Threat Modeling of Age-Restricted Content Access Systems: A Cybersecurity Perspective

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Kingslin, Sumathy, and D. Dhivya. "Threat Modeling of Age-Restricted Content Access Systems: A Cybersecurity Perspective." *Shanlax International Journal of Arts, Science and Humanities*, vol. 13, no. 3, 2026, pp. 93–96.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i1-Feb.10266

Dr. Sumathy Kingslin
Associate Professor
PG and Research Department of Computer Science
Quaid-E-Millath, Govt College for Women (A), Anna Salai, Chennai

D. Dhivya
Research Scholar, PG and Research Department of Computer Science
Quaid-E-Millath Govt College for Women (A), Anna Salai, Chennai

Abstract

The popularity of the use of online video streaming services has created an amplified fear on the issue of under-age viewers viewing age restricted content. The current methods of age-gating, self-stated date of birth, parental PINs, and document verification offer partial protection and can be easily overcome. This paper discusses the concept of age-restricted access systems through the cybersecurity lens and formulates the systematized threat model based on the STRIDE methodology. Client devices, networks, applications, and human interaction points are all considered through attack surfaces to determine the threats like spoofing, tampering, repudiation, information disclosure, and adversarial automation. It proposes a layered defense architecture comprising of authentication hardening, behavioral analytics, and privacy-preserving verification. The article highlights the importance of standard security assessment models to achieve efficient security protection of minors in online entertainment systems.

Keywords: Cybersecurity, Threat Modeling, Age Restriction, Multimedia Security, STRIDE, Child Online Safety.

Introduction

Children have been reduced to digital entertainment as the main source of information and leisure. Although these services are beneficial in educational aspect, they also expose the minors to violent, explicit or psychologically damaging content. In order to manage this risk, the providers have age-restriction measures; however, these are more oriented to low-risk scenarios and presuppose that the user behaves sincerely. Studies on child internet safety show that underage people often circumvent age restrictions by using a false date of birth or a joint account [1]. Security engineering wise, these are mechanisms that do not possess strong authentication and non-repudiation property [2].

The age verification should therefore be handled as a security-critical control just as authentication in financial systems [3]. The further development of generative artificial intelligence suppresses

conventional methods even more, allowing impersonation with the help of deepfakes and the creation of accounts automatically [4]. Continuous check or constant threat observation is rarely a part of current practices, and platforms can be easily manipulated [5].

This essay examines access control systems that limit access based on age by looking at them through a lens of cybersecurity as opposed to a particular verification system. These aim to (i) determine the attack surfaces of multimedia platforms, (ii) use a formal threat modeling framework, and (iii) provide a layered defense architecture that is balanced to protect, use, and provide privacy. The research includes a technology-neutral security model which can be used to inform platform designers and regulators.

Background and Related Context

Existing Age-Gating Practices

The most typical ones are self-proclaimed date of birth at the time of registration, parental PINs on joint devices, and periodic verification of documents. These are approaches based on honesty and do not provide much opposition to aggressive conduct. It has been demonstrated by security studies that users tend to share credentials among family members, which compromises account-based restrictions [6]. Sensitive services require one-time checks to be ineffective as there may be a change of circumstances during a session [2].

Cybersecurity Perspective

Threat modeling is a methodical method of predicting the way attackers are going to break a system [7]. The most popular taxonomy to this end is a taxonomy proposed by STRIDE, which is spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [7], [8]. In the case of child-intensive services, regulatory frameworks, including COPPA and GDPR-K [9], [10], require privacy-by-design and data minimization principles.

Threat Modeling Methodology

The analysis considers four principal attack surfaces:

1. The client device executing the application,
2. The network channel to backend services,
3. The application infrastructure managing policies
4. The human interaction layer involving parents or guardians. Applying STRIDE to these surfaces reveals multiple weaknesses.

Spoofing is a situation in which minors pose as adults with borrowed credentials or synthetic media. Tampering involves the use of local application files, blocking parental extensions, or any form of manipulating API requests [5]. The lack of reliable audit trails of profile changes in the system leads to repudiation. Information disclosure is a leakage of the viewing history or identity documents of the child because of unsecured storage [2]. Denial of service can also address verification endpoints in order to cause legitimate access, whereas elevation of privilege can be used to change restricted to unrestricted modes without due care.

Automation with the help of AI brings in new vectors. Bots can generate adult accounts in large quantities, and different adversarial tools have the potential to corrupt verification systems [4]. Such threats require dynamic defenses as opposed to rule-based controls.

Analysis of Attack Vectors

The most widely occurring risk is spoofing. Devices are shared by families and the minors can easily use the adult account without much restriction [1]. Attackers can use deepfake photos or

pre-recorded videos to cheat verification even in platforms that have secondary confirmation [4]. Threats of tampering attack the software environment, reverse engineering of mobile apps can identify some hidden flags to use against age modes, and VPN tools are often utilized to bypass geographical limitations [5].

Social engineering is also important. faked pages imitating the verification screen collect guardian credentials, and children can convince members of the adult population to temporarily disable restrictions [6]. The impact of the information disclosure is dire as the process of verification can consist of confidential family information; verifying it without proper encryption can result in permanent negative effects on the privacy [2]. These results show that age-gating needs to be developed as rigorously as digital identity.

Proposed Defense Architecture

Defense-in-depth should be advised. The identity assurance layer enhances verification by multi-factorizing confirmation, trusted device lists and periodic re-authentication, which are guidance in digital identity standards [2]. Instead of one check, access decisions must include context (e.g. device history, session continuity).

An analytics layer of behavior is used to track the usage patterns and identify any behavior that could be account sharing or compromise. An abrupt change in viewing patterns or location of access may cause step-up verification and do not add friction to standard users [3]. The application security tier puts in place safe coding standards, API gateway, integrity checks, and rate limits to prevent tampering and bots [5]. Lastly, a privacy layer will provide little data processing, local computation where possible, and open consent management in accordance with child-protection laws [9], [10].

Regulatory and Ethical Considerations

The field of protection of minors overlaps with the legal provisions of COPPA, GDPR-K, and national laws on information technology. These demand proportionality, data minimization as well as parental control [9], [10]. Too much monitoring may encroach on the rights of the children, as such the solutions should be able to balance the safety and dignity and autonomy [1]. Any method of verification must not engage in incessant storage of sensitive personal information and must offer explicable judgments [8].

Discussion

This analysis shows that access restriction concerning age cannot be regarded as a peripheral aspect. It is a fundamental security operation, which should be as rigorous as digital identity management. Adversarial capability and user honesty are highly undervalued and overestimated in the current practices in the industry. It would be beneficial to have benchmarks against which age-gating security can be judged to promote a more uniform protection level across platforms. Cybersecurity researchers, child psychologists, and policymakers need to collaborate in order to develop effective and socially-acceptable solutions.

Conclusion

This paper gave a cybersecurity-based analysis of age-restricted content access system. Using the STRIDE framework, significant weaknesses in both the technical and human levels were determined and a layered defense model suggested. The use of age verification as an element of security instead of a formality is more vital in protecting children in the digital age. The next round of research should be conducted in the form of formal risk assessment and user-oriented testing, as well as establishment of age-gating technology standardized security metrics.

References

1. S. Livingstone and M. Stoilova, The 4Cs: Classifying Online Risk to Children, London School of Economics, 2021.
2. National Institute of Standards and Technology, Digital Identity Guidelines (SP 800-63), NIST, 2020.
3. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Wiley, 2020.
4. R. Chesney and D. Citron, "Deep fakes: A looming challenge for privacy and security," California Law Review, vol. 107, no. 6, 2019.
5. OWASP Foundation, Application Threat Modeling Guide, 2023.
6. J. Bonneau, C. Herley, P. Van Oorschot, and F. Stajano, "The quest to replace passwords," in Proc. IEEE Symposium on Security and Privacy, 2012.
7. A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014.
8. Microsoft Security, STRIDE Threat Model Overview, 2021.
9. U.S. Federal Trade Commission, Children's Online Privacy Protection Act (COPPA), 1998.
10. European Union, General Data Protection Regulation – Child Provisions (GDPR-K), 2018.
11. ENISA, Cybersecurity and Child Online Protection, European Union Agency for Cybersecurity, 2022.
12. Information Commissioner's Office, Age Appropriate Design Code, UK ICO, 2020.