iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.57985

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

An Alternative to Traditional Credential Based Authentication

Mr. Peniel John Whistely[1], Lakshmi B[2], Pragathi N[3], Brindashree R C[4], Srusti M H[5]
[1]*Assistant Professor (Dept of CSE, Presidency University, Bangalore, Karnataka, India)*
[2, 3, 4, 5]*Students (Department of Computer Science and Engineering, Presidency University, Bangalore, Karnataka)*

Abstract: ***Passwords have served as our security over the years by preventing unauthorized access to one's data. Technology has advanced to the point where we are utilizing passwords in ways that are both considerably more secure and user-friendly than they ever have been. The industry and researchers have been compelled, therefore, by the flaws found and noted in this conventional system to look for alternatives where there is no risk of identity theft, hacking, or password cracking. The main developed password-less authentication methods are covered in detail in this chapter. Additionally, it makes an attempt to clarify each technique's finer points and operation by using a use-case graphic. The poor trying to would greatly benefit from and contribute to the callow attempting to investigate research prospects in this field. This work has illustrated biometrics' current place in the security field. In this study, we have also discussed the pros and cons of various approaches, as well as comments regarding the usability of biometric authentication systems.***

I. INTRODUCTION

Passwords have been compromised, stolen, and broken over the years. On social networking platforms, fraudulent agencies can purchase user data and login passwords online. Numerous incidents, like the Facebook data leak, the Yahoo security breach, the LinkedIn data leak, the Dropbox user account leak, etc., have been reported globally. An additional factor would be the growing range of platforms and apps available, which could compel the user to memorize an increasing number of passwords (Cortopassi, M., Edward, E., 2013). With the promotion, publicizing, and application efficiency driving growth in both technology and its user base, secure routes for password storage and communication are proliferating. Despite this, password-based login is more common these days due to the sharp rise in internet-connected gadgets and the increased number of users with online password-less authentication is becoming a more viable option for safe online account logging than it was previously. Password memorization becomes challenging, which encourages users to use the same password across most applications, leaving them vulnerable to hackers. This is the cause that can actively contribute to a rise in security lapses and make it simpler for hackers to obtain data. This has also encouraged the development of apps that save user accounts and passwords for each account that a user uses locally. In light of this, the password management system appears to be a viable and dependable method for storing complex passwords needed for single sign-on access to cross-platform systems. Because they save the cumbersome password in one location, the layperson perceives them as time-savvy and less laborious. Nevertheless, the user is unaware of how these applications could operate in the background to spread their private data over the internet. However, the user could unintentionally give the program permission to disclose sensitive information in addition to accepting the terms during the installation or registration process. This time, granting these kinds of apps blind access to secure accounts is a good way to gauge a user's reliability. Each user's password usage remains consistent and comparable. to one another, which would also lead to hackers use the hit-and-try strategy to guess passwords. Severe issues arise from this trial-and-error approach, such as obtaining remote access to user data that is kept on a server or client computer. We have reached the point where there won't be any more password breaches, with the assurance of more secure authentication and the complete elimination of password memorizing. One essential security investment that has many advantages is password less authentication.

A. Enhanced User Experience

It is not necessary for younger users to recall the usage of riddles and inquiries such as "What was the name of your first pet dog?" and "Which high school was it?" This shortens the signup procedure and spares users from having to go through the time-consuming registration process for new apps. Their interfaces and capacities are far more engaging than those of password-based authentication.

©IJRASET: All Rights are Reserved

B. *Improved Security*

We have more secure makeshift security when passwords are not used because there are no passwords to memorize. Any software development application's primary focus is security, which includes a few processes related to authorization, integrity, verification, and authentication. Password less authentication is one such method of authentication. Users no longer need to memorize complex passwords for various apps they use on a regular basis thanks to this authentication solution. Passwords are not needed for this kind of authentication in order to access any application. Passwords are becoming less and less relevant due to the increasing popularity of password-less authentication. Based on this improved user authentication system, this modern enterprise model guarantees effortless security.

C. *Driving Forces Toward Passwordless Authentication*

Everyone agrees that password-based authentication is not the best in terms of usability or security. But password-based systems are inexpensive to implement, and you don't have to train your end users with a new technology or process related to the credentials and their management

D. *Level Of Assurance*

The notion of "Level of Assurance" (LOA) holds significant importance in the context of authenticating techniques. The European Union, individual countries, NIST (US), and other organizations like GSMA have developed classifications that are used to assess authentication techniques. Higher rankings indicate more reliable digital identities in terms of authentication. There are two components to the assurance of an authentication technique: the method itself and the identity registration process. The final LOA for the digital identification and authentication method will be determined by taking the registration or technique with the lower score when calculating the overall LOA score. However, the Level of Assurance concept is retired in the recently published NIST Digital Identity Guideline (SP 800-63-3), which also includes three new formal evaluation categories: Identity Assurance Level (IAL), Authenticator Assurance Level, and The Federation Assurance Level (FAL) , (AAL). The Authenticator Assurance Level, which is used to assess the authentication method's strength, is the pertinent category for this whitepaper. We have shown the level (1, weak – 3, strong) at which the new NIST standards could map specific authentication mechanisms for the AAL.

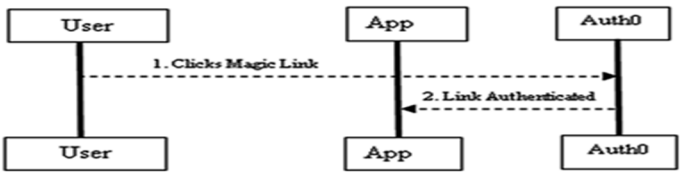
II. DIFFERENT TECHNIQUES OF PASSWORDLESS AUTHENTICATION:

The various password-less authentication modalities are:

A. *Magic Link Login Authentication*

Users frequently log in to multiple accounts in their daily lives, so instead of requesting passwords, simply ask for the username to generate a temporary authorization number for a session-full login. This code is simultaneously acknowledged to the mail id that the user has provided for the linked username. Afterwards, in order to access account-based services with time-limited access to the magic link, the user must click the link to confirm their identity. This authorization number is then swapped with the session key on the back end when the user login into the connected account, allowing them to access the account until the session expires. Additionally, this key is kept on the user's device. Later on, the magic link authentication thinks, The mail server's security is sufficient to verify the identity of the user, since the user cannot control the mail databases' backend security. The password less magic link login system's general flow could look something like this: The username needs to be filled out by the user. When you click "Submit," two API calls are made. To start the verification process, an authentication code will be generated and delivered to the registered user's email address. The second step is to verify the previously created authentication code with another that is obtained by the user when they navigate from mail to the app or account. Once the comparison is successful, the user is taken to the app, where the secure session key and the matching authentication code are exchanged to grant extended access to the account. The magic link is no longer active.

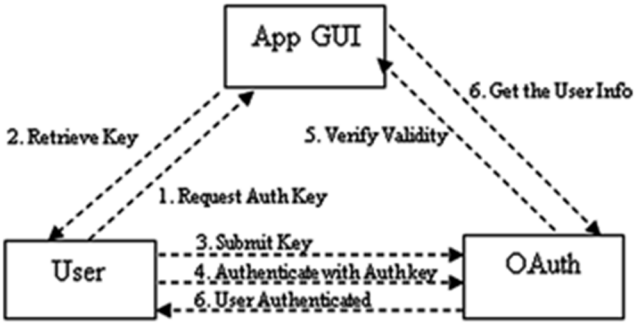
Figure 1(a). Working: Authenticated login to the user account



B. Token-Based Login (OTP Based)

This type of authentication is also called as HOTP (Hash Message Authentication Code based One Time Password). It happens between the client's token and token generated by the authentication server. Regardless of Time Based Token i.e.

Figure 1(b). API Calling in Token Based Login



C. Challenge Response Authentication Mechanism (CRAM)

This is a family of protocols that have the feature of one entity challenging another. The authenticated access is granted upon the second entity providing the correct response. It is a means of authenticating a person across an unsecured channel of communication without disclosing any information to a third party listening in.It is a two-step protocol that uses one-way hash functions to verify that a user is connected to the network via HTTP. This makes it impossible to determine the function's input by utilizing a generated hash. User authentication and digest authentication are the two steps. Similar to how the majority of smart card systems operate, CRAM necessitates the usage of both a password and a user smart card (Mizrah, L., L., 2011). One further illustration is the application of CAPTCHA, which detects automated registration, stops spam, and verifies human input. Key agreement mechanisms in cryptography, such as CRAM-MD5, Secure Shell CRS, and RSA-based Zero-Knowledge Proofs, are examples of secure CRAM. The primary flaw in this system is that the same challenge is sent repeatedly. Repetitive challenges from the server will lead to system gullibility and allow replay attacks. Without knowing the password, the attacker may be able to obtain secure access by simply replaying the hash of the last authentication that they recorded. The graphic below illustrates how a CRAM functions:

Figure 1(c). Authentication using CRAM



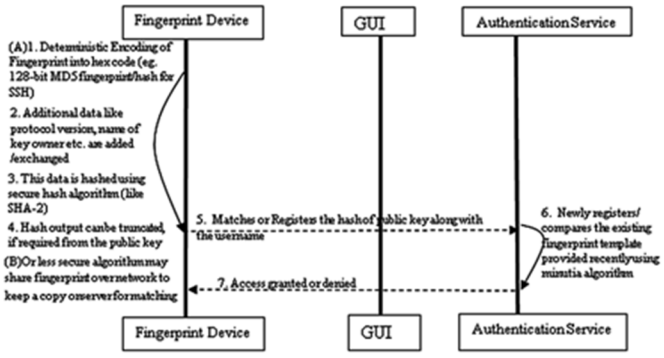
D. Fingerprint/ Thumbprint Authentication

Most of the app developers expect users to form a complicated combination of passwords that are unique and unguessable on first sight. Though it is need of time to having an easy yet secure authentication pass-code mechanism. This must be secure, unique, cannot be forged, and provides quicker access to app or service. One such way is using a fingerprint of the user that is easy to do as everyone possesses a smart-phone and also nothing to remember like in password-based authentication schemes. Authentication using fingerprints is not a novice concept, it has been in the market a couple of decades before in laptop, automatic suitcases and electronic doors etc. but now it has been fanned more with the prevalence of mobile gadgets. The fingerprint of the user is never sent over the network. In fact, when a user signs up using fingerprint authentication, a unique key pair, secret key, and the public key is generated on the user device. The user is created, the public key is assigned and the private key is saved in a key store and all this happens locally on the user device. Not only this much but fingerprints are also used biometric attendance system, a collection of forensic evidence during criminal investigations, to control access to devices like smartphone, laptops etc.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The most important part of fingerprint scanning and authentication is quality control which decides the ridges, valleys and required details of minutia points on fingers accurately. There is no problem called as forgetting passwords, creating a strong combination of alphanumeric cum special characters and as well as no fear of losing them. Swipe-and-PIN was also a promising alternative for payments using e-wallets is never transmitted across the network. In actuality, a unique key pair, secret key, and public key are generated on the user device upon signing up with fingerprint authentication. All of this occurs locally on the user device: the user is established, the public key is assigned, and the private key is stored in a key store. Not only that, but fingerprints are also used to manage access to gadgets like laptops and smartphones through the biometric attendance system, a collection of forensic evidence utilized in criminal investigations. The process of precisely determining the ridges, valleys, and necessary minutia points on fingers through quality control is the most crucial aspect of fingerprint scanning and identification. There isn't a problem with forgetting passwords, combining powerful alphanumeric and special character combinations, and not worrying about losing them. Another viable option for e-wallet payments was swipe-and-PIN.

Figure 1(d). Authentication using Thumb/Fingerprint:



III. PROPOSED MOTHODOLOGY

In order to compile all the information relevant to the study's scope and draw conclusions from it, the current literature-based comparative analysis relied on prior research findings. This allowed it to develop a new theoretical viewpoint in the field of knowledge, particularly with regard to the utility of the various biometric systems. An examination of the body of existing research in the field was made possible by the inductive methodological approach that was used. Because of this, the study is essentially qualitative in character and solely dependent on secondary sources of data, the interplay of which is freely acknowledged throughout the entire investigation. the compilation of at least 25 reliable sources, such as books, conference papers, and journals with SCOPUS listings on biometrics identification and verification systems were contacted to aid with the compilation. Using a thematic approach, the study conducted a comparative analysis of the various biometric systems, taking into account factors like distinctiveness, complexity, and universality in addition to acceptance and rejection rates, sensitivity, and security levels.

A. Enrollment

Gather biometric data: Using dependable sensors, gather high-quality biometric samples (such as fingerprints, face photos, and iris scans). Prepare the data: Improve the quality of the image, extract pertinent elements, and format it for storage. Make a template Create a distinct, safe template for every user, frequently utilizing algorithms such as: Bio-hashing: Data protection by irreversible change. Encoding of features: Key features are encoded for matching. Abrupt biometrics: Revocable privacy-focused templates.

B. Authentication

Take a fresh biometric sample. Take a new sample with the same sensor that was used for enrollment. Preprocess data: Use the same procedures as during enrollment for preprocessing. Retrieve attributes: Take out the pertinent features so you can compare. Compare the template to the match: Utilizing matching techniques such as these, compare extracted features with stored templates:

1) Correlation-based Calculate how similar two feature sets are to one another.
2) Distance-based: Determine the scores for the distances between the characteristics.
3) Finding corresponding patterns is the process of pattern matching.

C. Enhancements

Multimodal biometrics: For increased convenience and security, combine various features (such as a face and fingerprint). Liveness detection: Use strategies such as these to stop spoofing. Challenge-response: Pose tasks such as grinning or blinking. Analyze skin texture to find patterns in it. 3D scanning: Determine liveliness and depth. safeguarding the template: Use safeguard templates by: Encryption: safeguard templates during transmission and storage. Bind templates to cryptographic keys in biometric cryptosystems. Protection of privacy: Put in place precautions such as: Minimize data by gathering only what is required. Get express consent from the user before using their data. Transparency: Tell users how and where data is collected.

D. Continuous Improvement

Stay updated: Monitor advancements in algorithms, sensors, and security measures. Adapt to evolving threats: Address new attack vectors and vulnerabilities. Incorporate user feedback: Improve usability and acceptance.

Figure. 2: An example of the biometric enrolment, verification, and identification process:



IV. OBJECTIVES

The use of biometric login systems, such as fingerprint or facial recognition, offers several objectives and benefits in various contexts. The specific objectives may vary depending on the application and the organization implementing the system, but here are some common objectives associated with biometric login:

1) *Enhanced Protection:* When compared to conventional username and password login techniques, biometric login systems are intended to offer a higher level of protection. Because biometric information is specific to each person, it is more difficult for unauthorized users to obtain access.
2) *Prevention of illegal Access:* By guaranteeing that only people with the correct biometric data can enter, biometric systems help prevent illegal access. This is especially crucial for protecting locations and sensitive data.
3) *Fraud Prevention:* By making it more difficult for people to pose as someone else, biometric technologies assist prevent fraud. This is particularly important when it comes to access to vital systems and financial activities.
4) *Uniformity and Standardization:* To create a uniform strategy for deploying and overseeing biometric identification systems inside a company. To establish a standard point of reference for system design, development, testing, implementation, and upkeep, guaranteeing compliance with standards and best practices.

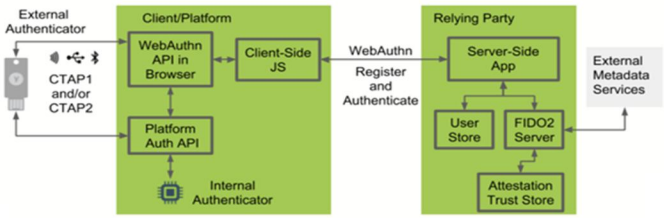
V. SYSTEM DESIGN & IMPLEMENTATION

The operational architecture for the proposed system is illustrated in the figure below:

The client submits a form, for example, requesting to begin the ceremony. At this stage, the username might or might not be known. The user may be seeking to register for a new account, for instance, or we may be utilizing username-less authentication. The program generates a user handle in an application-specific manner if the user does not already have one. Before continuing, the application may decide to request password or similar user authentication. The application provides a read-only database adapter that the library uses to look for the user's credentials if it knows the username. After the user authorizes the action, the client sends an application back with a Public Key Credential object answer. The request is retrieved by the application from temporary storage and approved. The request and answer to a "finish" method in the library, which is used to execute the logic for response validation. The validity of the response contents, including the challenge and origin, is confirmed by the library. The public key is returned by the database adapter. The authenticity signature is checked by the library. A POJO representation of the ceremony's outcome is returned by the library. This will contain the new credential's public key and credential ID for registration ceremonies. The application has the option to obtain details regarding the authenticator model and the trustworthiness of the authenticator attestation. This will comprise the username and user handle, the credential ID of the utilized credential, and the updated credential signature counter value for authentication ceremonies.

The program notifies the client of the failure if the outcome is unsatisfactory. In the event that the outcome meets the requirements, the program stores the updated if this is a ceremony for registration, the credential. In the event that this is an authentication ceremony, the program modifies the credential's signature counter that is kept in the database. The program ends by reporting success and carrying on with its business logic.

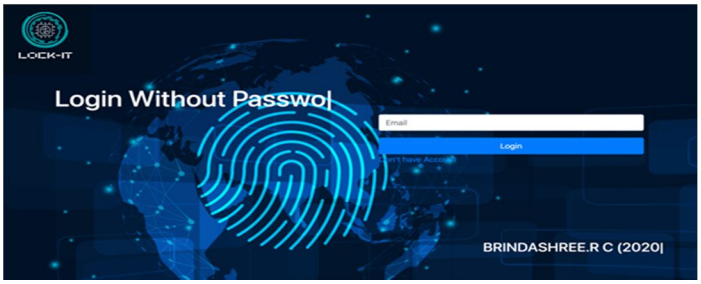
Figure3: Application Architecture

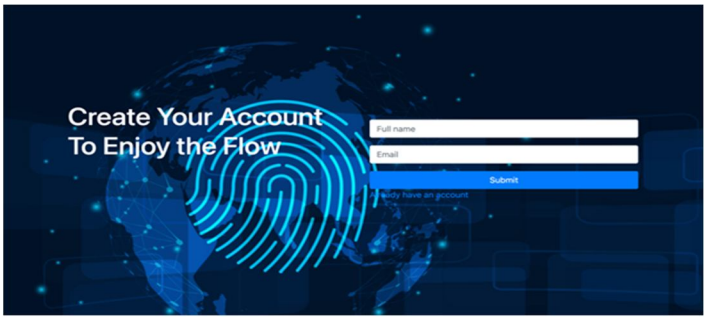


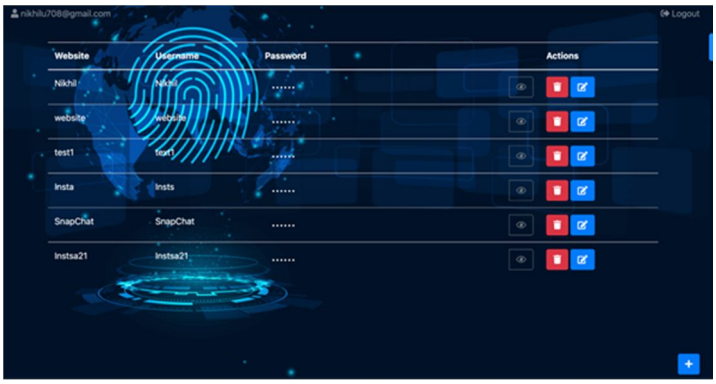
VI. RESULTS AND DISCUSSIONS

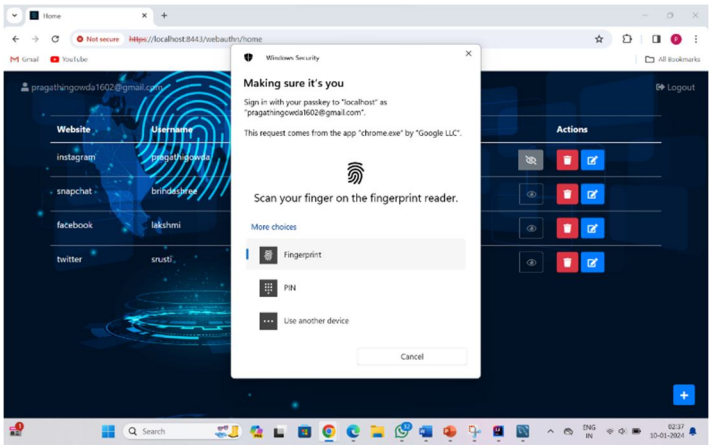
Because physical human traits are far harder to counterfeit than security codes, passwords, and hardware keys, biometric authentication is extremely dependable. Physical keys, ID cards, smart cards, and magnetic stripe cards are examples of tokens that can be misplaced, taken, copied, or left at home. Passwords might be shared, overlooked, or forgotten. People also need to memorize a lot of passwords and Personal Identification Numbers (PINs) for a variety of accounts, including computer accounts, bank accounts, ATMs, e-mails, cellular phones, websites, and so on, in today's fast-paced electronic environment. For a wide range of applications, biometrics offers the promise of quick, simple, accurate, dependable, and affordable verification. Tele-biometric systems are created when biometric systems are networked with telecommunications technologies. Enrollment and testing are the primary activities. Transportation & Storage Solutions. Issues There are seldom any laws in existence that specifically address the protection of biometric data, despite the extremely unique nature of such data. Instead, clauses pertaining to the protection of personal information and general privacy are what legal texts rely on. Nevertheless, occasionally it turns out that such laws are not well suited to biometric data. Even if biometric systems are more convenient and secure, it's important to address privacy issues and make sure that the right security measures are in place to protect people's biometric data. Furthermore, the precision and dependability of the selected biometric modality as well as the system's overall implementation affect how effective biometric systems are.

VII. SNAPSHOTS









REFERENCES

[1] Juels, A., Rivest, R. L., & Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), pp. 103–11

[2] Kumar, S., Garera, S., & Boneh, D. (2006). A model for role-based key management. ACM Transactions on Information and System Security (TISSEC), 9(3), 228–258

[3] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of Applied Cryptography. CRC press.

[4] Wang, Y., & Wu, J. (2010). An efficient and secure protocol for RFID systems resistant to desynchronization attacks. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications (pp. 254–265). Springer

[5] Juels, A., & Weis, S. A. (2005). Defining strong privacy for RFID. In International Conference on Pervasive Computing (pp. 98–107). Springer.

[6] Kapadia, A., Henderson, T., Kotz, D., & Triandopoulos, N. (2008). The whereabouts clock: Privacy through time in location-based services. In 2008 Second ACM Conference on Wireless Network Security (WiSec) (pp. 113–124). IEEE.

[7] Bonneau, J., Preibusch, S., Anderson, R., & Stajano, F. (2010). A password marketplace approach to studying user choice in graphical passwords. In Proceedings of the 26th Annual Computer Security Applications Conference (pp. 323–332). ACM

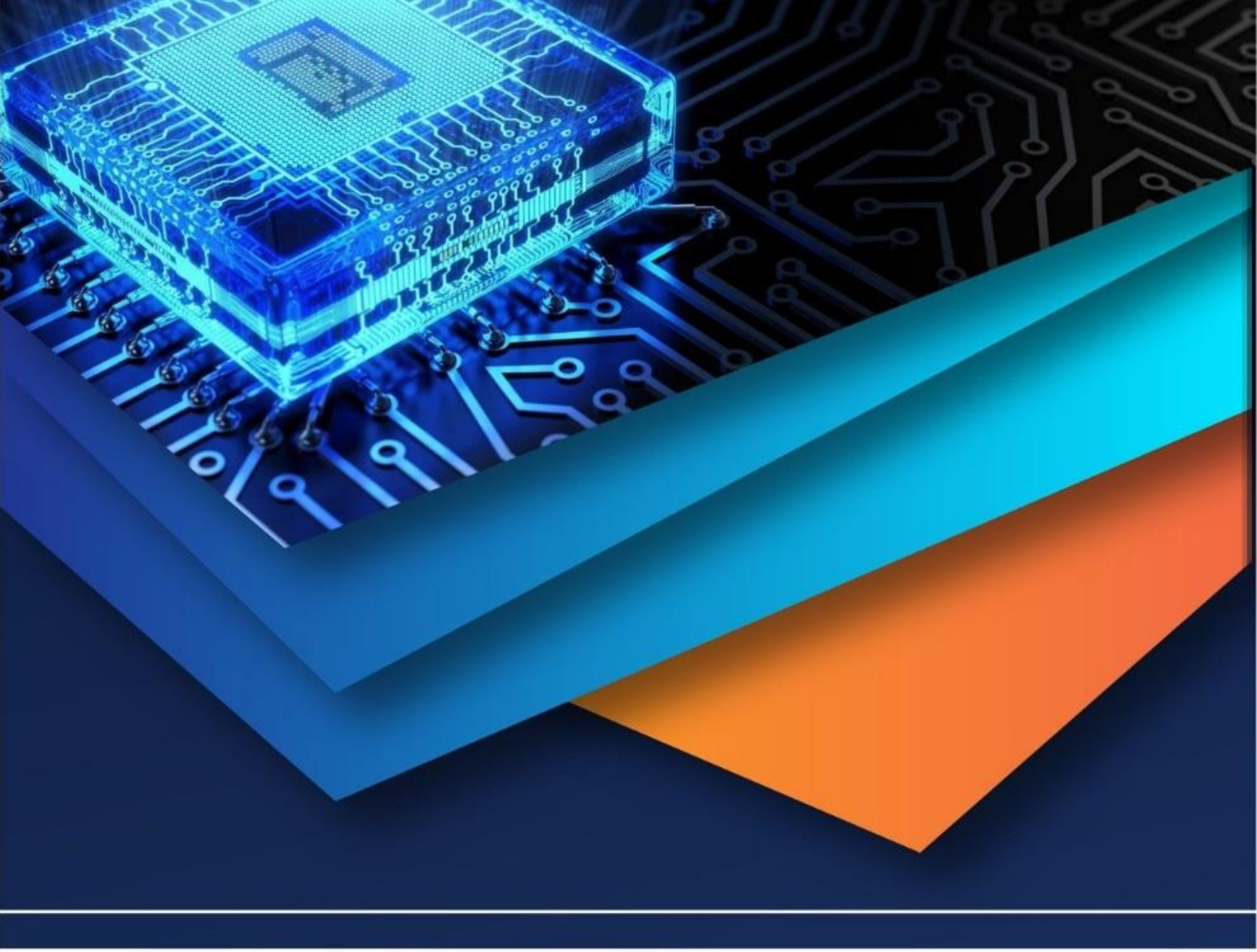
[8] Hong, J., & Landay, J. A. (2004). An architecture for privacy-sensitive ubiquitous computing. In Proceedings of the Second International Conference on Mobile Systems, Applications, and Services (MobiSys '04), pp. 177–189.

[9] Shirazi, F., Golestani, A., & Cankaya, H. C. (2015). A comprehensive study of biometric authentication systems. Procedia Computer Science, 52, 855–861

[10] Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770–772.

[11] Camenisch, J., & Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 93–118). Springer.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)