IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study Of The Intersection Between Usability And Security In Modern Online Applications

[1]Muskan Ostwal, [2]Mansi Garg, [3]Shirsaa Saha
[1]BTech CSE student, [2]BTech CSE student, [3]BTech CSE student
[1]Department of Computer Science and Engineering
[1]SRM University Sonipat, Delhi-NCR, India

***Abstract**:* Online applications are now at the center of life, personal and professional, offering unprecedented convenience but indeed significant security and privacy challenges in this digital era. The constant integration of billions of devices into everyday interactions by IoT and 5G networks has expanded the scope of connectivity. Increased use of such technologies has increased the rate of cyber threats associated with these technologies, yet security analysts often miss the vital vulnerabilities involved. The paper tries to explore online application security concerns and risks to privacy. Focus is made on the implications of having a 5G-enabled IoT infrastructure, promising much in high-speed, reliable connectivity but highly susceptible to exploitation.

This paper further analyses user interactions with built-in security features inside common applications and operating systems, showing the real reality of security tools: although they exist, it is not uncommon to find that they are hardly usable without jeopardizing end-users' effective defense mechanisms. Therefore, from the scope of the gap between user intention and practical security practices, this piece of research underscores the need for more intuitive designs and user-friendly interfaces for the improvement of digital safety.

The paper addresses the critical issues of online data collection and privacy breaches by urging developers to work on transparency and providing empowering solutions for users to take decisions. Integrating strong open-source standardization, improving hardware intelligence, and promoting industry collaboration, the paper suggests a safer and more secure environment for the future of online applications. Through a more comprehensive analysis, the research aims to provide insights for the mitigation of risks and enhancement of user awareness in actually contributing to a more secure digital ecosystem.

***Index Terms* -** Online Application, User Awareness, Cybersecurity, IoT security, 5G Networks, Data Protection.

I. Introduction

In modern times, online applications have penetrated the way people and organizations work, leveling information access and changing interactions for both personal and professional purposes. [1-2] Internet of things with rapid proliferation and high-speed 5G internet networks, this digital interconnection has heightened to unprecedented levels of convenience and efficiency. However, with such great interconnectivity come security and privacy concerns at new, higher levels, making an increasingly difficult challenge-and technological progress often parallels rising cyber threats. The paper therefore explores the delicate balance in this constantly evolving digital ecosystem between innovation and vulnerability.[3]

The proliferation of IoT devices and the adoption of 5G technology have revolutionized industries ranging from healthcare to smart cities, industrial automation, and beyond.[4] Billions of devices are now connected, creating intricate networks that communicate in real time, making daily operations more efficient than ever before. Yet, this web of connectivity also provides new entry points for malicious actors.[5] As a result, the digital landscape has seen a surge in cyber threats such as data breaches, ransomware, and identity theft. While security analysts deploy sophisticated tools and protocols to safeguard systems, the pace of technological innovation often outstrips security measures, leaving gaps that cybercriminals exploit.[6]

A significant factor contributing to this vulnerability is the disconnect between users and the security features embedded within the digital platforms they rely on many applications offer built-in tools like encryption and two-factor authentication, which are designed to protect users.[7] However, these features are often perceived as difficult to use, inconvenient, or unnecessary, leading to low adoption rates. This gap makes users more vulnerable to cyberattacks as they feel they are much safer. On the other hand, security needs to become even more intuitive and easy to use so that users can do the utmost towards self-protection.[8]

The advent of 5G technology brings faster communication as well as better reliability but brings along new threats. [9-10] The sheer number of connected devices utilizing 5G networks dramatically increases the attack surface available to cybercriminals.[11] Each IoT device represents a potential vulnerability that can be exploited if not properly secured, and the scale of interconnected networks amplifies the impact of any breach.[12] As 5G continues to drive technological innovation, security frameworks must evolve to keep pace with these advancements, ensuring that the benefits of 5G are not overshadowed by increased risks.[13]

Another significant problem discussed in this study is data privacy. Given the fact that more and more organizations rely on data-driven strategies, in most cases, users are not even transparent about how their personal information is obtained, processed, and used.[14] This situation may lead to mistrust, as users feel they are helpless in their data. Developers need to address the issue by creating transparent communication and empowering the user so they can decide over their digital footprints to bring back trust and increase privacy protection.[15].

Accessibility would also be the last but truly foundational element of a healthy digital ecosystem. Adherence to standards like WCAG 2.1 [16] ensures that digital platforms are accessible and usable by people with disabilities. This step not only meets legal requirements but also adds to the richness of user experiences and satisfaction for a more empowering online environment.[17]

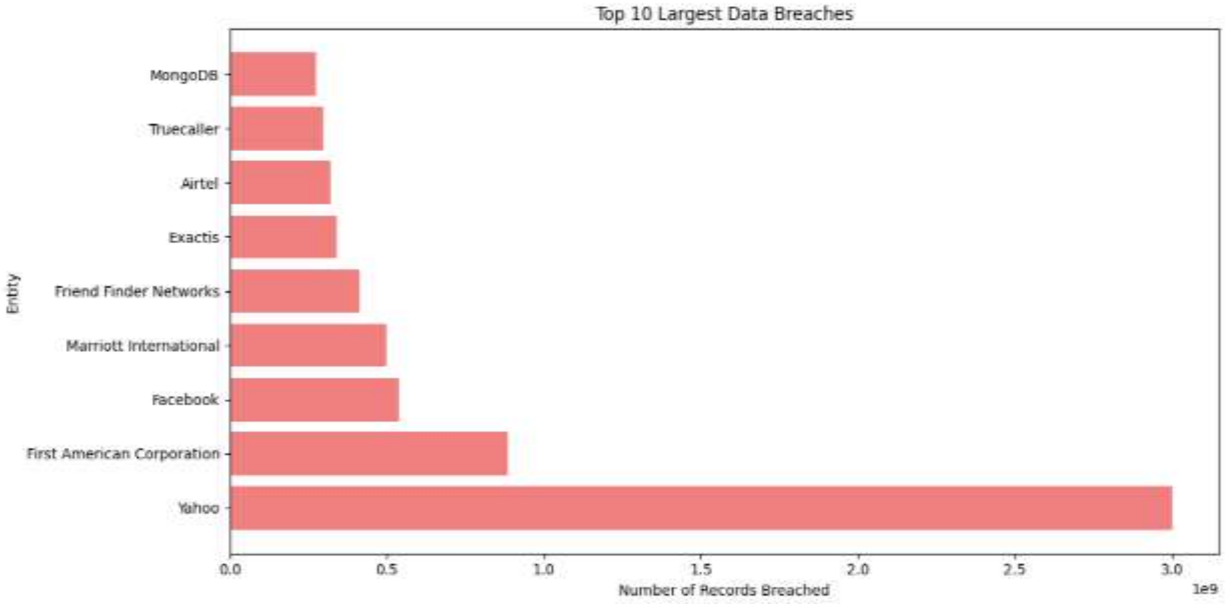


Figure 1. Top 10 Data Breaches

II. BACKGROUND STUDY

2.1 Rajeev Kumar and Asif Irshad Khan (2020)

The intersection of usability and security in online applications is increasingly scrutinized, particularly as the reliance on mobile and IoT devices grows. A study examining mobile application usability found that user perceptions of security are significantly influenced by the design of mobile security notifications (MSNs) and the overall app interface. Disruptive MSNs, while intended to enhance security, often irritate users, leading to decreased perceived security and a lower intention to continue using the app. This highlights the need for a shift in design strategies that prioritize seamless user experiences without compromising security.[18]

2.2 Balázs Csontos, István Heckl (2020)

Furthermore, the concept of continuous authentication has emerged as a method to provide passive user authentication through biometric and behavioural data. While this approach offers a potentially user-friendly alternative to traditional methods, it raises critical privacy concerns. Continuous authentication modes face challenges related to accuracy and the risk of replay attacks, underscoring the necessity of balancing usability with robust security measures .These studies emphasize that to create a secure digital environment, developers must integrate user-friendly design with effective security protocols, ensuring that users are empowered rather than hindered in their interactions with technology.[19]

2.3 Dr. Gregory D. Moody ,Dr. Jun Zhang (2020)

Public sector organizations are increasingly dependent on the internet to provide essential services, highlighting the importance of websites that are accessible, usable, and secure. To address this need, the European Union introduced a 2016 directive requiring member states to ensure that all public sector websites and mobile applications comply with the Web Content Accessibility Guidelines (WCAG) 2.1 at the AA level by September 2021. This directive emphasizes accessibility for individuals with disabilities, ensuring inclusivity across digital platforms.[20]

2.4 Ahmed Fraz Baig, Sigurd Eskeland (2021)

A study of Hungarian public sector websites revealed significant shortcomings in meeting these standards. None of the evaluated websites fully complied with WCAG 2.1 guidelines, and half of them showed poor usability. Additionally, nearly half of the websites were found to be using outdated software, posing security vulnerabilities. The research provided a set of recommendations to improve these areas, offering a framework for other public sector bodies to follow.[21]

2.5 Al-kfairy M, Alomari A, Al-Bashayreh MG, Tubishat M. (2024)

This review examines the Metaverse, highlighting key factors like usability, social influence, and interoperability. It stresses the importance of user-friendly design, accessibility, and inclusive experiences to enhance engagement. Social factors shape user behaviour, while interoperability challenges call for standard protocols across platforms. Ethical concerns such as digital harassment, privacy, and aggressive marketing require responsible development and regulatory frameworks. The review also identifies research gaps, particularly in healthcare, education, and the long-term effects of Metaverse interactions. Lastly, it notes the geographical and demographic biases in current research and the need for more inclusive, globally relevant studies on the Metaverse’s impact.[22]

III. PROPOSED MODEL

Proposed Model: Secure and Usable Online Application (SUA) Framework

This is the SUA Framework-a possible way to solve the consistently increasing difficulty of balancing between security and usability in modern online applications, especially now with IoT and 5G connectivity. The model is designed to bridge the gap that exists between good security features and a smooth user experience, necessary to make such applications popular. The SUA Framework lays emphasis on user-centered design, adaptive security, and transparency into controls of privacy. Such a framework with an integrated approach merges both digital safety and usability.

3.1 Core Elements

a. *Usability-Focused Security Features*

Context-Aware Security Notifications: The architecture provides an alert mechanism that is mildly intrusive, giving users directions while avoiding deluging them with useless prompts.[23] Notification mechanisms are context-aware, allowing security measures to be applied while minimizing the overall users' experience disruption.[24]

Simplified multi-factor Authentication (MFA), The SUA Framework, supports user-friendly security practices such as one-click two-factor authentication and intuitive biometric logins. This approach minimizes friction for the user while maintaining a high level of security.

b. *Adaptive Authentication Mechanisms*

Continuous Authentication Using behavioral biometrics and usage patterns, SUA Framework continuously authenticate the identity of users in a session without introducing repeated logins.[25] This will be done passively and enhance security while minimizing the interruption to the user.

Risk-Based Authentication: It varies the strength of the authentication needed depending on risk estimates - type of device, network conditions, behavior of the user. In high-risk interactions, more stringent security checks apply while basic interactions remain simple and convenient.[26].

c. *Privacy-First Approach*

Transparent Data Usage Policies: The SUA Framework promotes transparency by providing users with clear, accessible summaries of policies regarding data collection and processing. This helps users understand what happens to their information, thus enhancing trust.[27] Granular Privacy Controls: Users can easily change privacy settings to achieve a certain level of data sharing by configuring default settings for maximum privacy. This is in line with the standards for privacy by design, guaranteeing autonomy among users over personal data.

d. *Integrated Threat Response and Maintenance*

Real-Time Threat Detection: The framework incorporates real-time monitoring tools to detect potential threats and vulnerabilities as they arise. This allows for rapid responses to security incidents, reducing the risk of breaches.[28]. Automated Security Patching: Background updates are seamlessly applied to maintain the security of applications without interrupting the user experience. This ensures that systems remain up to date with the latest protections against emerging threats.

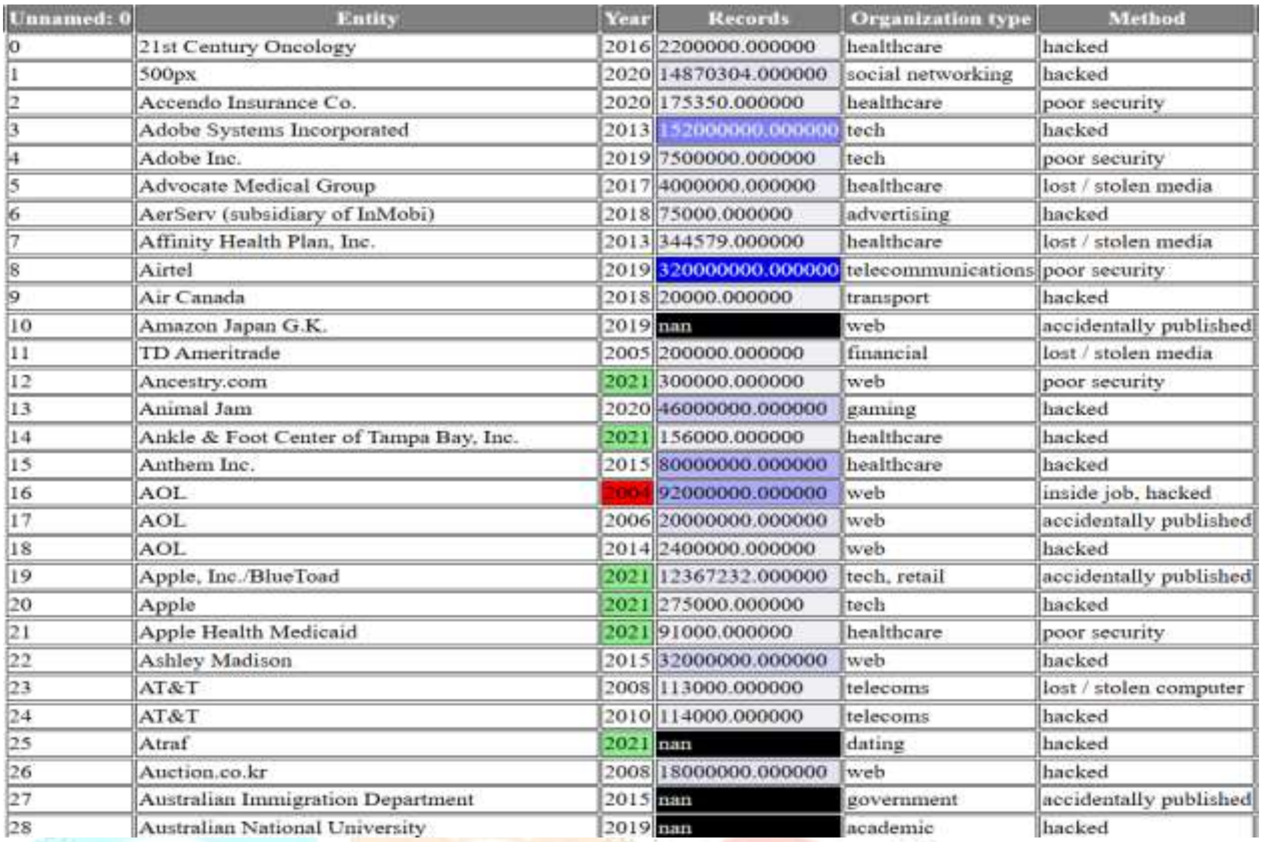
3.2 User Interaction Flow

Initial Configuration The initial application configuration asks people to step through a simplified security configuration process; the main features, for instance, like multi-factor authentication and privacy settings, are clearly defined and quickly enabled.

Context-Aware Authentication Using input patterns and the context of devices, the framework alters security conditions in real-time. Normal tasks might need minimal verification while high-risk actions entice extra layers of security. [29]

Privacy Management: Users are provided with a straightforward interface to manage their privacy settings, offering full transparency and control over personal data. This ensures that privacy preferences are both accessible and easy to modify.

Background Security Maintenance: The SUA Framework operates in the background, applying security updates and monitoring threats without user intervention, ensuring continuous protection without impacting usability.[30]



Unnamed: 0	Entity	Year	Records	Organization type	Method
0	21st Century Oncology	2016	2200000.000000	healthcare	hacked
1	500px	2020	14870304.000000	social networking	hacked
2	Accendo Insurance Co.	2020	175350.000000	healthcare	poor security
3	Adobe Systems Incorporated	2013	152000000.000000	tech	hacked
4	Adobe Inc.	2019	7500000.000000	tech	poor security
5	Advocate Medical Group	2017	4000000.000000	healthcare	lost / stolen media
6	AerServ (subsidiary of InMobi)	2018	75000.000000	advertising	hacked
7	Affinity Health Plan, Inc.	2013	344579.000000	healthcare	lost / stolen media
8	Airtel	2019	320000000.000000	telecommunications	poor security
9	Air Canada	2018	20000.000000	transport	hacked
10	Amazon Japan G.K.	2019	nan	web	accidentally published
11	TD Ameritrade	2005	200000.000000	financial	lost / stolen media
12	Ancestry.com	2021	300000.000000	web	poor security
13	Animal Jam	2020	46000000.000000	gaming	hacked
14	Ankle & Foot Center of Tampa Bay, Inc.	2021	156000.000000	healthcare	hacked
15	Anthem Inc.	2015	80000000.000000	healthcare	hacked
16	AOL	2004	92000000.000000	web	inside job, hacked
17	AOL	2006	20000000.000000	web	accidentally published
18	AOL	2014	2400000.000000	web	hacked
19	Apple, Inc./BlueToad	2021	12367232.000000	tech, retail	accidentally published
20	Apple	2021	275000.000000	tech	hacked
21	Apple Health Medicaid	2021	91000.000000	healthcare	poor security
22	Ashley Madison	2015	32000000.000000	web	hacked
23	AT&T	2008	113000.000000	telecoms	lost / stolen computer
24	AT&T	2010	114000.000000	telecoms	hacked
25	Atraf	2021	nan	dating	hacked
26	Auction.co.kr	2008	18000000.000000	web	hacked
27	Australian Immigration Department	2015	nan	government	accidentally published
28	Australian National University	2019	nan	academic	hacked

Figure 2. data breaches record

3.3 Python program for displaying the graphs

```
import pandas as pd
import matplotlib.pyplot as plt
# Load your dataset
file_path = r"df_1.csv"
df = pd.read_csv(file_path)
# Clean the dataset (remove unnecessary columns)
df_cleaned = df.drop(columns=["Unnamed: 0"], errors='ignore')
# Convert 'Records' column to numeric (handle non-numeric with errors='coerce')
df_cleaned['Records'] = pd.to_numeric(df_cleaned['Records'], errors='coerce')
# 1. Example 1: Data Breaches by Year
summary_by_year = df_cleaned.groupby('Year').size().reset_index(name='Number of Breaches')
# 2. Example 2: Top 10 Largest Data Breaches
top_10_breaches = df_cleaned.sort_values(by='Records', ascending=False).head(10)
# Plotting the Graphs
# Example 1: Plot Breaches by Year (Bar Chart)
plt.figure(figsize=(10, 6))
plt.bar(summary_by_year['Year'], summary_by_year['Number of Breaches'], color='skyblue')
plt.xlabel('Year')
plt.ylabel('Number of Breaches')
plt.title('Data Breaches by Year')
plt.xticks(rotation=45)
plt.tight_layout()
plt.show()
# Example 2: Plot Top 10 Largest Data Breaches (Horizontal Bar Chart)
plt.figure(figsize=(12, 6))
plt.barh(top_10_breaches['Entity'], top_10_breaches['Records'], color='lightcoral')
plt.xlabel('Number of Records Breached')
plt.ylabel('Entity')
plt.title('Top 10 Largest Data Breaches')
plt.tight_layout()
plt.show()
```

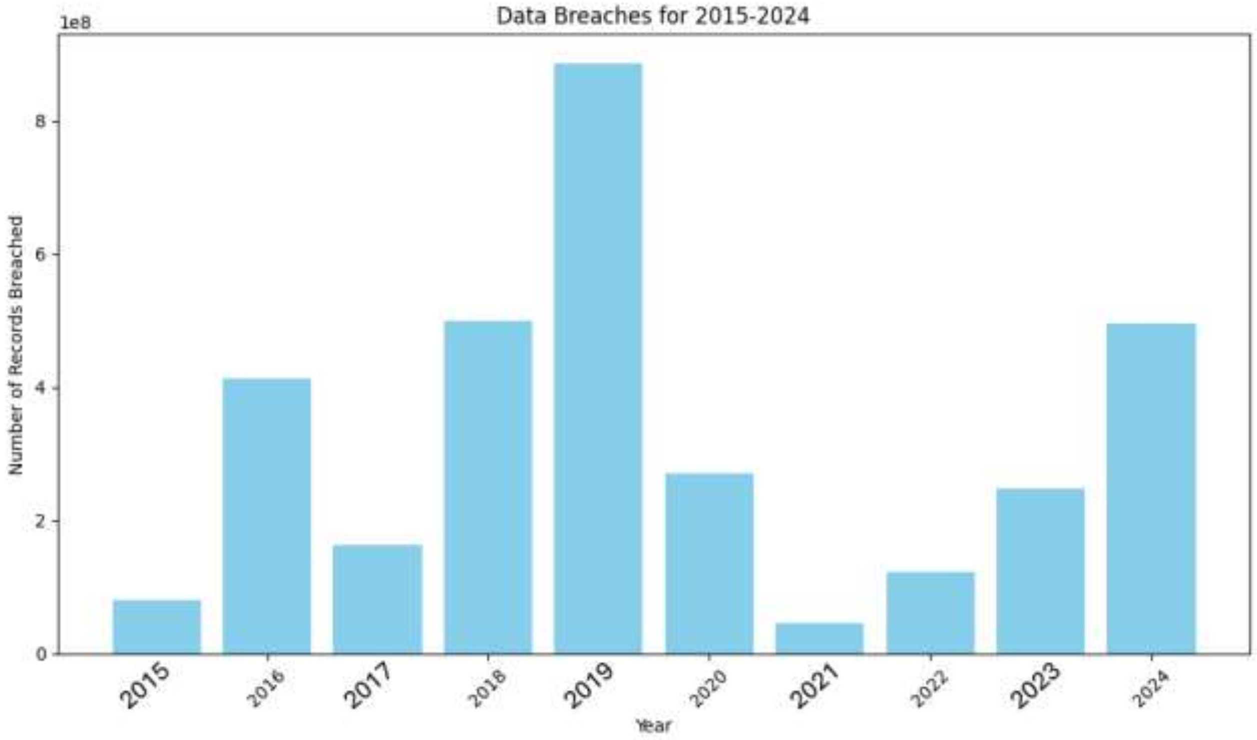


Figure 1. Data Breaches trend(2015-2024)

3.4 Benefits

Enhanced Usability: The SUA Framework concentrates on intuitive security tools and streamlined authentication processes in pursuit of user engagement and subsequently reduces friction, which helps users easily adopt and maintain secure behaviors.

Proactive Security: Continuous monitoring and automated response for threats allows the SUA Framework to mitigate risks in real time, ensuring user data safety and integrity of an application.

User Empowerment: The framework empowers users to take control of their digital footprint through transparent data policies and customizable privacy settings, which increases trust and compliance in digital applications.

Scalable Security: The framework addresses the increasing challenges of IoT and 5G technologies through its ability to evolve with the times, ensuring that the security measures are on par with technological advancements.

IV. RESULTS AND DISCUSSION

In this research ,we analysed some datasets which shows the data of the online applications with their names, with their type of application like healthcare , tech etc and with the year in which they we hacked or due to poor security their data was stolen. We created some graphs for better visualisation by using python with its libraries like pandas , matplotlib.

There are numerous studies based on the convergence of security and usability for online applications, both related to the challenge and opportunities for the digital landscape, particularly with the scale of IoT and 5G network expansions. First, the analysis confirms that though these security features, such as MFA and encryption, which are integrated into applications, their usability actually poses as the major barrier to widescale adoption. These features tend to be clumsy for users to have because they need to be designed in a way that offers them convenience and security simultaneously.

This further shows how continuous authentication techniques, grounded in behavioural biometrics, can be an exceptionally compelling replacement for traditional security controls but still have a lot to grow toward resolving issues of privacy and accuracy. Adaptive, context-aware security alerts dramatically minimized frustrations from users with near minimal deterioration in protection-behaviour than many applications' current aggravating notifications.

The research in the public sector stressed a real need for accessibility and usability in digital platforms, specifically in view of, inter alia, regulation requirements as observed in the WCAG 2.1. The study of Hungarian public sector websites showed that most organizations fall behind in terms of usability and security, hinting at the demand for more concerted efforts toward meeting the needs of regulation and ensuring digital access.

In particular, the proposed SUA framework of a simplified security process, continuous monitoring, and transparency of privacy has been shown as an example to a scalable model for many kinds of industries. This makes the SUA framework implement proactive defence mechanisms against emerging threats in IoT and 5G-enabled environments by its mechanism for real-time threat detection as well as automated patching.

Figures and Tables

Figure 1 shows the top 10 breaches of online applications from the year 2011 to 2024. **Figure 2** is the slight overview of the dataset and was created by using python in form of html webpage. **Figure 3** displays the graphs which shows the trend of data breaches from year 2015 to 2024.

IV. CONCLUSION

It really points to a fundamental necessity in terms of balancing the two variables, which are security and usability in designing and developing online applications. The continued evolution of such technologies as IoT and 5G will only increase the trend of demanding more intuitive and user-friendly security features. The proposed SUA framework outlines a possible way towards closing the gap between user intentions and practical security practices to facilitate secure yet efficient use of digital platforms.

In addition to that, the report puts a stamp under the necessity for data privacy transparency, a call to communicate in the clear manner of data collection in order to build and empower users. Further, continuous authentication and real-time threat detection mechanisms integrated into SUA would bring forward-thinking approaches to address dynamic cybersecurity challenges.

Balancing security and usability are integral in ensuring sustainable use of online applications in the long run. This is the work of developers, designers, and security experts working together to come up with solutions that not only protect the users but also enhance their experience, so it contributes to a safer and friendlier digital space. Adoption of frameworks like SUA may be the step forward to ensure such benefits are materialized without nullifying either security or usability.

V. ACKNOWLEDGMENT

I would like to express my deepest gratitude to **Dr Prakash Kuppuswamy**, for their unwavering guidance, support, and encouragement throughout the course of this research. Their invaluable insights, expertise, and continuous motivation have played a crucial role in shaping this work. I also wish to extend my heartfelt thanks to the Head of the Department of Computer Science and Engineering, **Dr Mohan M**, for creating an intellectually stimulating and supportive environment that made this research possible.

REFERENCES

[1] Dwivedi, Y.K., Hughes, D.L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J.S., Gupta, B., Lal, B., Misra, S., Prashant, P. & Raman, R., 2020. Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55, p.102211.

[2] Dwivedi, Y.K., Hughes, D.L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J.S., Upadhyay, N., Misra, S., Gupta, B., Lal, B. & Prashant, P., 2020. Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55, p.102211.

[3] Maple, C., 2017. Security and privacy in the Internet of Things. *Journal of Cyber Policy*, 2(2), pp.155–184.

[4] Attaran, M., 2023. The impact of 5G on the evolution of intelligent automation and industry digitization. *Journal of Ambient Intelligence and Humanized Computing*, 14(5), pp.5977–5993.

[5] Abomhara, M. & Køien, G.M., 2015. Cyber security and the Internet of Things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, May 22, pp.65–88.

[6] Thakur, M., 2024. Cyber security threats and countermeasures in the digital age. *Journal of Applied Science and Education (JASE)*, 4(1), pp.1–20.

[7] Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. & Jaiswal, A.K., 2021. A systematic literature review on cyber security. *International Journal of Scientific Research and Management*, 9(12), pp.669–710.

[8] Tan, M. & Teo, T.S., 2000. Factors influencing the adoption of Internet banking. *Journal of the Association for Information Systems*, 1(1), p.5.

[9] Radu, R. & Amon, C., 2021. The governance of 5G infrastructure: between path dependency and risk-based approaches. *Journal of Cybersecurity*, 7(1), p.tyab017.

[10] Radu, R. & Amon, C., 2021. The governance of 5G infrastructure: between path dependency and risk-based approaches. *Journal of Cybersecurity*, 7(1), p.tyab017.

[11] Schmitt, M., 2023. Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, 36, p.100520.

[12] Kimani, K., Oduol, V. & Langat, K., 2019. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, pp.36–49.

[13] Purohit, A., Kaushik, R. & Sharma, M.K., 2023. 5G and its impact on IoT: A review. *Journal of Nonlinear Analysis and Optimization*, 14(2).

[14] Saura, J.R., Ribeiro-Soriano, D. & Palacios-Marqués, D., 2021. From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. *International Journal of Information Management*, 60, p.102331.

[15] Laschinger, H.K., Finegan, J., Shamian, J. & Casier, S., 2000. Organizational trust and empowerment in restructured healthcare settings: Effects on staff nurse commitment. *JONA: The Journal of Nursing Administration*, 30(9), pp.413–425.

[16] Martinez, M., Dillen, W., Bleeker, E., Sichani, A.M. & Kelly, A., 2019. Refining our conceptions of 'access' in digital scholarly editing: Reflections on a qualitative survey on inclusive design and dissemination. *Variants: The Journal of the European Society for Textual Scholarship*, (14), pp.41–74.

[17] Kumar, V. & Pansari, A., 2016. Competitive advantage through engagement. *Journal of Marketing Research*, 53(4), pp.497–514.

[18] Kumar, R., Khan, A.I., Abushark, Y.B., Alam, M.M., Agrawal, A. & Khan, R.A., 2020. An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications. *IEEE Access*. DOI: 10.1109/ACCESS.2020.2970245.

[19] Csontos, B. & Heckl, I., 2021. Accessibility, usability, and security evaluation of Hungarian government websites. *Universal Access in the Information Society*, 20, pp.139–156. DOI: 10.1007/s10209-020-00716-9.

[20] Wu, D., Moody, G.D., Zhang, J. & Lowry, P.B., 2020. Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Journal of Network and Computer Applications*.

[21] Baig, A.F. & Eskeland, S., 2021. Security, privacy and usability in continuous authentication. *Sensors*, 21(17). DOI: 10.3390/s21175967.

[22] Baig, A.F. & Eskeland, S., 2021. Security, privacy and usability in continuous authentication. *Sensors*, 21(17). DOI: 10.3390/s21175967.

[23] Al-Kfairy, M., Alomari, A., Al-Bashayreh, M.G. & Tubishat, M., 2024. Unveiling the metaverse: A survey of user experience, social dynamics, and technological interoperability. *Preprints.org*, DOI: 10.20944/preprints202402.0785.v1.

[24] Iqbal, S., Kiah, M.L., Dhaghighi, B., Hussain, M., Khan, S., Khan, M.K. & Choo, K.K., 2016. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, 74, pp.98–120.

[25] Ammar, M., Russello, G. & Crispo, B., 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, pp.8–27.

[26] Oduri, S., 2024. Continuous authentication and behavioral biometrics: Enhancing cybersecurity in the digital era. *International Journal of Innovative Research in Science Engineering and Technology*, 13, pp.13632–13640.

[27] dos Santos, D.R., Marinho, R., Schmitt, G.R., Westphall, C.M. & Westphall, C.B., 2016. A framework and risk assessment approaches for risk-based access control in the cloud. *Journal of Network and Computer Applications*, 74, pp.86–97.

[28] Varker, T., Forbes, D., Dell, L., Weston, A., Merlin, T., Hodson, S. & O'Donnell, M., 2015. Rapid evidence assessment: Increasing the transparency of an emerging methodology. *Journal of Evaluation in Clinical Practice*, 21(6), pp.1199–1204.

[29] Al-Hawamleh, A., 2024. Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, 15(1), pp.1315–1331.

[30] Chirra, D.R., 2022. AI-powered adaptive authentication mechanisms for securing financial services against cyber-attacks. *International Journal of Advanced Engineering Technologies and Innovations*, 1(3), pp.303–326.

[31] Garfinkel, S. & Lipford, H.R., 2014. Usable security: History, themes, and challenges. *Morgan & Claypool Publishers*.

	Muskan Ostwal is an undergraduate student pursuing a Bachelor of Technology (BTech) degree in Computer Science and Engineering at SRM University Delhi NCR. Throughout academic journey, has actively participated in various research projects and technical workshops, honing both theoretical and practical skills.
	Mansi Garg, is an undergraduate student pursuing a Bachelor of Technology (BTech) degree in Computer Science and Engineering at SRM University Delhi NCR. Throughout academic journey, has actively participated in various research projects and technical workshops, honing both theoretical and practical skills.
	Shirsaa Saha, is an undergraduate student pursuing a Bachelor of Technology (BTech) degree in Computer Science and Engineering at SRM University Delhi NCR. Throughout academic journey, has actively participated in various research projects and technical workshops, honing both theoretical and practical skills.