Review of Secure User Identity Management Systems (UIMS) for Preventing and Controlling Cybercrime

Ernest O. NONUM, OJO O. Daniel.

Department of Computing Sciences, Admiralty University of Nigeria, Delta State

DOI: https://doi.org/10.51584/IJRIAS.2025.10030055

Received: 16 March 2025; Accepted: 20 March 2025; Published: 16 April 2025

ABSTRACT

The Internet has become the backbone of global communication, commerce, and daily life in today's interconnected world. While it has brought countless benefits, the digital age has also ushered in an era of sophisticated cybercrime. As organisations grow and add services such as e-commerce and global remote access services, controlling who is accessing what kind of information is also becoming a difficult task. From phishing attacks and identity theft to ransomware and financial fraud, cybercriminals exploit vulnerabilities in online systems, often targeting weaknesses in identity management. Addressing this threat requires a robust solution, and implementing a **User Identity Management System (UIMS)** emerges as a key strategy to secure digital identities and prevent cybercrime. In Nigeria, the trends of employing identification systems using textual information or conventional fingerprint biometrics for identification have not proved effective. An identification system, which employs fingerprint biometrics and conducts a one-to-many pattern-matching to authenticate the claimed identity of an individual (student), is proposed in this paper. This article explores some pivotal roles of UIMS in cybersecurity, its critical components, real-world applications, and future directions, providing a comprehensive overview of how identity management can mitigate cybercrime risks. Some of these roles included a two-factor authentication technique used in developing a system, and the traditional username and password were included with biometric features for robustness. Displayed the development and verification of user identity with strong, reliable Python IDM methods (Authentication), showed the implementation of a fingerprint module for the authorisation of clients, and tracked and analysed user actions to identify anomalies. Ensuring that identity data is protected and used responsibly, adhering to legal standards, results from a survey on why computers or networks are tools targeted or placed for cybercrimes and factors contributing to cybercrimes.

Keywords: Cyber Security, User Identity, Cyber Crime, Biometrics, Two-factor Authentication,

INTRODUCTION

User identities serve as the keys to accessing digital resources. When attackers gain access to these keys, they can impersonate legitimate users, bypass security systems, and carry out unauthorized actions, such as stealing data, initiating fraudulent transactions, or planting malware. Weak identity management systems, especially those relying solely on traditional username-password combinations, are particularly vulnerable. *(T. Alese, O. Owolafe, A. F. Thompson, B. K. Alese, 2021)* The fast speed of information transmission across the Internet and computer networks has made information dissemination almost instantaneous and affordable. Also, the rise in technological innovation and online communication has not only produced a dramatic increase in the incidence of criminal activities but has resulted in the emergence of a somewhat new variety of computer-related criminal activities. Thus, the complexity of the increase in the incidence of criminal activities and the possible emergence of new varieties of cybercrimes pose challenges for the legal system and law enforcement.

Cybercrime is any criminal activity carried out through digital systems, networks, or the internet. It includes many offences, such as data breaches, intellectual property theft, financial fraud, and malicious hacking. One common denominator in many of these activities is the misuse of user identities. Whether through stolen credentials, social engineering, or brute force attacks, cybercriminals often exploit identity vulnerabilities to execute their schemes.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

As the Internet came into widespread commercial use, the nature of computer crimes began to shift. 'While in some crimes, one component of the crime may have been committed using an electronic instrument, in other crimes, the crime as a whole is committed in the online or electronic environment. These crimes, known as cybercrimes, generally occur in the virtual community of the Internet or cyberspace. Viruses, worms, and Trojan horses are another serious threat. There is a variety of Cyber Crimes committed, but these are the most prevalent and appear to be among the most troubling to computer users. *(Mshana, 2015).*

This paper explores how modern user identity management systems can reduce the risk of cybercrime by providing secure authentication, real-time monitoring, and advanced technologies like biometrics.

LITERATURE REVIEW

The concept of this study lies in addressing the growing threats posed by cybercrime in an increasingly digital world. As online platforms and services become integral to daily life, the need for robust cybersecurity measures, particularly in identity management, has never been more critical. This study explores the reviews from different sources of a **User Identity Management System (UIMS)** as a comprehensive solution for securing digital identities, which are often the primary targets of cybercriminals. Some findings and insights from this study are significant for several key stakeholders, like Organizations and businesses, Government and Policymakers, the Technology and cybersecurity Industry, Academia and Researchers, and Individual Users.

This study is significant for its potential to influence the development and adoption of robust identity management practices that not only combat identity theft, fraud, hacking, and other forms of cybercrime but also foster a safer and more trustworthy digital ecosystem.

There has been a lot of research in the field of Secure User Identity Management Systems for preventing and Controlling Cyber Crime.

(T. Alese, O. Owolafe, A. F. Thompson, B. K. Alese, 2021) Gave an overview of the structure of the identity management system; the proposed identity management system consisted of a few properties whereby the client/user receives services from a service provider through the provision of partial identity with the identifier and the associated credential from the connecting identity provider. A client can be in the form of any entity, but this project is based on the assumption that each client is a person/user. The user profile for the project involved a set of user attributes that were used for customising the service and possibly restricting access to portions of the service. The control of access to the service provided also depended on the accuracy of user profile information, which assisted in making appropriate policy decisions. Access control entails granting access to particular resources and the auditable enforcement of that policy.

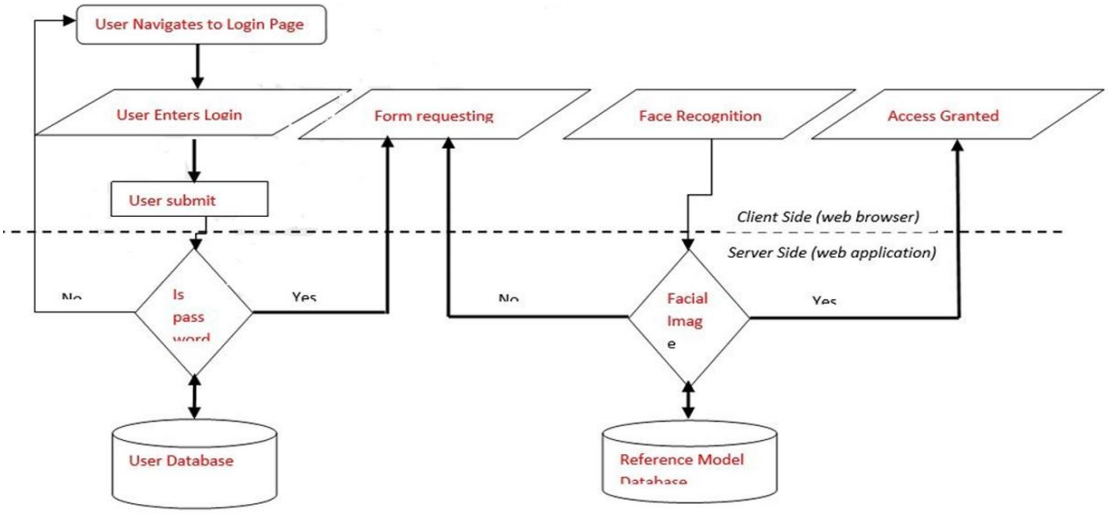

Figure 1: An overview of the structure of the Identity management system.

(Alese et al., 2021)

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

A workflow model was proposed for the system, which entails two providers;

1. Service Provider (SP): An organisation that provides services to clients or other SPs. It could also be referred to as the Trusted Party. This work adopted the use of the notation "SP" to denote the set of service providers.
2. Identity Provider (P): An organisation that provides digital identities to allow clients to receive services from an SP. In this work, the notation "P" is used for the set of identity providers. The life cycle of the proposed IDM system is made up of four (4) phases: registration, identification/authentication, authorisation, and deregistration.

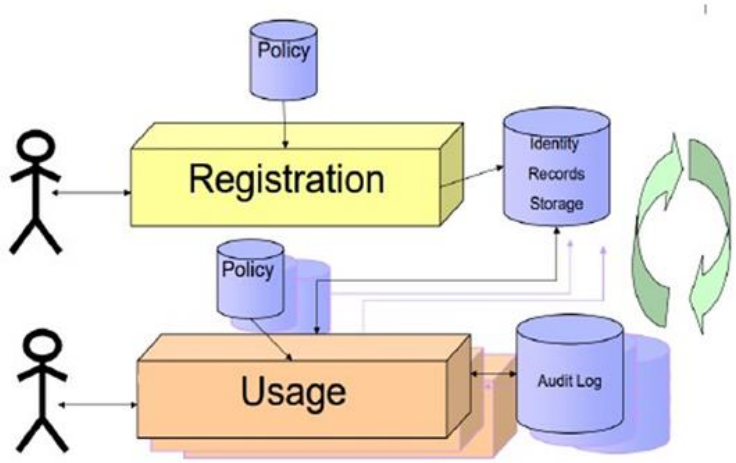

Figure 2: Workflow model of the proposed system.

(Alese et al., 2021)

(T. Alese, O. Owolafe, A. F. Thompson, B. K. Alese, 2021) Designed a Bio-Reg which is in three levels, namely: System Module, Algorithm Module, and User Module. Issues considered in the System Module include the process of capturing the digital representation of the biometric data and the hardware to be used. The Algorithm Module involves two phases: the Feature Extraction Phase and the Feature Matching Phase.

The Feature Extraction Phase is responsible for the extraction of fingerprint features, and the Feature Matching Phase determines whether two sets of representative features are extracted from the same source by matching the minutiae pattern from the captured sample with those in the database to determine any correspondence between them.

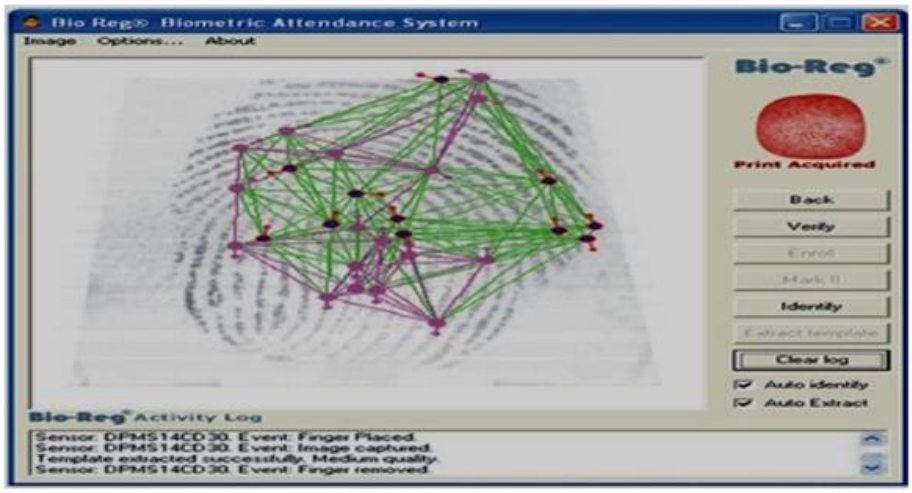

Figure 3. Digital Image of a Captured Finger.

(Alese et al., 2021)

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

(H.J, 2022) Focused on providing some top network attacks and Cyber Security techniques in mitigating them; this analysis was represented in a chart form to show the percentage of harm to the computer user.

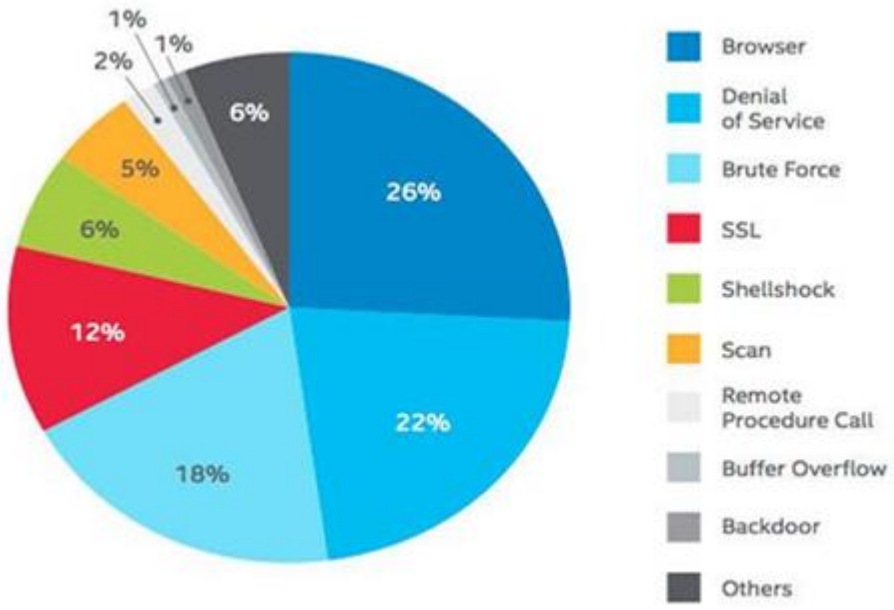

Figure 4: The above pie chart shows the major threats to networks and cyber security (Source: (Pallangyo, 2022).

Some techniques for mitigating these crimes include Access Control & Password Policy, Authentication of data, Malware scanners, Firewalls, and Anti-virus software.

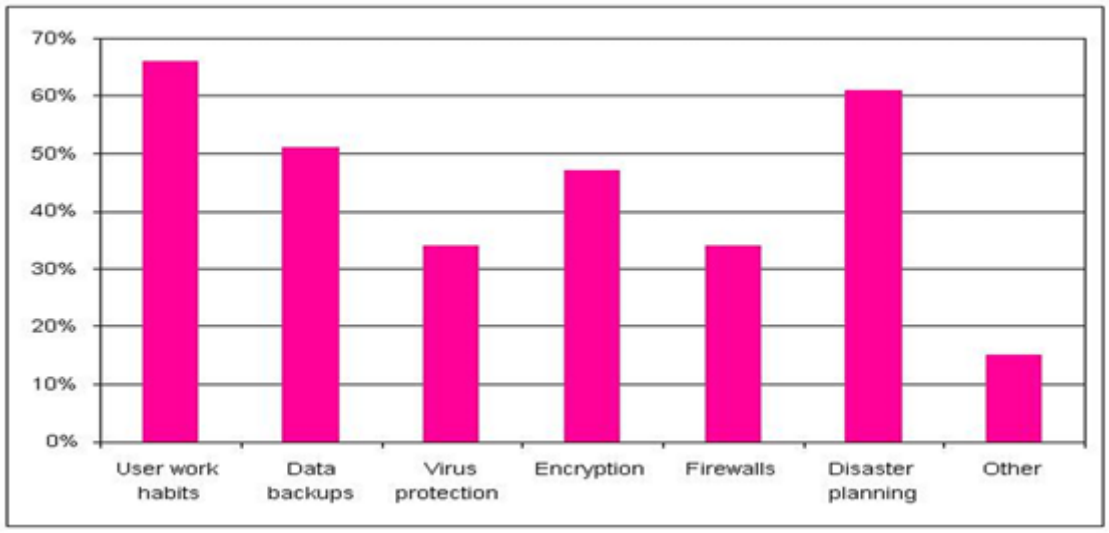

Figure 5: Techniques on Cyber Security(J. A., n.d.).

(Mshana, 2015) Surveyed the impact of cybercrimes on society, why computers/networks are targets for cybercrimes, and factors contributing to cybercrimes.

The survey research method was used because bias was less likely as subjects were randomly assigned to treatments, and subjects and researchers were blind to the identity of the treatments. Questionnaires and interviews were used for data collection. The researcher developed a questionnaire based on literature and related research. Surveys were used to gather information from the two educational institutions to represent youths, 15 musicians, 10 actors and five companies to explore different types of cybercrimes and their impacts. Data was obtained from 100 students from each educational institution and five members of

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

management from each company, to make a total of 250 as the sample size of the study. Out of 250 people, 200 responded, which is 80%. The survey respondents were small but informative and accurate because the instrument was reviewed before.

The researcher collected the data from the respondents through email and directly from the interview as a procedure after the distribution of questionnaires to the five educational institutions, and scoring was done after the collection of data. The five-point rating scale was used to record the score of all positive statements ranging from 5-1 for different response categories. Strongly Agree (SA), Agree (A), Undecided (U), Disagree (DA), and Strongly Disagree (SDA).

S/N	Impacts	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Child exploitation	N	120	70	0	10	0
		%	(60)	(35)	(0)	(5)	(0)
2.	Harassment	N	100	80	10	0	10
		%	(50)	(40)	(5)	(0)	(5)
3.	Digital Piracy	N	70	120	10	0	0
		%	(35)	(60)	(5)	(0)	(0)
4.	Hacking	N	80	80	10	20	10
		%	(40)	(40)	(5)	(10)	(5)
5.	Intentional damage	N	60	80	40	10	10
		%	(30)	(40)	(20)	(5)	(5)
6.	Spam	N	110	60	10	20	0
		%	(55)	(30)	(5)	(10)	(0)

Figure 6: Impacts of Cybercrimes in the society (Mshana, 2015).

S/N	Reasons	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Availability	N	100	80	10	10	0
		%	(50)	(40)	(5)	(5)	(0)
2.	Easy access	N	70	100	10	10	10
		%	(35)	(50)	(5)	(5)	(5)
3.	Affordable	N	60	100	20	10	10
		%	(30)	(50)	(10)	(5)	(5)

Figure 7: Why computers or networks are tools targeted or placed for cybercrimes (Mshana, 2015).

S/N	Factors	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Growth of the Technology	N	90	70	0	20	20
		%	(45)	(35)	(0)	(10)	(10)
2.	Economic factor	N	100	60	20	10	10
		%	(50)	(30)	(10)	(5)	(5)

Figure 8: Factors contributing to cybercrimes (J. A., n.d.).

(Akeem Olalekan AYUB & Linus AKOR (PhD)) Gave some consequences of cybercrimes, particularly in Nigeria as a nation. The study of the costs of cybercrime are enormous and mindboggling, and has identified cybercrime costs to include destruction of data, loss of productivity, thefts of money, intellectual property and personal data, disruption of business activities, restoration and deletion of data and systems, reputational harm and embezzlement (Morgan, 2017).

In Nigeria, cybercrime causes a lot of damage to the country's international image and reputation. Many Nigerians who travel outside the shores of the country are daily subjected to undue stigmatization and name-calling because of the activities of some Nigerian cybercriminals. Many Nigerians are treated without honour, respect, and dignity because some foreigners see and treat people of Nigerian extraction as

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

scammers, fraudsters, dupes, 419ers, etc. Such demeaning characterisation has done incalculable damage to the international image of Nigeria.

In financial terms, cybercrime has done grave damage to Nigeria's economy as the country is believed to have lost an estimated $9.3 billion to cybercrime in addition to other potential financial losses emanating from the erosion of consumer confidence and the stalling of foreign direct investment. Frank and Odunayo (2013) lamented that more than $80 billion is lost to software piracy annually in Nigeria, describing the trend as one of the fastest-growing online scams largely perpetrated by young Nigerians. (*AYUB & AKOR, n.d.)*

MATERIALS AND METHODOLOGY

This research study employed a qualitative and survey-based approach to examine the effectiveness of User Identity Management Systems (UIMS) in preventing and controlling cybercrime. Data was collected through multiple methods, including literature reviews, surveys, interviews, and expert discussions.

1. Literature Review: Academic journals, books, and case studies were analyzed to identify trends in identity management and cybercrime prevention.
2. AI Chat-Box Results: AI-based tools were consulted for exploratory insights, but the results were not considered peer-reviewed. Instead, they were used to identify emerging trends and potential areas for further investigation.

ANALYSIS OF RESULT

The analysis established that the User Identity Management System serves as a critical tool for organizations and governments to combat cybercrime. Below are some critical components and real-world examples of User Identity Management Systems (UIMS);

1. Advanced Authentication Methods: Traditional password-based authentication is no longer sufficient; a secure User Identity Management System must be integrated, some of which are:

1. Biometrics: Technologies like facial recognition, fingerprint scanning, and retina scanning provide unique and secure ways to verify identities.
2. Multi-Factor Authentication (MFA): Combining something users know (passwords), have (security tokens), and are (biometrics) ensures robust security.
3. Password-less Authentication: Cryptographic keys, smartphone-based verification, or biometric-only solutions eliminate the vulnerabilities of traditional passwords.

2. Identity Federation and Single Sign-On (SSO): A UIMS should support identity federation, allowing users to access multiple systems with a single identity, and SSO to streamline authentication across services. These features reduce vulnerabilities arising from managing multiple credentials. Okta is a leading identity management solution that provides Single Sign-On (SSO), Multi-Factor Authentication (MFA), and lifecycle management. It helps organizations securely manage user identities and access to applications and data.

3. Role-Based Access Control (RBAC): A UIMS should implement RBAC to assign access rights based on roles, ensuring that users can only access information or systems relevant to their tasks. This minimises the risks of accidental or intentional misuse. A real-world example is Auth0, an identity management platform that provides authentication and authorization services. It offers features like SSO, MFA, and user management to ensure secure access to applications.

4. Strong Privacy Safeguards: A UIMS must comply with regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Encryption, pseudonymisation, and secure data storage are essential to protecting user privacy.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

The analysis indicated how the UIMS serves as a critical tool for organizations and governments where;

1. Advanced Authentication Methods – The UIMS enhances security through multi-factor authentication (MFA), biometrics, and password-less authentication, which significantly reduce the risks associated with password-based breaches.
2. Identity Federation and Single Sign-On (SSO) – These features streamline authentication across multiple services while reducing the chances of identity-related attacks.
3. Role-Based Access Control (RBAC) – This mechanism minimizes insider threats and unauthorized access by ensuring that users only access what is necessary for their role.
4. Regulatory Compliance and Privacy Protection – The UIMS adheres to data protection regulations like GDPR and CCPA, ensuring that identity data is securely managed and reducing the risk of data leaks.

Furthermore, some key applications of the User Identity Management System for preventing and controlling cybercrime include;

1. **Protecting Financial Systems:** Banks and financial institutions use UIMS to secure online banking platforms and prevent fraud. Multi-factor authentication and behavioral analytics play a vital role in ensuring safe transactions.
2. **Safeguarding E-Commerce:** E-commerce platforms integrate a User Identity Management System to protect customer accounts and prevent unauthorized purchases or account takeovers.
3. **Enhancing National Security:** Governments implement UIMS in critical infrastructure, defense systems, and public services to prevent identity-based cyberattacks, including espionage and sabotage.

Different regions have adopted varying approaches to UIMS, influenced by legal, technological, and infrastructural factors. Providing a comparative analysis across regions to show the need for regulatory harmonization to enhance global adoption:

1. **Europe:** GDPR mandates strict privacy controls, requiring organizations to use consent-based identity management. AI-enhanced UIMS in Europe prioritize encryption and decentralized identity verification.
2. **North America:** The U.S. relies on multi-factor authentication (MFA) and zero-trust models. AI-driven behavioral analytics are widely used to enhance identity verification.
3. **Asia:** Countries like China have advanced biometric authentication in the public and private sectors. However, concerns over data privacy and government surveillance persist.
4. **Africa:** Adoption of UIMS is growing, but infrastructural limitations and regulatory gaps hinder widespread implementation.

Emerging technologies like machine learning and AI, and blockchain are revolutionizing user identity management and cybercrime prevention. Here are some instances:

In User Identity Management

1. Machine Learning and AI: Machine learning algorithms can predict identity theft and automate identity verification processes. AI-driven identity management systems offer real-time fraud detection, anomaly tracking, flagging deviations for further authentication, and automated identity verification. However, their implementation presents several technical challenges, such as:

- **Security Risks:** AI models can be vulnerable to adversarial attacks where malicious actors manipulate biometric data or behavioral analytics to bypass security measures. Additionally, deepfake technology poses a risk to facial recognition systems.
- **Infrastructure Challenges:** AI-powered UIMS require robust computational resources and cloud-based architectures. Scalability and integration with legacy systems remain hurdles, especially for large-scale deployments.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

- **Computational Costs:** AI-based solutions demand high processing power, increasing operational costs. Organizations must balance security and efficiency while ensuring user privacy compliance.

2. Blockchain: Blockchain provides a decentralized and immutable ledger for storing identity information. This ensures transparency and security, reducing the risk of identity fraud. The combination of AI and blockchain offers a robust solution for secure identity management.

In Cybercrime Prevention

1. **AI and Machine Learning**: AI's predictive capabilities help identify potential cyber threats early. Machine learning algorithms can detect patterns in cyber-attacks, enabling proactive measures to prevent breaches. AI can also automate responses to cyber threats, reducing the time taken to mitigate attacks.
2. **Blockchain**: Blockchain's decentralized nature makes it difficult for cybercriminals to alter data. It provides a secure method for recording transactions, ensuring data integrity. Blockchain can also be used to create tamper-proof logs of cyber incidents, aiding in forensic investigations.

While the User Identity Management System offers significant advantages, its implementation is not without challenges. Some of these **challenges** are;

1. **Scalability:** Managing millions of user identities, especially in large organizations or government systems, requires robust infrastructure.
2. **Cost:** High initial investment and ongoing maintenance costs can be barriers for small and medium-sized enterprises.
3. **User Adoption**: New authentication methods, particularly biometrics, may raise privacy concerns or resistance from users unfamiliar with the technology.
4. **AI Advancements:** AI-driven UIMS improves security but requires strong defenses against adversarial attacks.
5. **Biometric Authentication:** While biometrics enhance security, they also introduce significant risks:

i. **Data Breaches:** Unlike passwords, biometric data cannot be reset if compromised. High-profile breaches (e.g., Aadhaar data leaks in India) highlight vulnerabilities.
ii. **Privacy Concerns:** GDPR and other regulations impose strict guidelines on biometric data collection and storage. Organizations must implement encryption, anonymization, and strict access controls.
iii. **Legal Compliance:** Countries vary in biometric data governance. Europe enforces stringent privacy laws, whereas some regions have lenient regulations, increasing the risk of misuse.

As technology evolves, so will the capabilities of UIMS. Some anticipated advancements would be implemented; these advancements include:

1. **Quantum-Resistant Encryption:** Preparing for the era of quantum computing by adopting encryption algorithms resistant to quantum attacks.
2. **Integration with IoT**: Extending identity management to billions of connected devices, ensuring secure interactions in smart environments.
3. **Self-Sovereign Identity (SSI)**: Allowing users to own and control their digital identities without relying on centralized authorities, leveraging blockchain and decentralized identifiers (DIDs).

CONCLUSION AND RECOMMENDATION

In the fight against cybercrime, securing user identities is a critical first step. A well-selected User Identity Management System provides a comprehensive solution, integrating advanced authentication, real-time monitoring, and robust privacy safeguards. While challenges remain, the ongoing development of UIMS technologies promises a safer digital future. Governments, businesses, and individuals must recognize the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

importance of investing in secure identity management systems to prevent and control cybercrime. By staying ahead of threats and adopting innovative solutions, we can build a secure and trustworthy digital ecosystem.

With the tremendous expansion of the Internet during the last twenty years or so, more and more identities and credentials have been issued, making their management challenging both for service providers and users. To address this menace, there is a need for the review of different identity management solutions to control cybercrime. An Identity Management system has the potential to provide a secure and collaborative environment. The proposed system is dynamic, and by integrating a face recognition system, the system has robust security. The solution can be rendered as a service to enhance the extra security layer for applications since authentication takes place outside the application. This frees the customer from the burden of installing and operating the application on their computer and also eliminates the dreadful load of software maintenance, continuing operation, safeguarding, and support.

Use of the Internet is a risk that most companies have to take. The problem is to minimize the risks associated with so doing. Suppose there is no technology, hopefully the cybercrimes would not be found anywhere. As has been discussed in the paper, preventive measures should be taken to protect society as well as organizations from cybercrimes instead of avoiding the use of the technology.

Cybercriminals are smart, intelligent, and dynamic youngsters who employ several methods to consummate their atrocities by consistently updating their tactics to understand the psychology of potential victims. These include the victims' gender, age, economic status, and occupational group. The state of mind and ego of the vulnerable are often manipulated by cybercriminals to successfully prey on them. Unfortunately, cybercrimes are patterned in such a way that it is quite difficult to apprehend many of the perpetrators. AI-enhanced UIMS plays a vital role in securing digital identities and preventing cybercrime. However, security risks, high computational costs, and legal compliance must be addressed. A balanced approach, integrating AI while ensuring data privacy, is key to the future of secure identity management systems.

This is why I recommend that Internet users secure their computer systems by enabling firewalls that are capable of blocking connections from suspicious traffic and using standard identity management systems in the devices to grant authorization to legitimate users. Also, internet users should protect their electronic identity by being cautious when giving out personal details such as name, phone number, address, or financial information on the internet. Biometric authentication must incorporate encryption and privacy-preserving techniques to comply with legal standards. Organizations should integrate AI-powered risk assessment models to detect anomalies in real-time, internet users should avoid being scammed by being sensitive to or not replying to emails that request them to verify certain information or confirm their username, user ID, or password. They should also guard against clicking links or opening files emanating from suspicious sources, no matter how genuine they may seem or appear.

REFERENCES

1. T. Alese, O. Owolafe, A. F. Thompson, B. K. Alese. (2021). A User Identity Management System for Cybercrime Control. *Nigeria Journal of Technology*, 130-132 .
2. Akeem Olalekan AYUB & Linus AKOR (PhD) . (n.d.). Trends, Patterns and Consequences of Cybercrime in Nigeria . *journals759articles*, 254-256.
3. F. A. U. Imouokhome and A. O. Egwali . (2014). AN IDENTITY MANAGEMENT MONITORING SYSTEM. *Scientia Africana, Vol 1*, 291-295.
4. Mshana, J. (2015). Cybercrime: An Empirical Study of its Impact in the Society- A Case Study of Tanzania . *Journal235articles*, 78-79.
5. Pallangyo, H. J. (2022). Cyber Security Challenges, its Emerging Trends on Latest Information and Cyber Crime in Mobile Money Transaction Services. *Full Length Research Paper* , 199-204.
6. Clarke, R., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue III March 2025

7. European Union General Data Protection Regulation (GDPR). (2018). Available at: https://gdpr-info.eu
8. IBM Security. (2023). *Cost of a Data Breach Report*. Retrieved from https://www.ibm.com/security/data-breachIBM Security. (2023). *Cost of a Data Breach Report*. Retrieved from https://www.ibm.com/security/data-breach
9. *Identity Management Institute*. (2023, March 7). Retrieved from Identity Management Institute Web site: http:// identity managementinstitute.org