Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v.11 n.54, p. 89-97. July/August., 2025.

DOI: https://doi.org/10.5935/jetia. v11i54.1732

RESEARCH ARTICLE OPEN ACCESS

PERSONAL SECURITY CHECKLISTA COMPREHENSIVE APPROACH TO DIGITAL SECURITY

Hitesh Choudhary[1], Navish Ansari[2] and Shraddha Sandimani[3]

[1,3,4] Department of Information Technology, Universal College of Engineering, University of Mumbai, Vasai. India.
[2] University of Mumbai, Mumbai. India.

[1]https://orcid.org/0009-0002-0669-4288, [2]https://orcid.org/0009-0004-0256-9417, [3]http://orcid.org/0009-0003-3890-1736

Email: choudhaaryhitesh557@gmail.com, ansarinavish571@gmail.com, shraddhasandimani@gmail.com

ARTICLE INFO

Article History
Received: March 19, 2025
Revised: April 20, 2025
Accepted: June 15, 2025
Published: July 31, 2025

Keywords:
Digital Security,
Cybersecurity,
Personal Security,
Two-Factor Authentication,
Secure Browsing,
User Awareness,
Data Protection.

ABSTRACT

In today's hyper-connected society, protecting personal data is not only essential, but a continuous challenge. This article presents the design, development and evaluation of the "Personal Safety Verification List", a comprehensive web -based platform that enables users to identify vulnerabilities in their digital lives and implement robust safety measures. The system categorizes tasks on three levels - essential, optional and advanced - areas such as authentication, safe navigation, messages, social media protection and safety of physical devices. Taking advantage of modern technologies such as React.JS, Next.JS, TypeScript and Chart.JS, the platform offers real -time progress tracking through dynamic views. Extensive tests and user's iterative feedback indicate that this integrated solution not only increases the awareness of cyber security, but also motivates proactive behavior, simplifying complex protection strategies.

I. INTRODUCTION

I.1 BACKGROUND

The advent of digital technologies revolutionized the way we interact, communicate and conduct business. With the rapid expansion of on -line services and the omnipresence of mobile devices, sensitive personal information is now stored and transmitted by digital networks on an unprecedented scale. However, this digital revolution has inherent risks of crimes, data violations and identity theft are widespread concerns. Current security solutions usually address only unique aspects of digital protection, resulting in a fragmented security scenario that places the burden of user integration. The "Personal Security Verification List" is designed to fill this gap, consolidating various security measures in a friendly interface, thus allowing comprehensive digital protection [1],[2].

I.2 RATIONALE

Traditionally, safety tools demand user engagement across disparate applications with unique complexities and UI. This division is too much for not -technical users, who must have clear instructions. Specific events in the world of cyber security have highlighted the vulnerable nature of many systems, their complexity and failure to integrate. That's where the "Personal Security Verification List" helps: it groups security elements together in a single panel, so it's no longer complex to be digital safety practices and motivates users to deal with potential threats before they manifest [3], [4].

I.3 SCOPE AND RELEVANCE

This research targets individuals, families and even micro enterprises that require adequate digital security services but do not have the budget for full-fledged corporate solutions. The world we live in today is always evolving, and so are cyber threats, which is why

there is a need for a tool that not just trains users in best practices, but also monitors and updates in real time. The “Personal Security Verification List” is an educational tool- it features assets such as progress bars and radar charts, which assist users in surveying and enhancing their safety posture. This double function feature is especially important in the world of rapidly changing technology [5],[6].

II. OBJECTIVES

The "Personal Security Verification List" project has the following main goals and objectives:

- **Develop Security Policies:** Create a verification list covering essential areas, which includes authentication, safe web browsing, message security, social media account privacy, and device safeguarding [1]
- **Educate and Empower the User:** Outline and provide step-by-step instructions for each protective action that aims at empowering the users so as to help them practice effective safety measures [4].
- **Enable real-time Interactive Progress Tracking:** Add graphically appealing components such as, a radar chart and progress bar and panel whereby the users can monitor their level of safety in real-time [7].
- **Provide a coherent and simple end-user experience:** Provide an interface that combines a variety of safety features and offers great usability to individuals regardless of their technical skills [2].
- **Ensure extend ability and future inclusion:** Build the system on modular design principles so that additional options can be added in the future, such as, network scanning capabilities or real-time assessments of the strength of passwords for the changing cyber security environment [3],[5].

III. LITERATURE SURVEY

According to explore the effectiveness of multi-factor authentication (MFA) in reducing unauthorized access while also addressing its usability challenges. Their findings highlight the need for authentication systems that are both secure and user-friendly, a balance that is critical for widespread adoption [1]. According to investigate techniques such as ad blocking and script blocking, as well as the use of secure browsers like Brave and Tor, to enhance user privacy. Their research illustrates the increasing demand for robust privacy measures in an era where online tracking is pervasive [3]. Discuss advanced encryption methods to secure email communications, while examine the challenges and benefits of implementing end-to-end encryption in messaging apps. These studies underscore the importance of balancing high-level security with usability in everyday communication tools [5], [8]. Analyze how privacy settings on social media platforms can be optimized to protect personal data while still maintaining user engagement. Their work demonstrates that proper configuration can significantly reduce exposure to cyber threats [9]. Miller and Johnson (2021) provide a comprehensive review of cybersecurity trends, emphasizing the need for adaptive and integrated security solutions that can quickly respond to emerging threats.[6] Lee and Kim (2022) delve into recent advancements in real-time data encryption and secure data handling. Their study highlights the importance of a robust backend system that supports dynamic updates and secure information processing [7]. According to evaluate various user-centric security models, underscoring the significance of designing tools that are accessible and intuitive for non-technical users [2]. Argue that integrating multiple security measures into a single platform can significantly enhance overall digital protection by positively influencing user behavior and reducing redundancy [10]. Emphasize that effective user education is a critical component of any cybersecurity strategy. They show that well-informed users are less likely to fall victim to cyber threats and more likely to adopt proactive security measures [4].

IV. EXISTING SYSTEMS

IV.1 OVERVIEW OF CURRENT SOLUTIONS

The digital security landscape today is dominated by several niche tools, such as antivirus programs, MFA apps and VPN services. These independent solutions beget results for their particular domains, but typically demand users to leverage multiple applications that can't star as well. Security best practices are also not very well documented and are split across many documents that provide fragmented and often contradictory approaches [3], [2].

IV.2 GAPS IN EXISTING SYSTEMS

The following table outlines the limitations observed in existing digital security solutions:

Table 1: Gaps in Existing Systems.

Aspect	Current Approach	Limitation
Standalone Tools	Antivirus, MFA apps, VPN services	Lack integration; users must manage multiple uncoordinated applications [3].
Security Guidance	Dispersed information across various sources	Fragmented advice leads to inconsistent security practices [5].
User Interface	Complex, technical designs	High complexity deters non-expert users from full adoption [2].
Dynamic Updates	Static, infrequently updated content	Outdated guidelines that do not rapidly adapt to emerging threats [6].

Source: Authors, (2025).

V. PROBLEM STATEMENT

Despite the multitude of available digital safety tools and guidelines, it remains a critical need for a unified and easy -to -use platform that comprehensively addresses all aspects of personal digital security.

- **Users face various challenges:** Sources of fragmented information: The need to consult various uncoordinated resources usually results in incomplete and inconsistent security practices, leaving gaps in general protection [5].
- **Usability barriers:** Many advanced security systems require high technical proficiency, making them inaccessible to the average user who needs clear and simple guidance [2].
  Threats in rapid evolution: Cyber threats are continually emerging and evolving, but many existing solutions are static and slow to update, making them less effective in real-time defences [6].

This project aims to fill these gaps, creating an integrated platform that consolidates best practices, educational content and real -time monitoring in a comprehensive solution [1], [4].

VI. LIMITATIONS OF EXISTING SYSTEMS

Current digital security solutions have many remarkable disadvantages:

- **Separate functionality:** Many existing equipment operates independently, providing a safety method that usually ignores significant weaknesses due to lack of integration [3].
- **Excessive complexity:** The very technical nature of many applications creates a clear learning state, which discourages everyday users to join these devices perfectly [2].
- **Insecure and stable material**: Based on static and old guidelines, many systems are not compatible with new threats, which reduces their general efficiency in today's rapid change [6].
- **User's sub -optimal experience:** Scented security advice and very complex interfaces significantly reduce the user's participation, resulting in insufficient protection [8].

VII. PROPOSED SYSTEM

VII.1 SYSTEM OVERVIEW

The “Personal Security Verification List” has been designed as a comprehensive and web-based application that unifies all aspects of digital security on an affordable platform. This system guides users step by step by, ensuring their digital lives, providing practical tasks and educational content in a single integrated environment [1].

VII.2 KEY FEATURES

- **Comprehensive Checklist:** The machine organizes safety responsibilities into 3 degrees—Essential, Optional, and Advanced—covering vital domains inclusive of authentication, steady net surfing, messaging privacy, social media protection, and bodily device protection [9].
- **User-Centric Interface:** Featuring a smooth, responsive dark mode layout, the platform is optimized for both computer and cellular use, enhancing usability and decreasing visible fatigue [2].
- **Real-Time Progress Tracking:** Dynamic visualizations, which include radar charts and development bars, provide users instant comments on their security posture, allowing them to screen improvements and quick discover areas requiring similarly interest [7].
- **Educational Content:** Each safety project is observed by using distinct, smooth-to-apprehend steering, practical tips, and links to additional sources, empowering users to implement the endorsed measures efficiently [4].
- **Scalability:** The modular design of the platform permits for the seamless integration of future upgrades, which includes network scanning equipment and real-time password power reviews, ensuring the gadget remains adaptive to new cyber threats [10].

Table 2: Key Features.

Feature	Description	Benefit
Comprehensive Checklist	Categorizes tasks into Essential, Optional, and Advanced levels	Provides a structured security roadmap [9]
User-Centric Interface	Clean, responsive dark mode design	Enhances accessibility and ease of use [2]
Real-Time Progress Tracking	Radar charts and progress bars that update live	Allows for continuous monitoring of security improvements [7]
Educational Content	Detailed guidance and practical tips for each task	Empowers users with actionable security knowledge [4]
Scalability	Modular design supporting future integration	Future-proofs the system against emerging threats [10]

Source: Authors, (2025).

VII.3 SYSTEM ARCHITECTURE

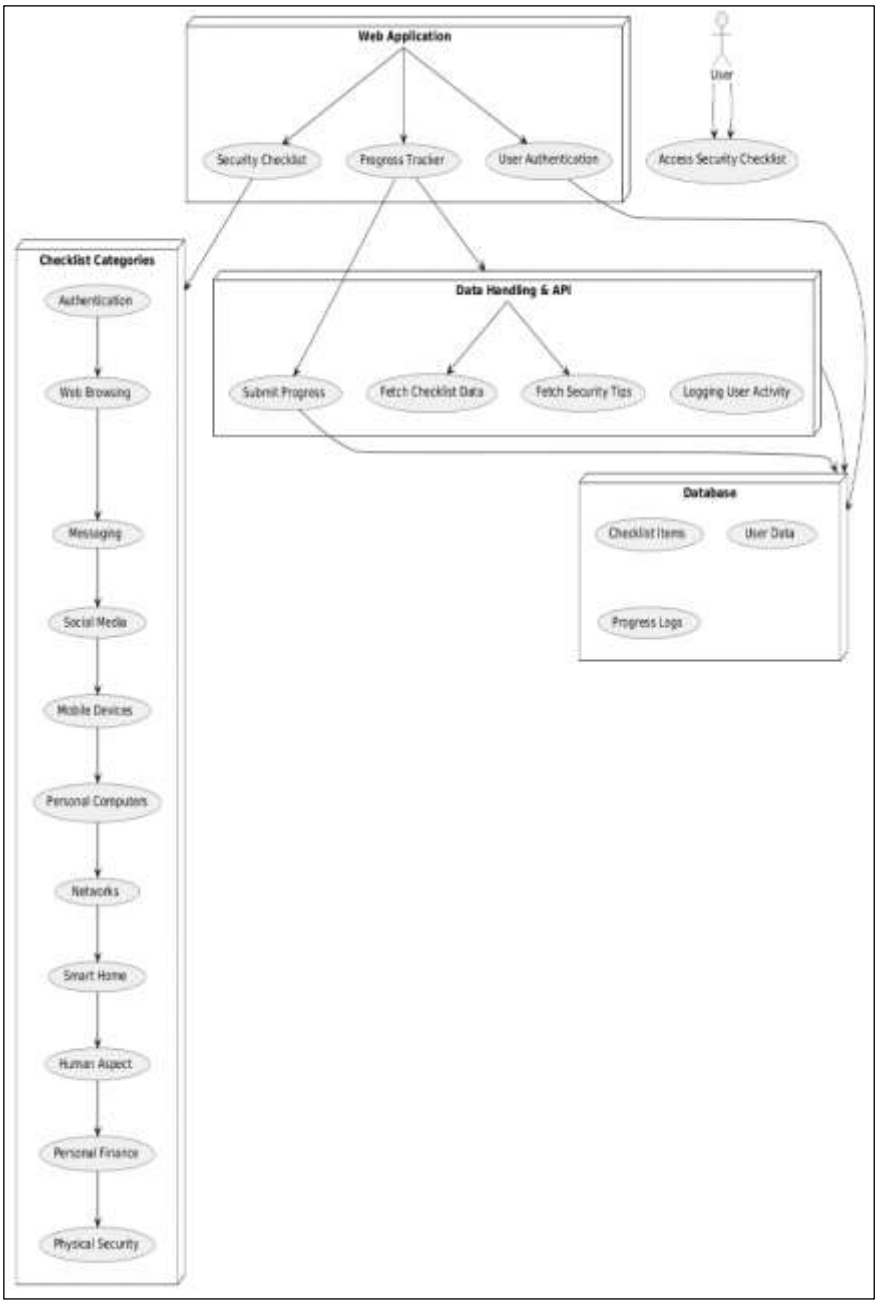

Figure 1: Personal Security Checklist System Architecture.
Source: Authors, (2025).

The structure of the web application made for tracking safety checklists is highlighted in the given diagram. Its components are defined as follows:

User interaction: Through the web application, a user can get access to the security check list.

Web application:
Three modules comprise the basic framework:
Safety Checklist: Documents all security task efforts undertaken by the user.
Pragati Tracker: Users assesses completion progress.
User authentication: Restricts access to authorized users only.
Data Handling and API Responsible for:
Presenting progress: Full position users have reached is updated by the users.
Getting checklist data: Check list item gets recurred.
Getting safety tips: Recommendations and best practices for security are rendered.
Logging User Activity: Trackable actions are logged.

Database Store:

- **Checklist Items:** Safety Procedures.
- **User data:** basic and detailed account data.
- **Pragati Log:** User Input activity record.

Checklist categories:

1. Authentication
2. Web Browsing
3. Email
4. Messaging
5. Social Media
6. Networks
7. Mobile Devices
8. Personal computing
9. Smart Homes
10. Personal Finance
11. Human aspect
12. Physical surveillance

As a result of this approach, the users are provided with the ability to track their safety practices, receive guidance, and assistance in monitoring the progress towards their targets in a secure manner. I can help you by providing more detailed information on any part if you want!

The architecture is designed to be both modular and scalable:

- **Frontend:** Developed with React.js and Next.js (using server-side rendering for faster performance) and written in TypeScript. Dynamic visualizations are powered by Chart.js. [1].
- **Backend:** A Node.js server manages authentication, data storage, and API calls, while MongoDB (or a similar NoSQL database) securely stores user data and checklist information [5].
- **Security Measures:** The platform integrates strong encryption and secure authentication methods (including 2FA) to ensure user data remains protected [8].

VIII. METHODOLOGY

VIII.1 DEVELOPMENT PROCESS

Our development technique became iterative and centered on the consumer, which includes numerous key levels:

- **Requirements Analysis:** Comprehensive research and interviews were performed to understand the not unusual digital safety challenges faced via customers. A tremendous revision of the educational literature and present structures have helped to outline the principal requirements for the system [1].
- **System Design:** Detailed wireframes, data flow diagrams (DFD) and use case diagrams have been designed to map the gadget architecture and consumer interactions. The design emphasized clarity, simplicity and simplicity of use [3].
- **Implementation:**
    - **Frontend Development:** The user interface was built the usage of React.Js and Next.Js, with TypeScript ensuring robustness and code renovation. The layout changed into optimized for response capacity among desk and furnishings devices [2].
    - **Backend Development:** An Node.JS server, supported by a MongoDB database, has been applied to manipulate user information and facilitate real-time updates from the safety tick list [5].
- **Test and Evaluation:** Strict tests had been achieved using the Jest and Reaction Test Library. Pilot customers supplied feedback that became usually incorporated to refine the platform [7].
- **Implementation and tracking:** The software turned into applied on a scalable cloud platform, and non-stop monitoring has been hooked up to tune overall performance, time of pastime and person involvement, making sure a super experience. [10]

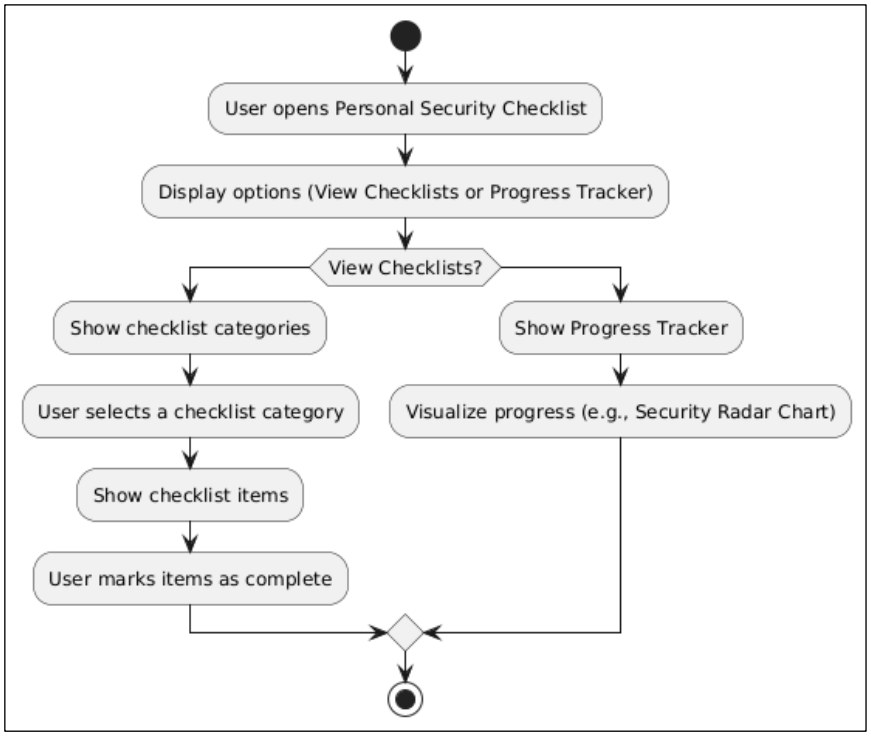

Figure 2: Flowchart of Personal Security Checklist.
Source: Authors, (2025).

This flowchart represents the user journey through the Personal Security Checklist web application. It visually explains how a user interacts with the system to either check security tasks or track their progress.

Step-by-Step Explanation of the Flowchart

1. **User Opens the Personal Security Checklist**

- The journey begins when the **user accesses the security checklist application**.
- This could be by **logging in** or **navigating to the checklist page**.

2. **Display Options: View Checklists or Progress Tracker**

- The system presents two choices:
- ☑ **View Checklists** – If the user wants to see security tasks and complete them.
- ☑ **Progress Tracker** – If the user wants to track their security improvements.

3. **Decision Point: Does the User Want to View Checklists?**

- The user decides between:
  - **"Yes" → View and complete security tasks**
  - **"No" → Check progress using Graphs**

Path 1: Viewing & Completing Security Checklists

If the user chooses to view the checklists:

Show Checklist Categories – The system displays security topics (e.g., Password Security, Social Media Safety, Financial Security).
User Selects a Category – The user picks a topic they want to improve.
Show Checklist Items – A list of security tasks appears for that category.
User Marks Items as Complete – Once a task is done, the user checks it off.
Example:

- The user selects **"Mobile Security"**
- Checklist item: "Enable Two-Factor Authentication"
- The user enables it and marks it as **completed** ☑

Path 2: Tracking Progress

If the user chooses to track progress:

Show Progress Tracker – The system loads a visual representation of progress.

Visualize Progress (e.g., Security Radar Chart) – The system displays security strengths and areas needing improvement.
Example:

- A radar chart shows that the user has completed 80% of Social Media Security but only 20% of Financial Security.
- This encourages the user to focus on weaker areas.

Final Step: The Process Loops

- Whether the user completes tasks or tracks progress, the system updates accordingly.
- The cycle continues until the user has completed all security tasks.

IX. RESULTS AND DISCUSSIONS

IX.1 IMPLEMENTATION RESULTS

Following the deployment of the "Personal Security Checklist," sizable checking out produced several noteworthy outcomes:

- **User Engagement:** Users always interacted with the platform, frequently revisiting educational content material and updating their safety settings. The dynamic visual tools, which includes radar charts and progress bars, effectively inspired users to finish duties and tune upgrades over time [4].
- **Usability:** The responsive dark mode interface turned into widely preferred for its simplicity, ease of navigation, and aesthetic attraction. Feedback from users with various stages of technical understanding confirmed that the tiered method (Essential, Optional, Advanced) helped them apprehend and manage their virtual safety more correctly.[8]
- **System Performance:** Technical reviews confirmed fast page load times, easy actual-time updates, and typical machine reliability. The effective integration of contemporary web technology with a robust backend architecture contributed to a high-overall performance platform that met user expectations [7].

IX.2 DISCUSSION

The findings suggest that an included, person-pleasant safety platform can significantly decorate private digital safety. By consolidating disparate security features into one complete interface, the "Personal Security Checklist" addresses the fragmentation common in modern-day answers. The inclusion of precise instructional content material demystifies complex security practices, constructing person self-belief and encouraging proactive engagement. Moreover, the platform's scalable design ensures it stays effective as new threats emerge, positioning it as a long-term answer for digital security [3],[8], [4].

Figure 3: Home Page of Personal Security Checklist.
Source: Authors, (2025).

The Personal Security Checklist make sure that your data is not been breached and leaked by any third party. The home page is consist of Progress bar, Graphs and Security Lists where the user can see there security of there any application and devices.

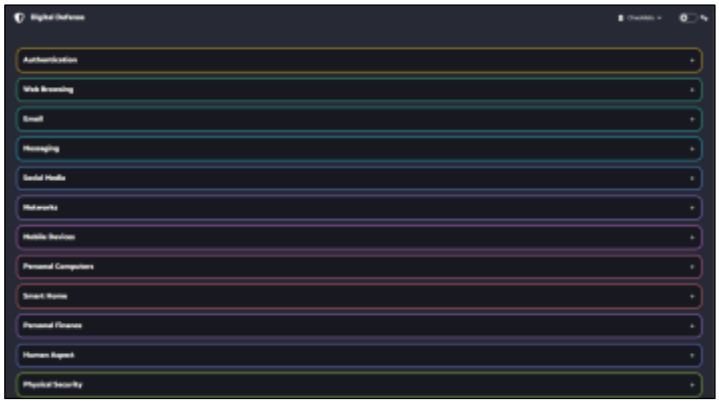

Figure 4: Category of Personal Security Checklist.
Source: Authors, (2025).

This Fig show the list of Personal Security Checklist where the user can choose any type of security from the category the user can choose the security and make the checlist more useful by checking the list which is been secure by the user. There are 3 Types of securtiy which is Essential, optional and advanced.

X. PERFORMANCE METRICS

To make certain continuous development, the subsequent key performance metrics are monitored:

- **User Engagement:** Active person counts, session durations, and the frequency of checklist completions are tracked to assess the platform's standard engagement and effectiveness in motivating users to take action. [4]
- **System Responsiveness:** Metrics including web page load times, replace latency, and gadget uptime are measured frequently to make certain a seamless person enjoy throughout all devices. [7]
- **Security Effectiveness:** The ratio of a success logins to unauthorized access attempts is constantly analyzed, in conjunction with periodic protection audits, to verify the gadget's integrity and effectiveness in defensive consumer data. [8]
- **User Satisfaction:** Surveys, net promoter rankings (NPS), and qualitative feedback are accrued and analyzed to assess consumer delight and discover potential areas for future enhancement. [10]

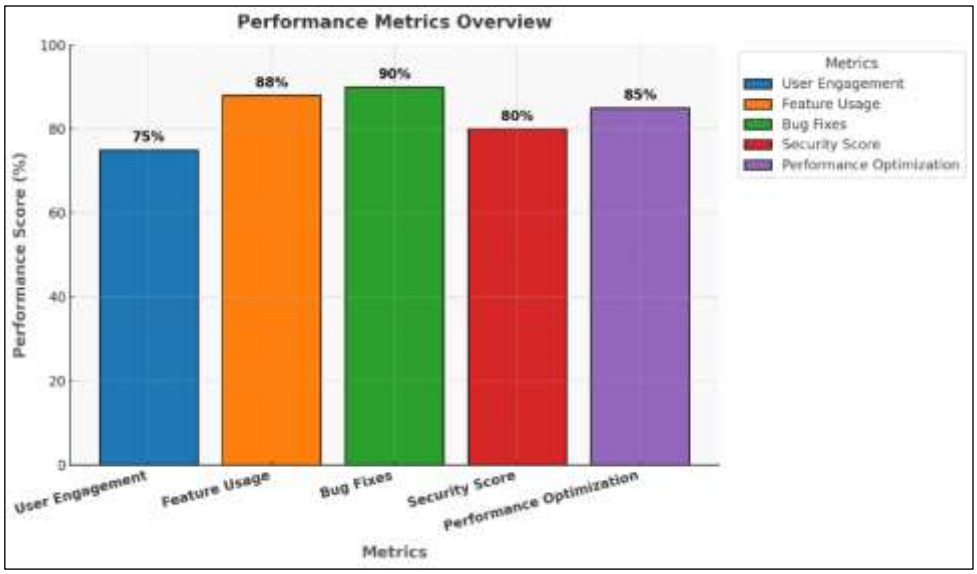

Figure 5: Performance Metrics.
Source: Authors, (2025).

XI. CONCLUSION

The "Personal Security Checklist" affords an progressive and integrated approach to virtual security through unifying multiple defensive measures into a unmarried, interactive platform. Our studies demonstrates that clear, actionable guidance paired with real-time progress tracking drastically enhances customers' capacity to stable their virtual lives. Early testing shows excessive stages of consumer engagement, usability, and delight. Moreover, the device's scalable and modular design guarantees it stays adaptable in the face of rising cyber threats. Continued improvement, together with planned future upgrades, will similarly fortify this platform as an vital device for complete digital protection.[5][6]

Future research and improvement for the "Personal Security Checklist" include:

- **Enhanced Network Scanning:** Integrating community scanning gear to locate vulnerabilities in home and business networks.
- **Real-Time Threat Intelligence:** Incorporating feeds of real-time hazard intelligence to replace security recommendations and alert users of latest dangers.
- **Advanced User Analytics:** Developing greater sophisticated analytics to higher recognize person behavior and tailor instructional content as a consequence.
- **Mobile Application Development:** Extending the platform to a dedicated cellular app to similarly improve accessibility and usefulness on smartphones and capsules.
- **User Training Modules:** Creating interactive education modules and webinars to similarly teach users on emerging cybersecurity threats and excellent practices.

XII. AUTHOR'S CONTRIBUTION

- **Conceptualization:** Mr. Hitesh Choudhary and Mr. Navish Ansari.
- **Methodology:** Mr. Hitesh Choudhary and Mr. Navish Ansari.
- **Investigation:** Mr. Hitesh Choudhary and Mr. Navish Ansari.
- **Discussion of results:** Mr. Hitesh Choudhary, Mr. Navish Ansari and Ms. Shraddha Sandimani.
- **Writing – Original Draft:** Mr. Hitesh Choudhary, Mr. Navish Ansari and Ms. Shraddha Sandimani.

- **Writing – Review and Editing:** Mr. Hitesh Choudhary, Mr. Navish Ansari and Ms. Shraddha Sandimani.
- **Resources:** Mr. Hitesh Choudhary and Mr. Navish Ansari.
- **Supervision** Mr. Hitesh Choudhary, Mr. Navish Ansari and Ms. Shraddha Sandimani.
- **Approval of the final text:** Mr. Hitesh Choudhary, Mr. Navish Ansari and Ms. Shraddha Sandimani.

XIII. REFERENCES

[1] Harrison, D. & Collins, A. (2024). *Authentication: Strengthening Access Control with Multi-Factor Authentication.* Cybersecurity in the Digital Age.

[2] Wang, L. & Patel, R. (2020). *Evaluating User-Centric Security Solutions: A Comparative Analysis.* Cybersecurity Journal.

[3] Brooks, N. & Thompson, L. (2023). *Privacy-First Web Browsing Techniques.* Navigating the Invisible Web.

[4] Davis, M. & Robinson, T. (2023). *The Role of User Education in Cyber Threat Mitigation.* Journal of Digital Security.

[5] Jameson, O. & Reynolds, S. (2022). *Securing Emails: Strategies to Prevent Phishing and Data Breaches.* Guardians of the Inbox.

[6] Miller, A. & Johnson, B. (2021). *Cybersecurity Trends in the Digital Age: A Comprehensive Review*. Journal of Cybersecurity Research.

[7] Lee, S. & Kim, H. (2022). *Advances in Real-Time Data Security and Encryption*. Journal of Information Security.

[8] Foster, L. & Bennett, S. (2024). *Ensuring End-to-End Messaging Privacy*. Whispers in the Digital World.

[9] Turner, E. & Clark, M. (2023). *Social Media: Navigating Privacy and Exposure on Online Platforms.* The Social Labyrinth.

[10] Martinez, C. & Gomez, F. (2021). *Integrated Security Systems and Their Impact on User Behavior.* International Journal of Cybersecurity.