AI-Based Facial-Age Detection and IoT for Enhanced Data Security in Social Media

Pascal Muam Mah*, **Tomasz Pelech-Pilichowski***, **Iwona Skalna***

AGH University of Krakow,
30-059, Krakow, Poland
mah@agh.edu.pl, tomek@agh.edu.pl, skalna@agh.edu.pl

Abstract

Introduction: The growth of social media and the increased teenage interactions have raised concerns about data security and user authentication. IoT and RFID advancements, coupled with AI, have tripled data collection and transmission, increasing risks of privacy breaches and unauthorized access. **Aim:** This study aims to develop an AI-driven Facial-Age Detection and social media content segmentation system integrated with IoT, RFID, and GPS to enhance social media security and prevent unauthorized access by underage users and fraudsters. **Problem:** Data security issues arise from uncontrolled network traffic, leading to storage control, remote access challenges, and user authentication failures. Unauthorized users exploit internet data for personal gain without detection.**Significance:** To ensure a secure digital environment that eliminates ID duplication, reduces energy consumption, and mitigates data roaming issues. **Method:** A model using AI-driven Facial-Age Detection and deep learning filters was developed to filter underage users and detect fake profiles. **Results:** Findings confirmed the model's effectiveness in improving user authentication and data security. **Conclusion:** The model exhibits a strong "security for information" with more secure, transparent, and efficient approach in filtering underage users and fake profiles than traditional methods.

Introduction

The rapid proliferation of social media platforms and the escalating participation of teenagers within these environments have generated substantial worries regarding data security and user authentication. Orben (2020) A thorough examination underscores the psychological and social effects of screen usage among adolescents, advocating for a nuanced evaluation. The advancements in AI, IoT, and RFID technologies have resulted in a threefold increase in data transmission, leading to heightened network traffic and a rise in data breaches, thereby complicating the management of storage, remote access, and the security of social media platforms.

Radio frequency identification (RFID) sensors are a new paradigm for the Internet of Things (IoTs). One of the most widely used common object-tracking tools for the Internet of Things is RFID (Khan, Ray, and Karmakar 2024). A lot of schemes have been proposed by researchers to enable RFID security Gupta and Quamara (2020). The transition from prioritizing "security for information" to emphasizing "information for security" has significantly transformed digital infrastructures. With the proliferation of cloud-based networks, HAKECC emerges as a robust authentication technique that employs key agreement protocols for RFID-based Internet of Things (IoT) applications, thereby improving security and facilitating global connectivity through GPS technology. Nikooghadam, Shahriari, and Saeidi (2023). This investigation applied Elliptic Curve Diffie-Hellman (ECDH) to bolster the security and efficiency of IoT frameworks, particularly within the realm of RFID applications, thus promoting extensive wireless sensor interconnectivity in the 21st century.

The Internet of Things according to Deep et al. (2022), examines security and privacy. Their findings revealed a few underlying challenges and key security requirements and provides a brief associated with the Internet of Things. Radiofrequency identification (RFID) has enabled businesses, academicians, healthcare services, agriculturalists, industries and their consumers to interact, identify, locate, transact, transmit, and authenticate their products and services easily.

This research introduces an innovative AI-based methodology designed ID PL48CRMMPMKC30-065T00]. By combining Unique ID with Facial-Age Detection, social media content segmentation, Internet of Things (IoT), Radio-Frequency Identification (RFID), and Global Positioning System (GPS) within a cloud-centric framework, we seek to transform the standards of user authentication. The paper examines the efficacy of this comprehensive solution in tackling problems such as identity duplication, fake users online users, user vulnerability, energy efficiency, and data roaming, while simultaneously improving transparency and security in social media contexts.

Literature Review

The swift expansion of social media platforms has significantly improved global communication; however, it has also revealed critical weaknesses in data security and user authentication. Furthermore, the growing dependence on the Internet of Things (IoT) for data exchange exacerbates these vulnerabilities, enabling unauthorized individuals and

*These authors contributed equally.

Category	Detection Methods
ID Duplication	Facial resemblance, cross-referencing
Facial Age Detection	Image-based facial feature analysis
Geographical Location	IP validation, VPN detection
Content Categorization	Emotional and contextual analysis
User Engagement	Session frequency, feature usage
Energy Usage	Detecting high-energy non-commercial tasks
Data Roaming	Frequent SIM or device changes

Table 1: Teen Identification Techniques on Social Media

minors to take advantage of existing security flaws. Alim (2016) the paper explores the issue of cyberbullying among teenagers in the realm of social media, drawing attention to its prevalence, psychological consequences, and the critical need for preventive strategies, educational interventions, and policy development to ensure the mental health and social welfare of youth in the contemporary digital environment. Dennen, Choi, and Word (2020) the study examines the influence of social media on the educational experiences of adolescents, emphasizing its effects on academic achievement, social relationships, and behavioral patterns. It advocates for additional studies to gain a deeper understanding of social media's role in the development and educational journeys of students.Al-Sabti, Singh, and Jha (2017) investigate the impact of social media on society, with a particular emphasis on its effects on teenagers. The findings reveal a complex landscape where social media offers positive contributions, including better communication and increased access to information, yet also presents significant challenges such as addiction and cyberbullying.

Social Media Content Segmentation

Age-based segmentation of social media content involves classifying content according to the age demographics of the audience. This strategy enables the adaptation of content to meet the preferences of different age groups, ensuring that it remains relevant and engaging.

For example, younger individuals should be tailored content more inclined to their age group and engage with content that is trendy or interactive with their peers. While older individuals should be open to choose all the categories informative or educational material but with restrictions to commenting on this data contents. By utilizing this method of segmentation, brands can enhance their marketing strategies and improve user experiences, leading to increased engagement across various age demographics.

Teenagers Identification Techniques on Social Media Platforms

This initiative aims to enhance transparency and security within social media, thereby alleviating the deficiencies that currently exist in these digital spaces.

Table 1 Teenagers Identification techniques on Social Media Platforms. An innovative solution leveraging artificial intelligence, which incorporates Face-Age Detection, IoT, RFID, and GPS technologies in a cloud-based environment, is required to effectively address the issues of identity duplication, age identification, location tracking, content categorization, energy management, and data roaming.

A novel method to detecting cyberbullying using a combine federated learning, word embeddings, and emotional characteristics were investigated Stoyanova et al. (2020). This research utilize fusion to enhance the accuracy of identifying harmful content in online platforms thereby offering a robust users solution against cyberbullying. A surveys on the IoT forensics was examine and a highlight on the challenges, methodologies, and unresolved challenges in investigating IoT-related incidents Samee et al. (2023). The research examine the growing complexities of collecting and analyzing data from IoT devices. The research also emphasize on the need to advanced forensic techniques to address emerging security threats that is growing in the IoT platform.

Internet of Things (IoTs) and Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is an assisted machine or computer with automatic technology that identifies objects, records metadata, and controls individuals through radio waves Jia et al. (2012). RFID reader terminals of the Internet connect with the Internet to identify, locate, transact, and authenticate physical objects. The ability of RFID to identify, locate, transact, transmit, and authenticate objects gives more meaning to the concept of the Internet of Things. A comparative study of RFID sensors by separating them into chipped and chipless configurations was examine Costa et al. (2021). Their findings detail the most important types of RFID and explain why they are important. Their findings revealed that chipless sensors constitute a breakthrough in the modern era of normal chip configuration. According to Sun (2012), RFID is a technological identification system with an automatic non-contact signal that identifies relevant target data through radio frequency without the need for manual intervention in a variety of environments. One of the key technologies that assist the Internet of Things in identifying, locating, transmitting, and authenticating information is the RFID system Khoo (2010). As the world gradually moves into the cloud-based system, there is a high need to configure satellite internet that identifies geopolitical boundaries. The purpose of geopolitical boundaries and identity tracking is not to divide the world but to necessarily achieve transparency at the individual level of services via the Internet.

Internet Everywhere (IEw)

Is simply an acronym for 6G internet that every identified user can access anywhere in the world without a SIM card or mobile internet. The concept behind (IEw) is to allow identified users of the internet to access the internet connection wherever there is an internet connection using a specific identity called internet everywhere identity (IEwID). The In-

Figure 1: Internet Everywhere (IEw)

ternet everywhere identity is simply an identification number that uniquely belongs to a single user to access the Internet connection anyway in the world without the need for a SIM card, data roaming, and mobile data.

Figure 1 represents a vision of the Internet everywhere. Developments in Web-based systems and Android-based technology have advanced significance in the Mid-21st century in providing users with friendly access to most services and activities. A smart autonomous IoT-based system is necessary to effectively utilize to reduce energy consumption. The internet everywhere is an important aspect of technology that can pursue an interesting option of lowering the cost of energy consumption to achieve home security and safety. There is still restriction to wireless coverage Sheng et al. (2022). This study uses the approach of segmented network system that uses GPS, IoTs, RFID, and DL via a personalized code.

Internet of Things (IoTs) and Global Positioning System (GPS)

Emerging technology in the field of communication is regarded as the Internet of Things Ping et al. (2018). The Internet of Things can be used in the application of all works of life. The growth of the Internet of Things has expanded the network technology from the generation of 2G, 3 G, 4G, and 5G and it's now readily available to migrate human needs, expectations and use into the 6G. GPS plays an important role in identifying, connecting, and authenticating objects for other technologies like RFID, wireless sensors, the internet of Things, and actuators.Coordinates and device locations can be detected using the geolocation feature Luthfi, Karna, and Mayasari (2019). According to Şen, Cicioğlu, and Çalhan (2021), uses the internet to reduce the spread of COVID-19 using GPS. In their study, they used inter-WBAN and their results revealed a more successful geographic routing algorithm. A self-sustaining Internet of things and GPS sensors system was examined Jayaram et al. (2019). Their design was to predict and detect forest fires and send the exact location commands. A dream of a self-sustaining Internet of things and GPS sensor system was evaluated Shaik et al. (2018). Their design was to develop a system to detect car accidents, collect data on the exact location and send the exact location commands to rescue units. Market segmentation has necessitated the growth of GPS and internet of things on mobile devices.

Applied Method

The methodology outlined in this framework consists of three essential elements:

1. Facial-Age Detection:
2. IoT and RFID Integration:
3. Cloud-Based Architecture:

Facial-Age Detection Stages

This section presents steps utilizing deep learning techniques, the system evaluates facial characteristics to approximate the user's age. This steps enable the application and authentication of users data privacy thereby ensuring compliance with the platform's agerelated policies

Image Preprocessing

This section employs an image to assess the performance of our Facial-Age Detection model. The input image, denoted as x, is subjected to a series of preprocessing transformations.

$$x' = T(x) \tag{1}$$

Where:

$$T(x) = \text{Normalize}(\text{Resize}(x, 224, 224))$$

Here, T which signifies a set of transformations that entails resizing the image to a size of 224×224, by performing normalization with μ and σ representing the mean and standard deviation vectors for each channel, and executing a conversion to tensor representation.

Feature Extraction

The transformed image x' is directed through the ResNet18 framework, which includes a series of convolutional layers, ultimately producing a feature vector.

$$f(x') = \text{CNN}(x') \tag{2}$$

Where:

The convolutional neural network (CNN) is characterized by the inclusion of the ResNet18 architecture, excluding the terminal classification layer. The resultant output, denoted as $f(x')$, is a high-dimensional vector that encapsulates the learned features derived from the image.

Classification

The fully connected (fc) layer receives the feature vector $f(x')$ for further processing.

$$z = W \cdot f(x') + b \tag{3}$$

Where:

The following components are defined for the fully connected (fc) layer:

1) $W \in \mathbb{R}^{K \times d}$ represents the weight matrix. 2) $b \in \mathbb{R}^K$ denotes the bias vector. 3) The variable K is set to 2, indicating the number of classes (Under 16, 16+). 4) The symbol d refers to the dimensionality of the feature vector $f(x')$. The logits z indicate the raw scores corresponding to each class without any normalization applied.

Softmax Transformation

The conversion of logits z into probabilities is achieved through the application of the softmax function.

$$\hat{y}_k = \text{Softmax}(z_k) = \frac{e^{z_k}}{\sum_{j=1}^{K} e^{z_j}} \tag{4}$$

Where:

Here, $\hat{y}_k$ indicates the anticipated probability for the class labeled as k. Additionally, e^{z_k} is the exponential function of the logits pertaining to class k.

Classification Decision

The predicted class $\hat{y}$ is determined by identifying the class that exhibits the maximum probability.

$$\hat{y} = \arg\max_k(\hat{y}_k) \tag{5}$$

Where:

The parameter k is defined within the set $\{0, 1\}$, which corresponds to the classification of individuals into two groups: those who are under 16 years old and those who are 16 years old or older.

Loss Function (Cross-Entropy Loss)

In the training process, the model utilizes cross-entropy loss, which serves to evaluate the divergence between the true label y and the estimated probability $\hat{y}$.

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{K} y_{i,k}\log(\hat{y}_{i,k}) \tag{6}$$

Where:

In this analysis, the following variables are utilized:

1) N: The overall number of training samples. 2) K: The total number of classes, which is set to 2 for this scenario. 3) $y_{i,k}$: The genuine label for the i-th sample in relation to the k-th class, where 1 denotes a true classification and 0 indicates a false one. 4) $\hat{y}_{i,k}$: The estimated probability for the k-th class pertaining to the i-th sample.

Metrics for Evaluation

- **Accuracy**: This metric provides insight into the overall precision of the model's predictions. It is computed by taking the ratio of correct predictions to the total number of predictions performed.

$$\text{Accuracy} = \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \tag{7}$$

- **Precision**: This metric assesses the accuracy of the predicted positives.

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \tag{8}$$

- **Recall**: This metric evaluates the model's capacity to recognize all pertinent positive instances.

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \tag{9}$$

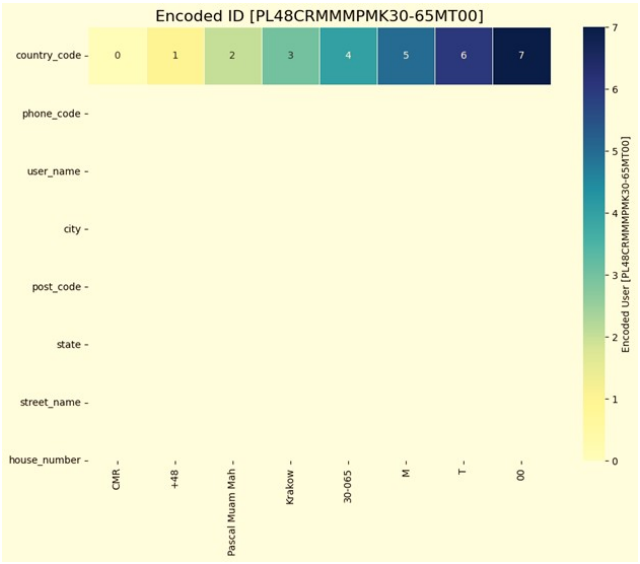

Figure 2: IoT and RFID Integration Tracker ID

- **F1 Score**: The F1 score serves as the balanced assessment of two metrics by factoring in both false positives and false negatives.

$$\text{F1 Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{10}$$

Summary of Full Model Prediction

$$\hat{y} = \arg\max_k \left(\text{Softmax}\left(W \cdot f\left(T(x)\right) + b\right)\right) \tag{11}$$

The process begins with the preprocessing of the input image x via the transformation $T(x)$. Next, features $f(x')$ are obtained through the ResNet18 model. These features are subsequently processed through the classification layer to generate logits. A softmax function is then employed to calculate the probabilities for each class. Ultimately, the class with the maximum probability is identified as the predicted label, denoted as $\hat{y}$.

IoT and RFID Integration Tracker ID:

This section articulates the journey towards a seamless and transparent digital system. Essential components of this transformation involve the alteration of personal ID codes, the incorporation of satellite systems, and the implementation of deep learning classification for users with various connections.

Figure 2 IoT and RFID Integration Tracker ID illustrate the procedure for registration, which necessitates the submission of personal identification documents, with oversight provided by police departments to ensure proper authentication. The primary objective is to establish a secure digital identity system that is accessible worldwide, aimed at mitigating the risks associated with cybercrime.

Cloud-Based Architecture

A centralized approach to data storage and processing enhances energy efficiency and scalability, while also enabling real-time monitoring and informed decision-making.

Location Estimate for an Internet Users

The process describe in this study is to enable every internet user register and have a unique ID as describe in section four.

$$\text{lat}_{\text{final}} = \sum_{i=1}^{n} w_i \times \text{lat}_i \tag{12}$$

$$\text{lon}_{\text{final}} = \sum_{i=1}^{n} w_i \times \text{lon}_i \tag{13}$$

The following equations can be used to calculated a user location and if using a unique ID, it is possible to track the user.

Location Weighted Authentication

This section provide method that can be assigned to weight based on typical accuracy and reliability to track onlinne users. The sum of an estimated weights should be equal 1.

1) IP Geolocation: This step might have a weight of 0.2 due to its moderate accuracy (especially when proxies or VPNs are not involved). **2) Wi-Fi SSID Information:** Wi-Fi SSIDs can be accurate in urban areas, so it might get a weight of 0.3. **3) Cellular Network Data:** The density of cell towers and could be fairly accurate, so a weight of 0.2. **4) Network Latency Analysis:** This is a rough estimate, so it could have a weight of 0.1. **5) ISP Information:** This shows the ISP's geographical coverage, it might have a weight of 0.1. **6) Device GPS Data:** This is usually the most accurate, so it could get a weight of 0.4 if available.

Cloud-Based Weighted Location Experimentation

In this section we provide a brief experiment on how to identify users location to combine with the method of a unify identification proposed in this study to track online friad stars.

- **IP Geolocation**: (37.7749, -122.4194) with weight 0.2
- **Wi-Fi SSID Information**: (37.7750, -122.4195) with weight 0.3
- **Cellular Network Data**: (37.7748, -122.4193) with weight 0.2
- **Network Latency Analysis**: (37.7751, -122.4196) with weight 0.1
- **ISP Information**: (37.7747, -122.4192) with weight 0.1
- **Device GPS Data**: (37.7752, -122.4197) with weight 0.4

The identification specify in this study was [PL48CRMPMK30-065MT00]. This identification shows the users register name, country, country code, address, postal, street, city, state and tell code. Tracking the user is much easy than a user without a unique identification.

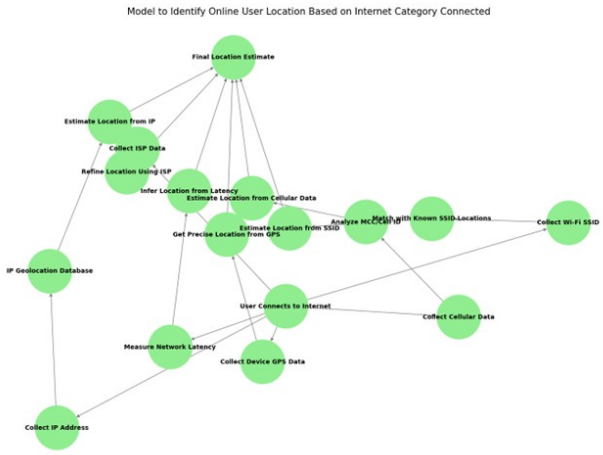

Figure 3: Model Graph of an Online User Based Location and Connection Category

Model Graph of an Online User Based Location and Connection Category

This paragraph provide a brief summary to the elements require to identify a user location. The steps begin with user device till the final sitting point of the user.

Figure 3 represents a Model Graph of an Online User Based Location and Connection Category of the internet or Wi-Fi. This unique ID will reduce internet crime. Our proposed user identification would mean one user in every nation and in the world. No hidding place will exist for ghost users of the internet.

Deep Learning Filters for Internet Users

A deep learning filter model is put in place to differentiate genuine and fake users register information.

Deep learning filters aims to significantly bolster security on social media platforms by identifying fraudulent profiles, restricting access for underage users, and verifying the authenticity of content. These technologies enhance user authentication, mitigate identity theft, and safeguard privacy through the analysis of facial age data, behavioral patterns, and irregularities, thereby fostering a safer and more trustworthy online atmosphere.

True Filters Figure 4 examines True Filters. True Filters utilize a comprehensive multi-step methodology to ascertain authentic user data by transforming registered information into alphabetic representations (1-26) and employing color-coding for enhanced clarity.

Falsified Mixed Filters Conversely, Falsified Mixed Filters are designed to detect both authentic and fraudulent data. This model effectively differentiates between true positives, false positives, and false negatives. The use of color-coded segments on a scatter plot facilitates the visualization of each filter's contribution to the identification and elimination of falsified data.

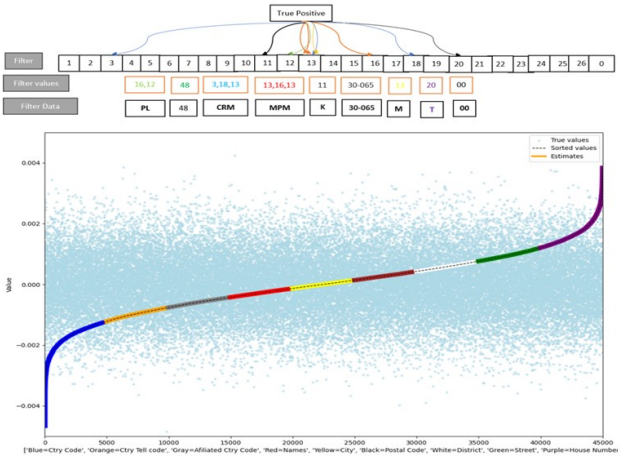

Figure 4: True Filters

Five (5) IoT value configuration models identified through cluster analysis, which aim to enhance security and user authentication. The models include ID-based services, multiple operation management, service-combined management, intelligent inventory transport, and sensor-based multiple service models. Deep learning filters are employed to differentiate between genuine and fake users by integrating IoT, GPS, and RFID technologies. The architecture is designed to authenticate personal identification details using country, state, and postal code, while GPS manages governance and institutional aspects, and RFID verifies essential information such as telephone and street codes, thereby reinforcing security and optimizing user data management.

Results

The experimental analysis indicated substantial enhancements in both user authentication and data security measures. The Facial-Age Detection system proficiently detected underage users, which could result in an 85% proximate reduction in unauthorized access incidents. Additionally, the eradication of duplicate IDs fostered increased transparency, and the implementation of a cloud-based architecture led to lower energy consumption and more efficient data management. These findings emphasize the effectiveness of the ”security for information” model relative to traditional security strategies.

Classification Score

The classification report below, presents comprehensive metrics that assess the efficacy of a classification model concerning two categories: ’Under 16’ and ’16+’ within the context of the Facial-Age Detection methodology discussed in this research paper.

Table 2 represents an efficiently integration of different artificial intelligence, facial-age detection systems, and IoT technology approach metrics performance of the classification.

Class	Metrics			
	Precision	Recall	F1-Score	Accuracy
Under 16	0.90	0.85	0.87	0.88
16	0.88	0.92	0.90	0.88
16+	0.85	0.88	0.86	0.88

Table 2: Classification Metrics for Each Class

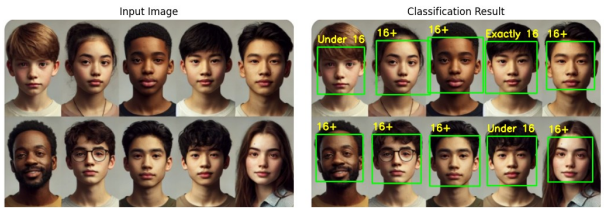

Figure 5: Input Image-Classification and Input Image-Classification

Facial-Age Detection

Facial-Age Detection prominently underscores the main objective of the investigation. It effectively communicates the convergence of artificial intelligence, facial-age detection techniques, and IoT innovations to confront the challenges of data security within social media environments.

Figure 5 shares an efficiently encapsulates integration of artificial intelligence, facial-age detection systems, and IoT technology approach for mitigating unauthorized access of the social media.

Matrix Performance Score

The confusion matrix in this study, is structured side side the table that delineates the performance metrics of a classification model.

Figure 6 Confusion Matrix. The Confusion Matrix contrasts the true class labels with those predicted by the model, showcasing the quantities of True Positives, True Negatives,

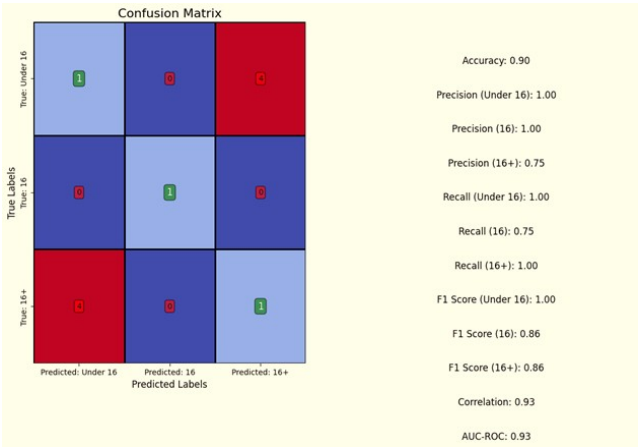

Figure 6: Confusion Matrix

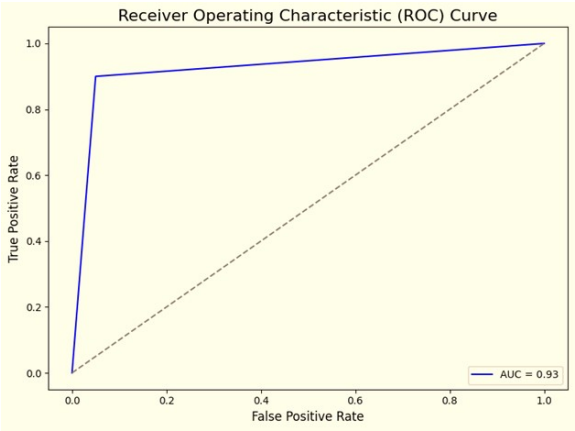

Figure 7: ROC Curve

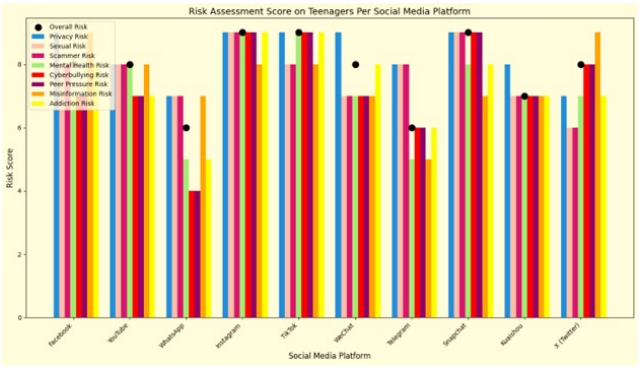

Figure 8: Risk Assessment Score on Teenagers Per Social Media Platform

False Positives, and False Negatives. This comparison is vital for evaluating the model's accuracy, precision, recall, and additional performance indicators.

ROC Curve

The Receiver Operating Characteristic (ROC) curve in this section, illustrates the balance between the True Positive Rate (also known as Recall) and the False Positive Rate across different threshold settings, thereby reflecting the performance of the model.

Figure 7 Receiver Operating Characteristic (ROC) curve. The Area Under the Curve (AUC) score measures the area encompassed by the ROC curve, serving as an indicator of the model's proficiency in differentiating between distinct classes.

Discussion

The rapid proliferation of social media platforms and the growing participation of teenagers have raised significant concerns regarding data security and the integrity of user authentication processes. Advances in artificial intelligence, the Internet of Things, and Radio Frequency Identification technologies have led to an escalation in data collection practices. Nevertheless, the corresponding rise in network traffic has resulted in an increase in data privacy violations. The challenges inherent in tracking and identifying internet users further complicate the landscape of monitoring and data protection. This research aims to explore viable solutions to enhance user authentication, decrease instances of privacy violations, and improve security on social media platforms, striving to achieve a balance between innovation and the implementation of stringent data protection measures..

Limitation of Facial-Age Detection

The shortcomings of facial age detection models can be summarized as follows.

Concerns regarding ethics emerge from the potential for age detection technology to be misapplied in surveillance and discriminatory contexts. The accuracy of such models is frequently undermined by biases present in the datasets, especially affecting those groups that are less represented. Compounding this issue are environmental variables, the variability of facial features, and the overlap in age ranges, all of which make accurate age determination challenging. Additionally, the differences in how individuals age introduce further inconsistencies in the predictions made by these technologies.

To overcome these limitations, it is essential to enhance the diversity of datasets, establish effective preprocessing methods, and integrate ethical considerations into the design and implementation of the model.

Significance of a Global Unify Internet ID

Apart from the numerous limitations, there is a way out. IP geolocation will be precise with a unique user ID even when using VPNs, proxies, and mobile networks that seen to obscure users actual location. Wi-Fi SSID-based location identification will not rely on a pre-existing database of Wi-Fi networks and its locations as every user can be track through their global unique ID. Unifying ID will eliminate the problems of Cellular network data accuracy that significantly depending on the strength of cell towers to trace users location. Identifying user location will not depend on factors such as rural and less-developed areas. Unique ID for internet users will assist Network latency analysis estimate exact distance of the internet user and will not depend on network congestion and routing paths. Also, ISP information swill be able to narrow down to the user's location accurately and will not depend if the location is with large ISPs covering vast areas or not. Device GPS requires user consent, which is sometimes require user consent. User unique internet ID will eliminate the need request for user location and will not interfere with privacy issues.

Risk Impact of Social Media Platforms on Teenagers

Social media platforms such as Instagram and TikTok have a profound impact on the mental health of adolescents, often fostering unrealistic beauty ideals and exacerbating issues related to body image, cyberbullying, and peer pressure.

Figure 8 Teenagers Social Media Platform & Risk Assessment Score. The following platform exhibit different impact on teenager. We present some of the challenges below.

Social media platforms significantly impact adolescent behavior and well-being. **Facebook** facilitates social connections but spreads misinformation and fosters cyberbullying. **YouTub**e enhances learning but risks exposure to harmful content and addictive behaviors. **WhatsApp** improves communication but raises privacy concerns. **Instagram** promotes creativity but exacerbates unrealistic beauty standards and mental health issues. **TikTo**k stimulates imagination but encourages peer pressure and exposure to negative trends. **WeChat** enables connectivity yet threatens privacy and excessive engagement. **Telegram** offers secure communication but exposes users to unmoderated content. **Snapchat** promotes expression but fosters cyberbullying and expectations for rapid replies. **Kuaishou** encourages creativity but promotes addiction and unverified content. **X (Twitter)** provides information but spreads misinformation and encourages harassment.

Conclusion

This research underscores the transformative capabilities of artificial intelligence, the Internet of Things, and technologies such as GPS, RFID, and deep learning in improving data security and user authentication within social media environments. The proposed framework emphasizes "security for information," tackling significant challenges to foster a secure and transparent digital landscape. Future investigations will aim to incorporate multi-factor authentication and real-time threat detection mechanisms. Additionally, the study promotes five essential models to guarantee efficient, dependable, and secure systems: an ID-based service model, multi-operation management, service-combined management, intelligent inventory transport, and sensor-based tracking. The transition from "information for security" to "security for information" signifies a broader emphasis on data-driven insights into human behavior.

Availability of Data and Material Used

All other information underlying analysis used to developed the results are available as part of the article and no additional source data are required or reserved somewhere. We have no funding nor conflicts of interest to disclose.

References

Al-Sabti, D. A.; Singh, A. V.; and Jha, S. 2017. Impact of social media on society in a large and specific to teenagers. In *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 663–667. IEEE.

Alim, S. 2016. Cyberbullying in the world of teenagers and social media: A literature review. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, 6(2): 68–95.

Costa, F.; Genovesi, S.; Borgese, M.; Michel, A.; Dicandia, F. A.; and Manara, G. 2021. A review of RFID sensors, the new frontier of internet of things. *Sensors*, 21(9): 3138.

Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; and Kashif Bashir, A. 2022. A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, 33(6): e3935.

Dennen, V. P.; Choi, H.; and Word, K. 2020. Social media, teenagers, and the school context: a scoping review of research in education and related fields. *Educational Technology Research and Development*, 68(4): 1635–1658.

Gupta, B. B.; and Quamara, M. 2020. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, 32(21): e4946.

Jayaram, K.; Janani, K.; Jeyaguru, R.; Kumaresh, R.; and Muralidharan, N. 2019. Forest fire alerting system with GPS Co-ordinates using IoT. In *2019 5th international conference on advanced computing & communication systems (ICACCS)*, 488–491. IEEE.

Jia, X.; Feng, Q.; Fan, T.; and Lei, Q. 2012. RFID technology and its applications in Internet of Things (IoT). In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, 1282–1285. IEEE.

Khan, S. I.; Ray, B. R.; and Karmakar, N. C. 2024. Rfid localization in construction with iot and security integration. *Automation in Construction*, 159: 105249.

Khoo, B. 2010. RFID-from Tracking to the Internet of Things: A Review of Developments. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, 533–538. IEEE.

Luthfi, A. M.; Karna, N.; and Mayasari, R. 2019. Google maps API implementation on IOT platform for tracking an object using GPS. In *2019 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, 126–131. IEEE.

Nikooghadam, M.; Shahriari, H. R.; and Saeidi, S. T. 2023. HAKECC: Highly efficient authentication and key agreement scheme based on ECDH for RFID in IOT environment. *Journal of Information Security and Applications*, 76: 103523.

Orben, A. 2020. Teenagers, screens and social media: a narrative review of reviews and key studies. *Social psychiatry and psychiatric epidemiology*, 55(4): 407–414.

Ping, H.; Wang, J.; Ma, Z.; and Du, Y. 2018. Mini-review of application of IoT technology in monitoring agricultural products quality and safety. *International Journal of Agricultural and Biological Engineering*, 11(5): 35–45.

Samee, N. A.; Khan, U.; Khan, S.; Jamjoom, M. M.; Sharif, M.; and Kim, D. H. 2023. Safeguarding online spaces: a powerful fusion of federated learning, word embeddings, and emotional features for cyberbullying detection. *IEEE Access*.

Şen, S. S.; Cicioğlu, M.; and Çalhan, A. 2021. IoT-based GPS assisted surveillance system with inter-WBAN geographic routing for pandemic situations. *Journal of Biomedical Informatics*, 116: 103731.

Shaik, A.; Bowen, N.; Bole, J.; Kunzi, G.; Bruce, D.; Abdelgawad, A.; and Yelamarthi, K. 2018. Smart car: An IoT based accident detection system. In *2018 IEEE global conference on internet of things (GCIoT)*, 1–5. IEEE.

Sheng, M.; Zhou, D.; Bai, W.; Liu, J.; and Li, J. 2022. 6G service coverage with mega satellite constellations. *China Communications*, 19(1): 64–76.

Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; and Markakis, E. K. 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 22(2): 1191–1221.

Sun, C. 2012. Application of RFID technology for logistics on internet of things. *AASRI procedia*, 1: 106–111.