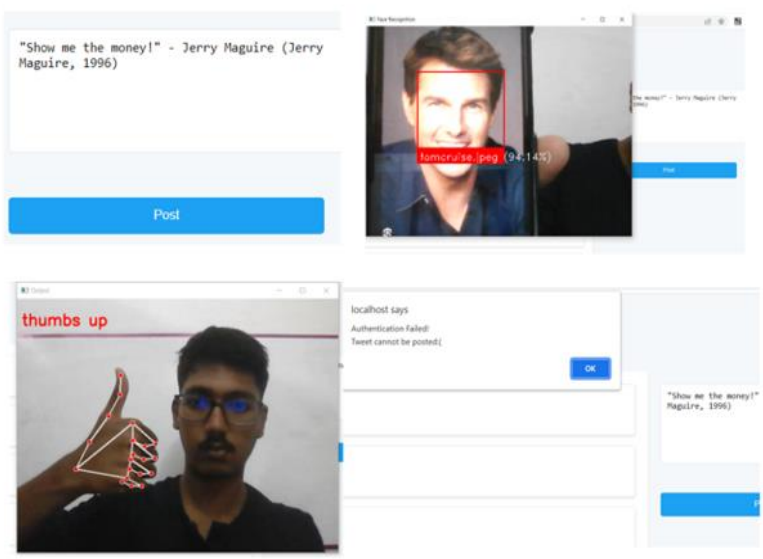


Fig 3.2.4: User is not valid user for the account (b)

The unauthorized user somehow bypassed facial recognition stage and but couldn't bypass the hand gesture recognition due to lack of idea of what the actual user's hand gesture is used to verify that person.

CONCLUSION:

The proposed user authentication represents a state-of-the-art approach to enhance security and streamline user authentication. By leveraging Multimodal biometric using face and hand gesture recognition continuous behavioral analysis, and real-time notifications, this innovative system provides a very secure and reliable solution to verify users effectively and ensure the highest level of security for online platforms when compared to other already existing system. To futher fortify the logging in phase, we can use geo-locking mechansim by comparing the users phone's location with logging in device location.

REFERENCE

[1] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," in IEEE Network, vol. 33, no. 2, pp. 82-88, March/April 2019, doi: 10.1109/MNET.2019.1800240.

[2] Haider Mehraj, D. Jayadevappa, Sulaima Lebbe Abdul Haleem, Rehana Parveen, Abhishek Madduri, Maruthi Rohit Ayyagari, Dharmesh Dhabliya,Protection motivation theory using multi-factor authentication for providing security over social networking sites,Pattern Recognition Letters,Volume 152,2021,Pages 218-224,ISSN 0167-8655,

[3] Muhammad Sajjad, Salman Khan, Tanveer Hussain, Khan Muhammad, Arun Kumar Sangaiah, Aniello Castiglione, Christian Esposito, Sung Wook Baik,CNN-based anti-spoofing two-tier multi-factor authentication system,Pattern Recognition Letters,Volume 126,2019,Pages 123-131,ISSN 0167-8655,

[4] Panguluri, S.D., Lakshmy, K.V., Srinivasan, C. (2022). Enabling Multi-Factor Authentication and Verification in Searchable Encryption. In: Sharma, D.K., Peng, SL., Sharma, R., Zaitsev, D.A. (eds) Micro-Electronics and Telecommunication Engineering . ICMETE 2021. Lecture Notes in Networks and Systems, vol 373. Springer, Singapore. Panguluri, S.D., Lakshmy, K.V., Srinivasan, C. (2022). Enabling Multi-Factor Authentication and Verification in Searchable Encryption. In: Sharma, D.K., Peng, SL., Sharma, R., Zaitsev, D.A. (eds) Micro-Electronics and Telecommunication Engineering . ICMETE 2021. Lecture Notes in Networks and Systems, vol 373. Springer, Singapore

[5] Ioannis Stylios, Spyros Kokolakis, Olga Thanou, Sotirios Chatzis,Behavioral biometrics & continuous user authentication on mobile devices: A survey,Information Fusion,Volume 66,2021,Pages 76-99,ISSN 1566-2535,https://doi.org/10.1016/j.inffus.2020.08.021.

[6] Alsaadi, Israa. (2021). Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review. International Journal of Scientific & Technology Research. 10. 15-21.

[7] L. Zahrouni, D. Blackwood, S. Rizvi, J. Gualdoni and M. Almiani, "Preventing identity theft using biometrics based authentication system," 2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), Aqaba, Jordan, 2017, pp. 1-6, doi: 10.1109/AEECT.2017.8257767.

[8] Yang, W.; Wang, S.; Sahri, N.M.; Karie, N.M.; Ahmed, M.; Valli, C. Biometrics for Internet-of-Things Security: A Review. *Sensors* **2021**, *21*, 6163. N. Sidaty, M. Viitanen, W. Hamidouche, J. Vanne and O. Déforges, "Live Demonstration: End-to-End Real-Time ROI-based Encryption in HEVC Videos," *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, Italy, 2018, pp. 1-1, doi: 10.1109/ISCAS.2018.8351775.

[9] J. -h. Yeh, S. Sridhar, G. G. Dagher, H. -M. Sun, N. Shen and K. D. White, "A Certificateless One-Way Group Key Agreement Protocol for End-to-End Email Encryption," *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*,

Taipei, Taiwan, 2018, pp. 34-43, doi: 10.1109/PRDC.2018.00014.

[10] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," *2017 International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2017, pp. 1-5, doi: 10.1109/ICISC.2017.8068718

[11] B. Thuraisingham, M. Kantarcioglu and L. Khan, "Integrating Cyber Security and Data Science for Social Media: A Position Paper," *2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, Vancouver, BC, Canada, 2018, pp. 1163-1165, doi: 10.1109/IPDPSW.2018.00178.

[12] R. Sandeep, S. Sharma and P. K. Bora, "Perceptual video hashing using 3D-radial projection technique," *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, Chennai, India, 2017, pp. 1-6, doi: 10.1109/ICSCN.2017.8085727.

[13] P. Pourghomi, A. A. Halimeh, F. Safieddine and W. Masri, "Right-click Authenticate adoption: The impact of authenticating social media postings on information quality," *2017 International Conference on Information and Digital Technologies (IDT)*, Zilina, Slovakia, 2017, pp. 327-331, doi: 10.1109/DT.2017.8024317

[14] N. Alomar, M. Alsaleh and A. Alarifi, "Social Authentication Applications, Attacks, Defense Strategies and Future Research Directions: A Systematic Review," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1080-1111, Secondquarter 2017, doi: 10.1109/COMST.2017.2651741.

[15] A. Gupta, P. Prabhat, R. Gupta, S. Pangotra and S. Bajaj, "Message Authentication System for Mobile Messaging Applications," *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, Jammu, India, 2017, pp. 147-152, doi: 10.1109/ICNGCIS.2017.32.

[16] Dhillon, P.K., Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. *J Reliable Intell Environ* **4**, 141–160 (2018). Drozdowski, Pawel, Christian Rathgeb, Antitza Dantcheva, Naser Damer and Christoph Busch. “Demographic Bias in Biometrics: A Survey on an Emerging Challenge.” *IEEE Transactions on Technology and Society* 1 (2020): 89-103.

[17] Masala, G.L., Ruiu, P., Grosso, E. (2018). Biometric Authentication and Data Security in Cloud Computing. In: Daimi, K. (eds) Computer and Network Security Essentials. Springer, Cham

[18] Gunasinghe, H., & Bertino, E. (2017). PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones. IEEE Transactions on Information Forensics and Security, 13(4), 1042-1057.

[19] Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems, 106, 1-14.

[20] Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Systems Journal, 14(1), 39-50.

[21] Shuai, M., Xiong, L., Wang, C., & Yu, N. (2020). A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem. Computer Communications, 160, 215-227.

[22] Narwal, B., & Mohapatra, A. K. (2021). A survey on security and authentication in wireless body area networks. Journal of Systems Architecture, 113, 101883

[23] M. Vijay, G. Indumathi,Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications,Journal of Information Security and Applications,Volume 58,2021,102707,ISSN 2214-2126

[24] F. Zhang, A. Kondoro and S. Muftic, "Location-Based Authentication and Authorization Using Smart Phones," 2012 IEEE 11th

International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 2012, pp. 1285-1292, doi: 10.1109/TrustCom.2012.198.

[25] C. P. SHAN, W. HON LOON, L. K. WIN, D. DIN and S. C. SEAK, "Automated Login Method Selection in a Multi-modal Authentication System : Login Method Selection based on User Behavior," 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Malaysia, 2019, pp. 120-124, doi: 10.1109/ISCAIE.2019.8743992.“Face Recognition and Geolocation based Authorization and Authentication: A Survey.” (2020).

[26] “Face Recognition and Geolocation based Authorization and Authentication: A Survey.” (2020).

[27] Morris, Andrew & Jassim, Sabah & Sellahewa, Harin & Allano, Lorene & Ehlers, Johan & Wu, Dalei & Koreman, Jacques & Garcia-Salicetti, Sonia & Ly-Van, Bao & Dorizzi, Bernadette. (2012). Multimodal Biometric Authentication forSmartphones - art. no. 62500D. Proc SPIE. 10.1117/12.668776.

[28] A. S. Hanbazazah, "The Need for Social Intelligence Training for Industrial Engineers," 2020 Industrial & Systems Engineering Conference (ISEC), Makkah, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/ISEC49495.2020.9230043.

[29] : D. A. Tamburri, P. Kruchten, P. Lago and H. van Vliet, "What is social debt in software engineering?," 2013 6th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), San Francisco, CA, USA, 2013, pp. 93-96, doi: 10.1109/CHASE.2013.6614739

[30] F. Dalpiaz, "Social threats and the new challenges for Requirements Engineering," 2011 First International Workshop on Requirements Engineering for Social Computing, Trento, Italy, 2011, pp. 22-25, doi: 10.1109/RESC.2011.6046716.

[31] S. Sabouni, A. Cullen and L. Armitage, "A preliminary radicalisation framework based on social engineering techniques," 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), London, UK, 2017, pp. 1-5, doi: 10.1109/CyberSA.2017.8073406.