iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61304

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 IV Apr 2024- Available at www.ijraset.com

Auto-Logout Google Account Extension

Saurabh Sawant[1], Suraj Yadav[2], Anuj Kapileshwari[3], Sahana Godale[4], K. S. Charumathi[5]
[1, 2, 3, 4]*Student,* [5]*Professor at Pillai College of Engineering, Department Of Information Engineering Pillai College of Engineering, New Panvel, India*

Abstract: ***This project aims to develop a browser extension that automatically logs out users from their Gmail accounts upon browser closure, bolstering security, especially during power outages. It also alerts users before closing the browser if any webpage has a logged-in Google account to prevent unauthorized access. Given the risks associated with forgotten password emails and the broad access granted by Google accounts, such as to Drive and Photos, the extension plays a crucial role in mitigating potential data breaches. Additionally, it facilitates the management of Google account data, including location information and device identifiers, offering proactive protection against unauthorized access and security threats like phishing attacks and malware.***

Index Terms: Google Account, Gmail, Browser Extension, Security, Unauthorized access, Automatic Logout, Phishing attack, Malware.

I. INTRODUCTION

This project aims to develop a security extension for Gmail users. The extension ensures automatic logout upon browser closure, reducing the risk of unauthorized access. In cases of power outages, it logs out accounts upon system reboot and internet reconnection. Additionally, it warns users before closing the browser and monitors Google account logins on websites. By addressing vulnerabilities associated with staying logged in, such as exposure to malicious attacks and data breaches, the extension enhances user security. It simplifies the login process for websites that support Single Sign-On (SSO) with Google, enhancing user convenience and security. Furthermore, it enables remote data wiping and location tracking for signed-in devices, providing added protection against threats like virus-infected emails and phishing attacks.

II. LITERATURE SURVEY

Concerns over internet security and privacy have grown in recent years, and a lot of people are looking for solutions to protect their personal data. The Google account auto-logout extension is one such tool that might assist users in safeguarding their online personas.

The research on Google account extensions that automatically log users out is examined in the literature review. The advantages of the extension and the different approaches taken to create auto-logout capability are discussed. Furthermore, these extensions' efficacy in safeguarding users' security and privacy is examined.

A. Zakariae and Ahmed [1]

It employs this method to create the Random Password Generator. It makes use of the Kerberos V5 protocol, which relies on a user's single sign authentication instead of password authentication. It requires the production of two keys: the basic key is the first, and the derived key is taken from the basic key.

B. Thomas Groß [2]

They created it after thoroughly analyzing the Security Assertion Markup Language (SAML)-based Single-Sign protocol at the protocol level. Simpson and Gross conducted a poll to classify intentional and unintentional security flaws in Federated Identity Management (FIM) frameworks. They also offered solutions for those security incidents that were suggested by other people.

C. Shi et al.'s [3]

Their analysis looked at the SSO implementation weaknesses in mobile apps. They created and executed MoSSOT (Mobile SSO Tester), an automated black box security testing tool for Android apps that makes use of the SSO services offered by Facebook R, WeChat R, and Sina, three well-known service providers.

D. L. Ramamoorthi and D. Sarkar [4]

For the purpose of efficiently and successfully maintaining active SP and IDP sessions, a browser plugin is recommended. Through the use of a Single Sign-on (SSO) environment, an Identity Provider (IDP) authenticates a user for the first Service Provider (SP). The data that the IDP generates and keeps in an active IDP session is saved by the user's web browser. Every SP additionally creates and maintains one active service session.

TABLE 1 Summary of literature survey

SN	Paper	Advantages and Disadvantages
1.	Zakariae and Ahmed (2021) [1]	Benefits: One sign, cryptography, authentication each session of salt, Preventing dictionary, force, and brute-force assaults Its untrustworthy host and untrusted network are drawbacks, and the source has to be changed to call the proper Kerberos libraries.
2.	Thomas Groß (2020)[2]	Benefits: Single-Sign on based on Security Assertion Markup Language (SAML) analysis. Negative aspects include HTTP Referer Attack and connection hijacking. offers only partial defense against man-in-the-middle attacks.
3.	Shietal. (2020)[3]	Benefits: It examines the weaknesses in mobile apps that use SSO to access popular websites like Facebook, Google ID, and Google ID. Cons: App secrets leakage, shoddy authentication, and logical errors.
4.	L. Ramamoorthi and D. Sarkar (2020)[4]	Benefit: Alerting the User When Signing Out. IDP session validation during SP SIGN-OUT is triggered. Cons: More chance of account compromise; intricate system; human input necessary.

III. METHODOLOGY

The methodology for developing the browser extension entails initial requirement analysis to determine security needs, followed by research and design for architecture and functionality. Development involves coding features like automatic logout and alert mechanisms, with rigorous testing to ensure robustness and adherence to security standards. Deployment includes publishing on browser extension stores and providing user guidance. Continuous feedback-driven iteration, security monitoring, updates, and comprehensive documentation and support complete the process, ensuring a resilient and user-friendly solution.

A. System Architecture

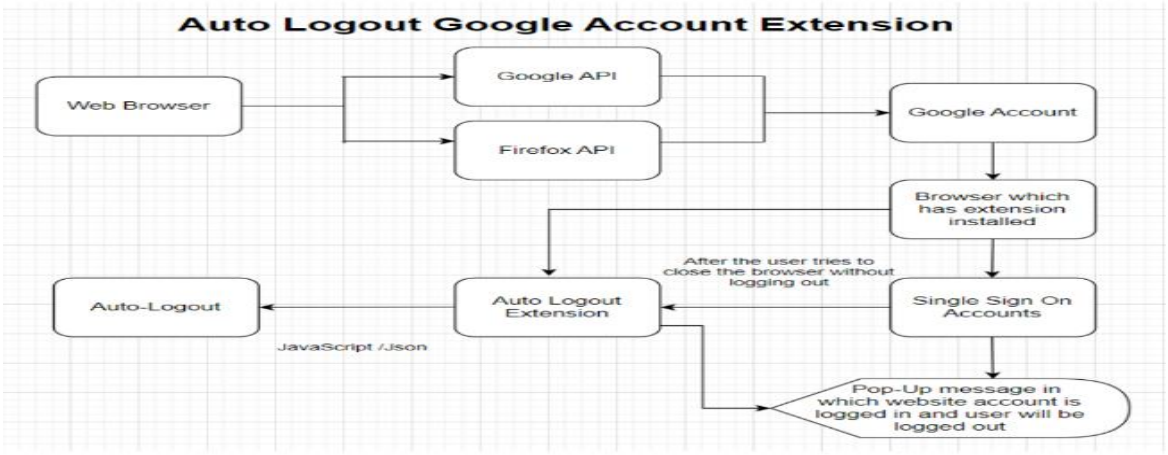


Fig 1 proposed architecture

1) Web browser: An internet browser is a piece of software that lets users view web pages and online services.
2) Google API: Google API gives developers access to the capabilities of numerous Google products, including Gmail, Drive, and Maps, and enables them to engage with Google services.
3) Google account: An account with Google gives you access to a number of Google services, including Gmail, Drive, and Documents.
4) Browser with extension installed: This system requires a browser with the Auto Logout extension installed in order to function. You can install the extension on well-known web browsers like Firefox and Chrome.
5) Single Sign-On (SSO): This technology minimizes the need for users to remember numerous usernames and passwords by enabling them to log in to numerous apps and services with only one set of credentials.
6) The Auto Logout extension is a browser add-on that, following a certain amount of inactivity, automatically logs users out of their Google accounts.
7) Pop-up message for logged-in accounts: When a user uses a public or shared computer, a pop-up notification can alert them to the fact that they are signed into their Google account and serve as a visual reminder to log out.
8) Auto Logout from account: To safeguard users' privacy and stop illegal access to their Google accounts, the Auto Logout extension will automatically log users out of their accounts after a certain amount of inactivity.

B. *Implementation Details*

a) *Describe the functionality:*

The first stage is to describe the extension's functionality in accordance with the project specifications. In this instance, when the browser is closed, the extension ought to log the user out of Gmail automatically. This method detects when the user shuts the browser window by utilizing JavaScript's "unload" event. The extension will log the user out when the event is triggered. This is how it operates:

- The extension watches for the browser window's "unload" event.
- The "unload" event is triggered when the user closes the browser window.
- The user's Google account is logged out when the extension recognizes the occurrence.

For instance, the extension will recognize the "unload" event and log the user out of their Google account if the user exits the browser window or tab.

b) *Browser Storage:*

The user's login credentials are kept in the browser's local or session storage by means of this technique. The extension has the ability to verify the storage after the user closes the browser and log them out if the data is lost. This is how it operates:

- The Google account extension saves the user's login credentials in the browser's storage once they log in.
- The extension looks for the user's login credentials in the storage when the user closes the browser.
- The extension locks the user out of their Google account if the information is no longer available.

For instance, the extension will search the browser's storage for the user's login credentials if they log in to it and then dismiss it. The extension will log the user out of their Google account if the information is no longer available.

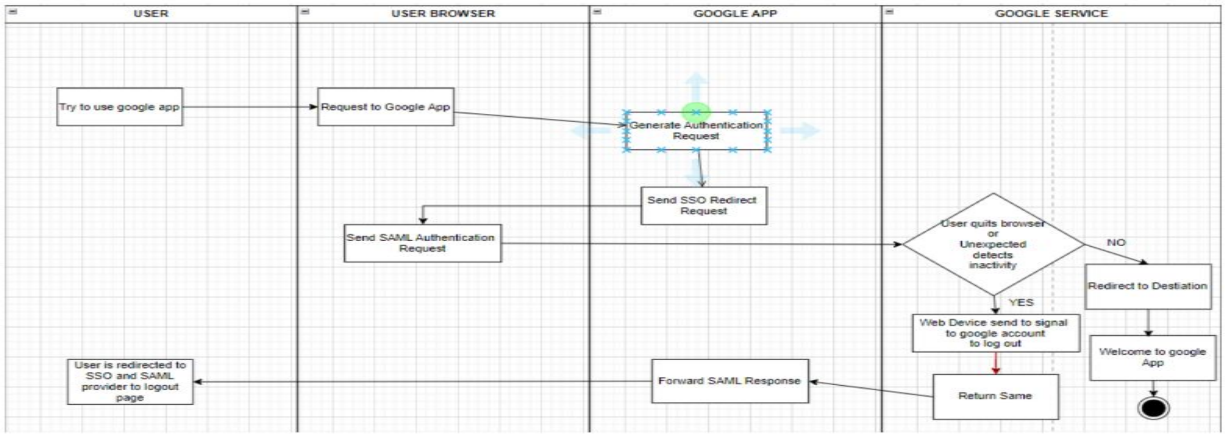


Fig 2 activity diagram

1) User uses browser- This is the starting point of the flowchart, indicating that a user is actively using the web browser.
2) Request to Google app - If the user tries to log in using their Google account, the website or application sends a request to the Google app.
3) Generate authentication request - The Google app generates an authentication request to verify the user's identity.
4) Send SSO Redirect Request - The authentication request is then redirected to a Single Sign-On (SSO) server.
5) Send SAML Authentication Request - The SSO server sends a Security Assertion Markup Language (SAML) authentication request to the user.
6) User quits browser or unexpectedly detects inactivity - If the user quits the browser or if there is no activity detected for a certain period, the system initiates a logout.
7) Web Device sends signal to Google account to log out - A signal is sent to the user's Google account to log out.
8) Return Same - A response is sent back to the SSO server.
9) Forward SAML Request - The SAML authentication request is forwarded to the Google app.
10) Web Device sends signal to Google account to log out - A signal is sent to the user's Google account to log out.
11) Redirect to Destination- If the user is still active and authenticated, the SSO service redirects the user back to the Google app or service they were trying to access.
12) Welcome to Google app- The user is then logged in and welcomed to the Google app or service. If the user has become inactive or quit the browser, they will be logged out automatically by the Auto Logout extension.

C. *Hardware and Software Specifications*

The experiment setup is carried out on a computer system which has the different hardware and software specifications as given in Table 3.1 and Table 3.2 respectively.

TABLE 3.1 hardware details

Processor	i5 10th gen processor
HDD	512 GB
RAM	4 GB

TABLE 3.2 software details

Operating System	Windows 10
Programming Language	Javascript, JSON

IV. RESULTS AND DISCUSSION

A. *First browser: Gmail account Login*

Installing our extension in your browser is the first step. Depending on your browser, the installation process could be different (e.g., Chrome, Firefox, Edge). Usually, the browser on your machine has to have our extension installed.

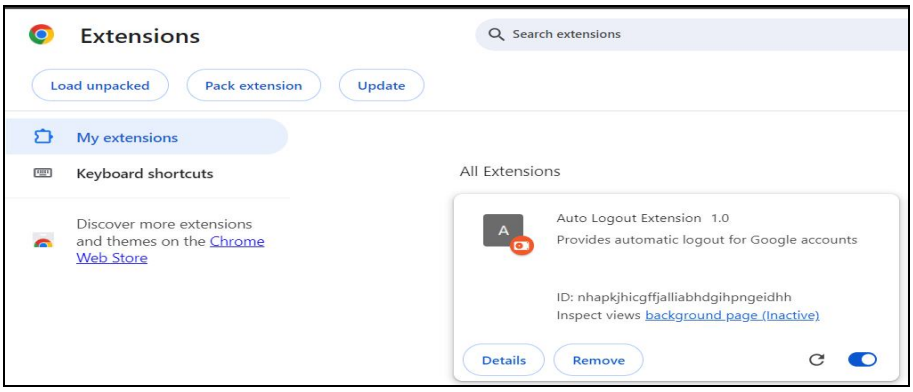


Fig 3.1 extension loading page

You can now access your Gmail account by signing in. To log in, open a new tab or window, go to https://mail.google.com, the Gmail website, and enter your email address and password.

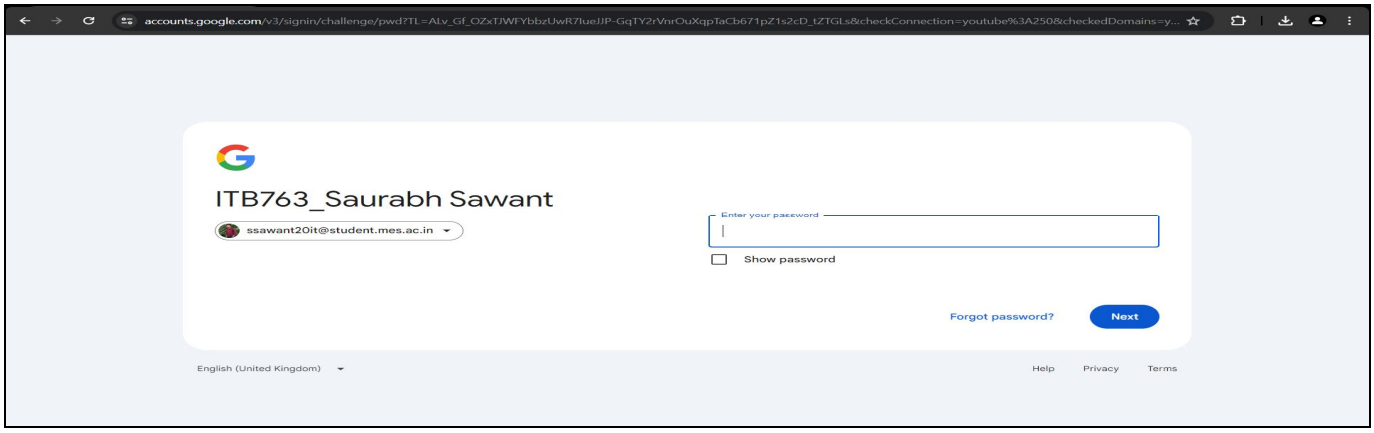


Fig 3.2 account login

B. Extension for auto logout

To utilize the extension, click on its icon in the browser's toolbar after logging into Gmail. Depending on what it is used for, the extension could offer different features or functionalities linked to Gmail or other online tasks.

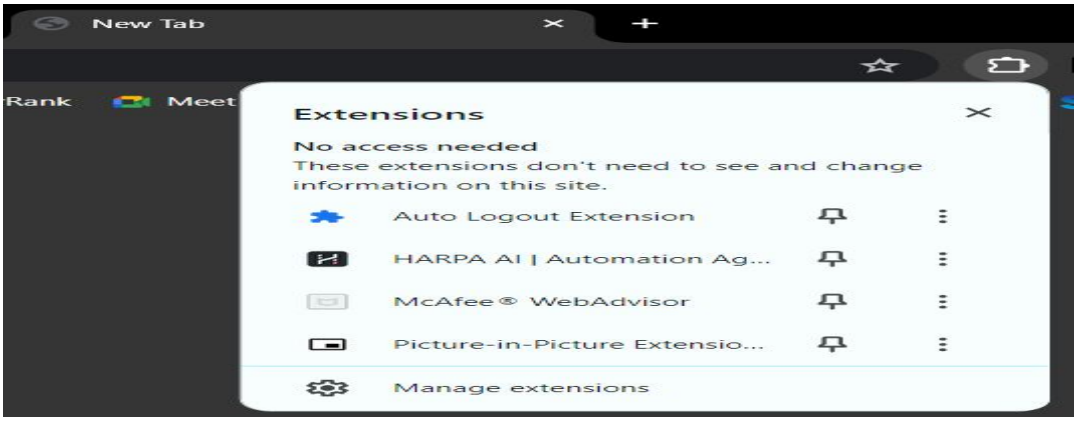


Fig 3.3 loaded extension

C. List of active tabs

You may examine all of the accounts that are currently logged in by clicking on the extension icon, which will cause a list of open tabs to appear. Additionally, you can quickly log out by clicking on the handy button we've included.

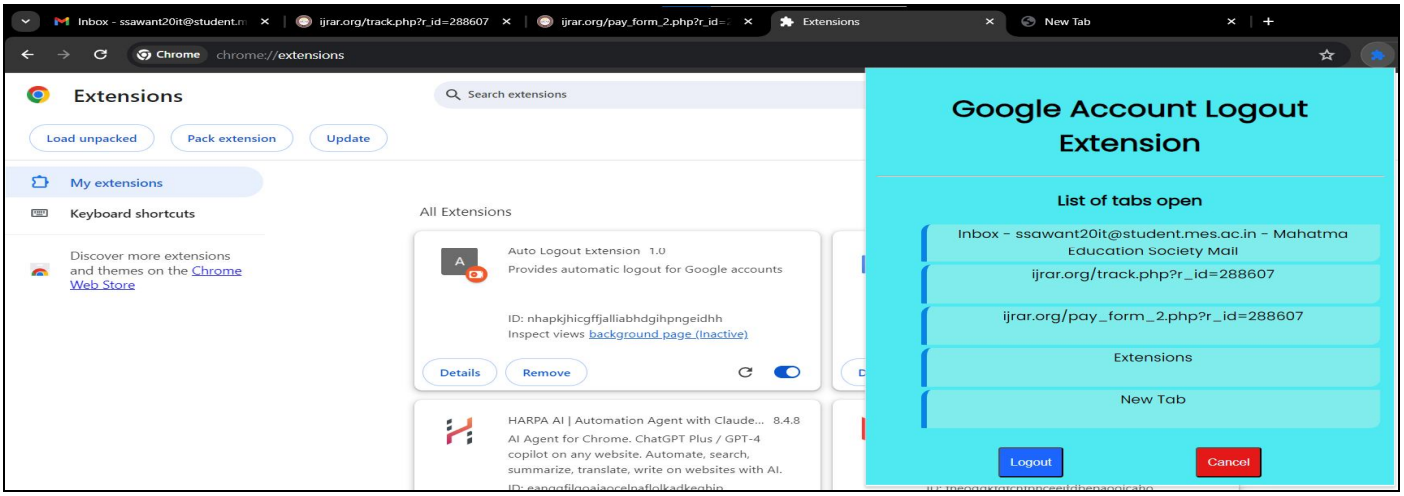


Fig 3.4 extension view

D. Second browser: Mozilla Firefox

The installation process for this extension is comparable to that of the Chrome browser and may also be done in the Firefox browser. It operates in the same manner as Chrome.

Fig 3.5 firefox browser extension loading page

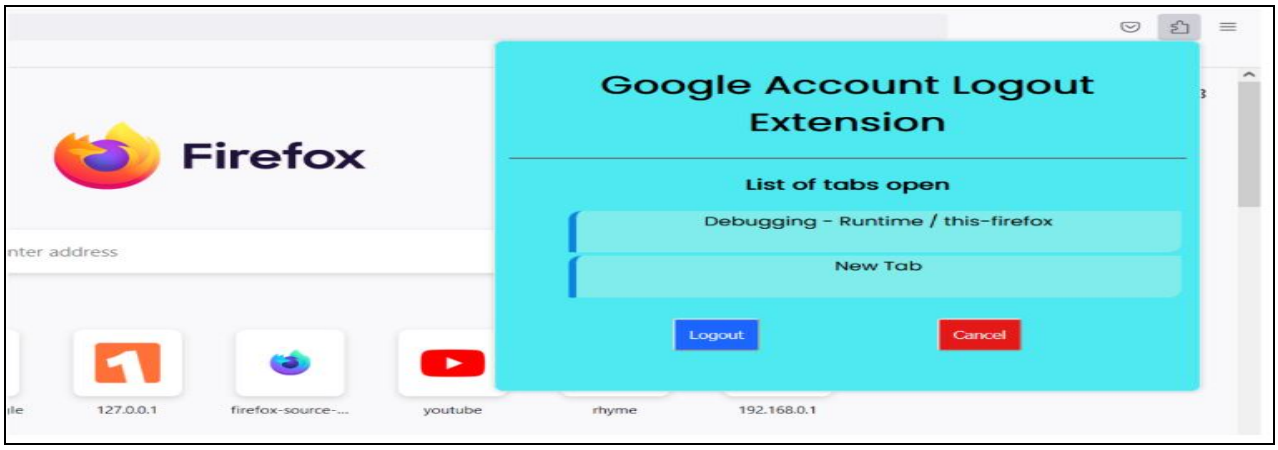


Fig 3.6 extension view in firefox

E. Google Account closed

You can sign out of all logged-in accounts at once by either closing the browser completely or clicking the logout button. Your privacy and security are ensured since you will notice that you have been logged out of those accounts when you open the browser again.

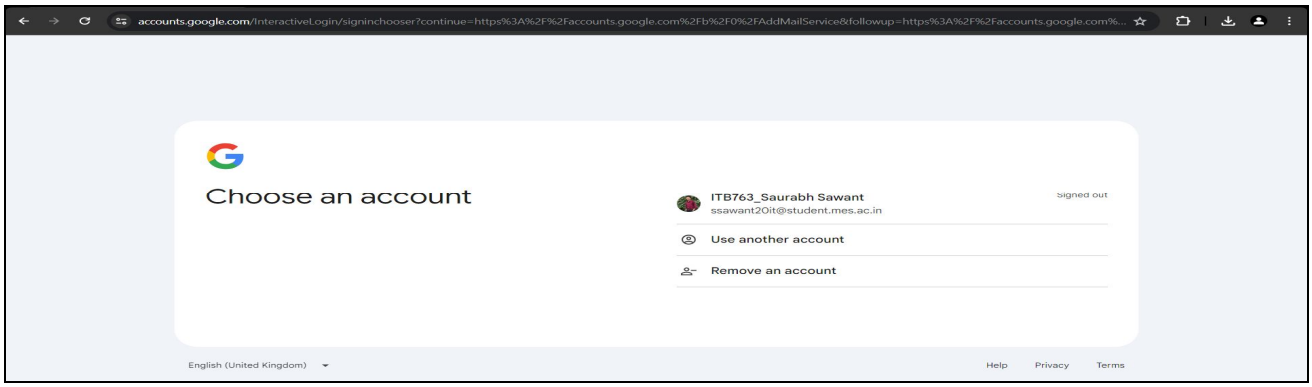


Fig 3.7 account logged out

V. CONCLUSION

The goal of the project report is to create a Google account extension that automatically logs users out when they use shared or public computers, protecting their privacy and security. The extension will be made to automatically remove users from their Google accounts following a certain period of inactivity, lowering the possibility of data breaches and unwanted access.

The first section of the paper highlights the issue of keeping Google accounts open on shared or public computers, which might expose private data. The paper then goes into the different ways that solutions are already accessible, like utilizing a password manager or manually logging out, before offering the auto-logout extension as a more secure and convenient choice.

The study describes the technical specifics of the extension, such as its user interface, compatibility with various browsers, and interaction with Google security mechanisms. It also goes into the difficulties encountered and how they were resolved during the development process.

In the report's conclusion, it is discussed how the auto-logout extension might help users feel more secure and at ease, as well as how it might influence the community at large by encouraging safe online behavior. The research concludes by outlining some potential directions for the extension's future development, such adding more security measures or enhancing its interoperability with other services.

VI. ACKNOWLEDGMENT

We would like to express our special thanks to our major project guide Prof. K.S Charumathi who guided us through the project and who helped us in applying the knowledge that we have acquired during the semester and learning new concepts.

We would like to express our special thanks to Dr. Satishkumar Varma, Head, Department of Information Technology, who gave us the opportunity to do this major project because of which we learned new concepts and their application.

We are also thankful to our major project coordinator Prof. Sheetal Gawande along with other faculties for their encouragement and support.

Finally we would like to express our special thanks to Principal Dr. Sandeep Joshi who gave us the opportunity and facilities to conduct this major project.

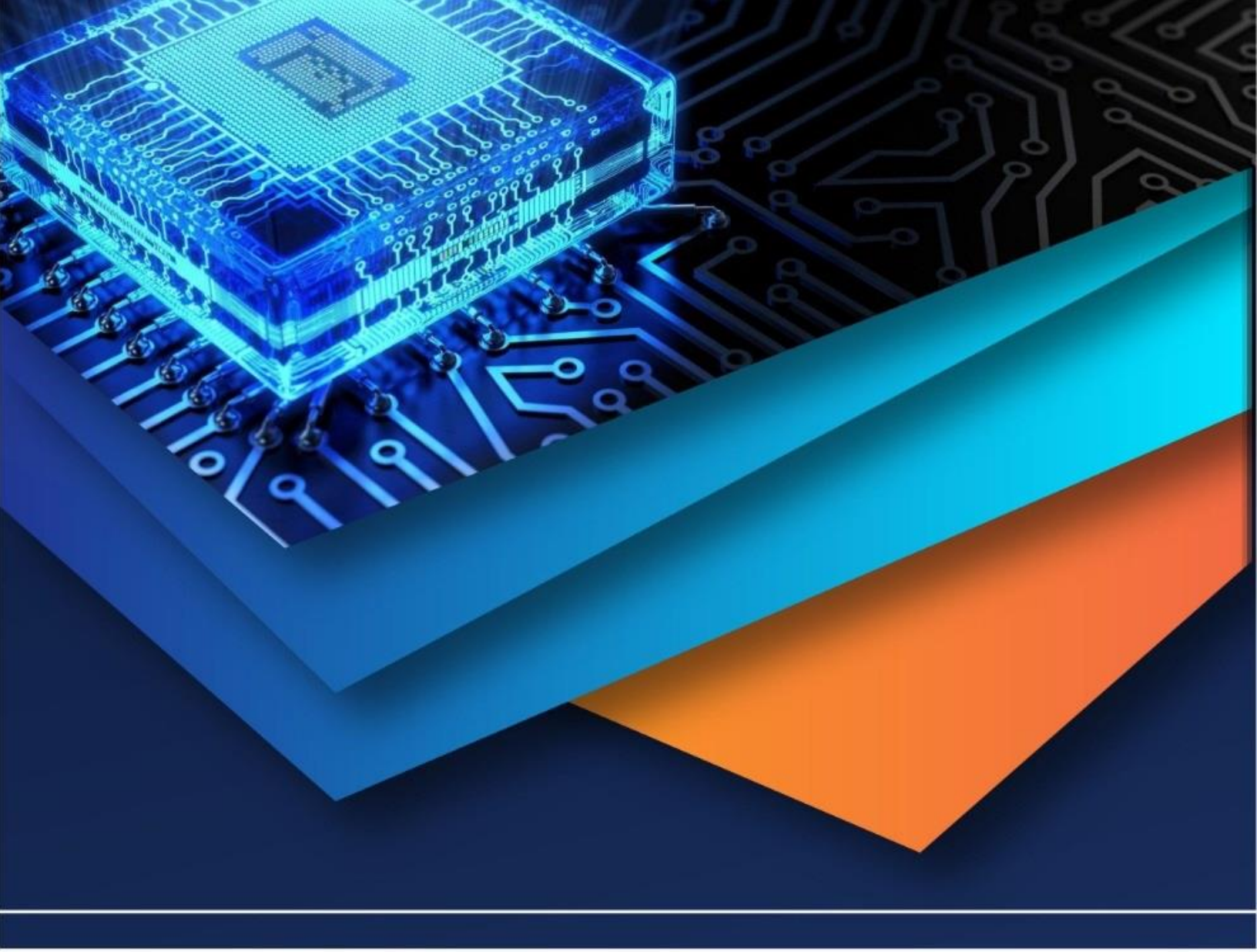
REFERENCES

[1] Zakariae TBATOU, Ahmed ASIMI, Younes ASIMI, Yassine SADQI “Kerberos V5 :Vulnerabilities and perspectives” 978-1-4673-9669-1/15/$31.00 ©2021 IEEE

[2] T. Groß, ‘‘Security analysis of the SAML single sign-on browser/artifact profile,’’ in Proc. 19th Annu. Computer. Security. Appl. Conf., 2020, pp. 298–307.

[3] Shietal., A. Madhu, and J. J. Kizhakkethottam, ‘‘Security issues of single sign on Web services,’’ in Proc. Int. Conf. Soft-Comput. Netw. Secur. (ICSNS), Feb. 2020, pp. 1–4

[4] L. Ramamoorthi and D. Sarkar, ‘‘Single sign-on implementation: Leveraging browser storage for handling tabbed browsing sign-outs,’’ in Developments and Advances in Defense and Security, Á. Rocha and R. P. Pereira, Eds. Singapore: Springer, 2020, pp. 15–28.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY