Periodico di Mineralogia
ISSN: 0369-8963
Volume 93, No. 6, 2024

SECURITY ISSUES IN BIG DATA GENERATED IN EDUCATION FIELD

Rahul Waghamare[1], Dr. Bhavana Narain[2], Dr. B T Jadhav[3]

[1] Research Scholar, School of IT, MATS University, Raipur, CG
[2] School of IT, MATS University, Raipur, CG
[3] Yashavantrao Chavan Institute of Science, Satara

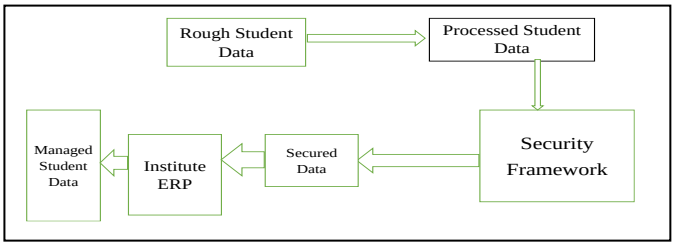
Abstract
Now a days BD (Big Data) and IoT (Internet of Things) are popular and mostly used terms in various fields. Education is one of the fields where large amount of data generated due to IoT devices used by Students, Teachers and Institute. Big data in education can originate from a variety of sources.

The volume and information gathered and generated from various IoT devices and applications and audio, video, images data by humans, organizations and applications are increasing every second and has almost doubled in year. There are different ways of data generating, we say that is heterogeneous data is generated. Data is gathered from a wide range of sources inside the educational system in order to evaluate the success of educational plans, monitor student growth, student behaviour, and assess student performance.

Here we have to systematically look into the security risks associated with big data streaming for Internet of Things devices in Education Fields. These are Data Privacy, Lack of Visibility, Limited Security Integration, Lack of Physical Security, Poor Testing, Open-source Code Vulnerabilities, and Overwhelming Data Volume etc.

In this research paper we focus on data generated in Education fields and on Security Issues. Big Data generated in Education fields have security issues and minimizes by applying Framework to minimize the security issues in Education Field. Framework is suggested to minimize the security issues as given below.

Keywords: *Key Index: Big Data, Analysis, Education fields*

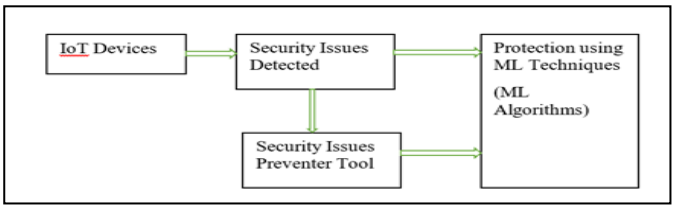


Graphical Abstract

1. INTRODUCTION

In recent years, the education sector has witnessed a significant transformation fuelled by the spread of digital technologies and the widespread adoption of data-driven decision-making processes. One of the most profound signs of this transformation is the emergence of Big Data in education, characterized by the collection, analysis,
and utilization of large volumes of data to enhance teaching, learning, and administrative processes. While Big Data holds huge ability for revolutionizing education, its common adoption also aises a many of security concerns that must be addressed to safeguard sensitive information and ensure the security, integrity and privacy of educational data.

There are number of security issues associated with Big Data generated in the education field. Through an examination of



the unique challenges and vulnerabilities in-built in educational data systems, this research paper aims to focus on the complications of securing Big Data in education and propose strategies and best practices for modifying security risks. We have to focus on security issues such as data privacy, authentication, access control, and data gaps, this research endeavours to provide educators, politicians, and stakeholders with actionable insights to support the security posture of educational institutions in the era of Big Data.

We have security challenges faced by educational organizations, analyse the potential consequences of security breaches in educational data systems, and outline practical measures to strengthen security protocols and safeguard sensitive information in the education field.

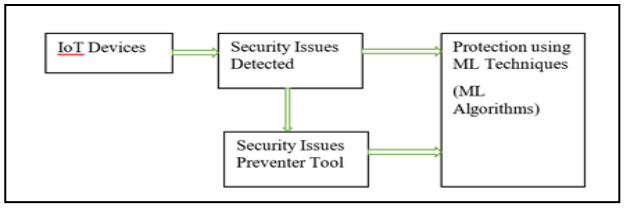


Fig: Security Framework

Securing educational institutions and their stakeholders has advanced significantly with the creation of a framework for resolving security concerns in the field of education using machine learning techniques. This research paper has allowed for suggest secures framework for security issues.

2. Data generated in the education field:

1. Student Performance Data: This includes data on academic achievement, test scores, grades, attendance records, and disciplinary actions.

https://doi.org/10.5281/zenodo.14032437

2. Teacher and Staff Data: Information about teachers and staff, such as qualifications, experience, professional development activities, and performance evaluations.
3. Enrolment Data: Data on the number of students enrolled in different programs, courses, or grade levels, as well as demographic information such as age, gender, race/ethnicity, and socioeconomic status.
4. Financial Data: Budgetary information, expenditure reports, funding sources, and financial aid data related to educational institutions.
5. Curriculum and Instruction Data: Data related to curriculum development, instructional materials, teaching methods, and educational technology usage.
6. Assessment Data: Data collected from formative and summative assessments, standardized tests, and other measures used to evaluate student learning and program effectiveness.
7. Special Education Data: Information on students receiving special education services, including Individualized Education Programs (IEPs), accommodations, and outcomes.
8. Graduation and Dropout Rates: Data on the number of students completing their educational programs successfully and those who leave school before completion.
9. School Climate and Safety Data: Surveys, incident reports, and other data related to school climate, safety measures, bullying, and student well-being.
10. College and Career Readiness Data: Information on college acceptance rates, career pathways, workforce readiness programs, and alumni outcomes.
11. Research Data: Data collected from educational research studies, including experimental data, survey responses, and qualitative observations.
12. Administrative Data: Data related to school operations, facilities management, transportation, and other administrative functions.

This data is collected, analysed, and used by educational stakeholders such as teachers, administrators, researchers, and parents to make informed decisions, monitor progress, improve educational outcomes, and ensure accountability within the education system.

3. Security Issues in Education Fields:

Developing a framework for addressing security issues in the education field using machine learning techniques involves understanding various threats and vulnerabilities specific to this domain. Here are some key security issues to consider:

1. Data Privacy: Educational institutions handle sensitive student and staff data, including personal information, academic records, and financial details. Protecting this data from unauthorized access, leaks, and breaches is crucial.
2. Cyber Attacks: Educational institutions are increasingly targeted by cybercriminals for various reasons, including ransomware attacks, phishing attempts, and Distributed Denial of Service (DDoS) attacks. These attacks can disrupt operations and compromise sensitive information.
3. Identity Theft: Educational systems often require users to provide personal information for registration, authentication, and access purposes. Weak identity verification processes can lead to identity theft and unauthorized access to educational resources.
4. Insider Threats: Employees, students, or other individuals with access to educational systems may pose a threat to security intentionally or unintentionally. This could include leaking sensitive information, abusing privileges, or introducing malware into the system.
5. Intellectual Property Theft: Educational institutions engage in research and development activities, producing valuable intellectual property. Protecting research data, patents, and copyrighted materials from theft or unauthorized use is essential.
6. IoT Security: The proliferation of Internet of Things (IoT) devices in educational environments introduces new security risks. Vulnerabilities in connected devices such as smart classrooms, wearable technologies, and campus infrastructure can be exploited by attackers.
7. Social Engineering: Attackers may use social engineering techniques to manipulate individuals within the educational institution into divulging confidential information or performing actions that compromise security.
8. Malware and Phishing: Malicious software and phishing emails are commonly used to gain unauthorized access to educational systems. Machine learning techniques can help in detecting and mitigating these threats by analysing patterns and behaviours.
9. Inadequate Security Awareness: Lack of awareness among students, faculty, and staff about cybersecurity best practices can increase the likelihood of security incidents. Training programs and awareness campaigns are essential to promote a culture of security within the institution.
10. Third-Party Risks: Educational institutions often rely on third-party vendors and service providers for various functions, including cloud services, learning management systems, and student information systems. Ensuring the security of these third-party relationships is crucial to prevent data breaches and other security incidents.
programming flow chart for the system

4. Tools for solve Security Issues:

Addressing security issues involves a combination of tools, practices, and approaches. Here's a rundown of some key tools commonly used in the field of cybersecurity:

1. Firewalls: Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. They can be hardware or software-based.
2. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): IDS monitor network or system activities for malicious activities or policy violations and report them, while IPS proactively blocks or prevents those activities.
3. Antivirus Software: Antivirus programs detect and remove malicious software (malware), including viruses, worms, and Trojan horses.
4. Vulnerability Scanners: These tools scan systems for known vulnerabilities, helping organizations identify and prioritize security issues.
5. Security Information and Event Management (SIEM) Systems: SIEM systems collect and analyze security data from various sources across an organization's IT infrastructure to identify and respond to security threats.

 https://doi.org/10.5281/zenodo.14032437

6. Encryption Tools: Encryption helps protect data by converting it into a code that can only be accessed with a decryption key. Tools like PGP (Pretty Good Privacy) or GnuPG (GNU Privacy Guard) provide encryption capabilities.
7. Penetration Testing Tools: These tools simulate cyberattacks on a computer system, network, or web application to identify vulnerabilities that attackers could exploit.
8. Multi-factor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of identification before accessing a system or application.
9. Secure Web Browsers and Plugins: Using web browsers and plugins that prioritize security features, such as sandboxing, automatic updates, and anti-phishing measures, can help mitigate security risks when browsing the internet.
10. Security Frameworks and Standards: Frameworks like NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls provide guidelines and best practices for implementing and managing cybersecurity programs effectively.

Remember, while these tools are essential, they should be part of a broader cybersecurity strategy that includes policies, procedures, and ongoing training to ensure comprehensive protection against evolving threats. Additionally, regular updates and maintenance of these tools are crucial to their effectiveness.

5. Framework for Security Issues:

Addressing security issues in the education field requires a comprehensive framework that covers various aspects such as data protection, physical security, cybersecurity, and policy implementation. Here's a step-by-step solution framework:

1. Assessment and Analysis:
- Identify potential security threats and vulnerabilities within the education system.
- Conduct risk assessments to prioritize threats based on their likelihood and potential impact.
- Analyse existing security measures and their effectiveness in mitigating risks.

2. Policy Development:
- Develop comprehensive security policies that address both physical and digital security concerns.
- Define roles and responsibilities for stakeholders involved in implementing security measures.
- Ensure compliance with relevant laws and regulations related to data protection and privacy.

3. Data Protection:
- Implement robust data protection measures to safeguard sensitive information such as student records, financial data, and personal information.
- Utilize encryption technologies to secure data both in transit and at rest.
- Establish data backup and recovery procedures to mitigate the risk of data loss or theft.

4. Cybersecurity Measures:
- Deploy firewalls, intrusion detection systems, and antivirus software to protect against cyber threats such as malware, phishing attacks, and ransomware.
- Conduct regular security audits and vulnerability assessments to identify and remediate potential weaknesses in the network infrastructure.
- Provide cybersecurity training and awareness programs for staff and students to educate them about best practices for maintaining security online.

5. Physical Security Enhancements:
- Implement access control measures such as biometric authentication, keycard systems, and security cameras to restrict unauthorized access to school premises and sensitive areas.
- Conduct security patrols and surveillance to monitor for suspicious activities and prevent incidents such as theft, vandalism, or intrusions.
- Ensure proper maintenance of physical infrastructure to address vulnerabilities such as broken locks or malfunctioning security equipment.

6. Incident Response and Recovery:
- Develop a formal incident response plan outlining procedures for detecting, responding to, and mitigating security incidents.
- Establish communication channels and escalation procedures for reporting security incidents to relevant authorities and stakeholders.
- Conduct post-incident reviews to identify lessons learned and implement improvements to prevent similar incidents in the future.

7. Continuous Improvement:
- Regularly review and update security policies and procedures to adapt to evolving threats and technologies.
- Engage in ongoing training and professional development for staff to ensure they remain informed about the latest security best practices.
- Foster a culture of security awareness and vigilance among all members of the education community.

By following this step-by-step framework, educational institutions can strengthen their security posture and better protect their students, staff, and sensitive information from potential threats and vulnerabilities.

6. Methodology

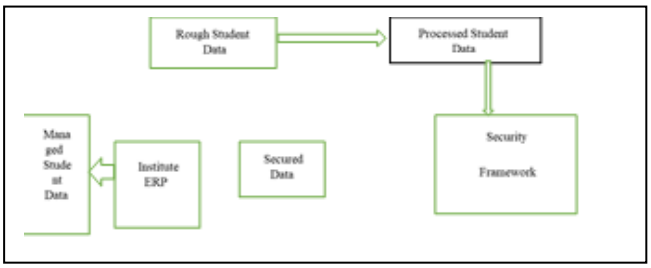


Fig 1: Security in Education Field

Certainly! Securing big data generated in the education field is crucial to protect sensitive information and ensure privacy. Here's a detailed methodology:

1. Identify Data Sources: Begin by identifying all data sources in the education sector. This could include student records, academic performance data, attendance records, teacher information, research data, and administrative records.
2. Data Classification: Classify the data based on sensitivity and importance. Some data, like student health records or financial information, may be more sensitive than others. This classification helps in determining the level of security measures needed for each type of data.

 https://doi.org/10.5281/zenodo.14032437

3. Risk Assessment: Conduct a comprehensive risk assessment to identify potential security threats and vulnerabilities. This assessment should consider both internal and external threats, such as unauthorized access, data breaches, malware attacks, and insider threats.
4. Data Encryption: Implement encryption techniques to protect data both in transit and at rest. This includes encrypting data stored in databases, on servers, and during transmission over networks. Strong encryption algorithms and key management practices should be employed.
5. Access Control: Establish robust access control mechanisms to ensure that only authorized users can access sensitive data. This involves implementing role-based access control (RBAC), multi-factor authentication (MFA), and least privilege principles to limit access to data based on user roles and responsibilities.
6. Data Masking and Anonymization: Implement techniques such as data masking and anonymization to protect sensitive information while still allowing for data analysis. This involves replacing sensitive data with fictional or obscured values to prevent unauthorized access.
7. Secure Data Storage: Utilize secure data storage solutions that comply with industry standards and regulations. This may include deploying firewalls, intrusion detection systems (IDS), and encryption protocols to protect data stored on servers, cloud platforms, and other storage devices.
8. Regular Security Audits: Conduct regular security audits and assessments to evaluate the effectiveness of security controls and identify any gaps or weaknesses. This includes penetration testing, vulnerability scanning, and compliance audits to ensure adherence to security policies and regulations.
9. Employee Training and Awareness: Provide training and awareness programs to educate employees about security best practices and the importance of safeguarding sensitive data. This includes training on password hygiene, phishing awareness, and proper handling of sensitive information.
10. Incident Response Plan: Develop a comprehensive incident response plan to quickly respond to and mitigate security incidents. This plan should outline procedures for detecting, reporting, and responding to security breaches, as well as protocols for notifying affected parties and regulatory authorities.
11. Compliance with Regulations: Ensure compliance with relevant data protection regulations and standards, such as the General Data Protection Regulation (GDPR) and the Family Educational Rights and Privacy Act (FERPA). This involves staying updated on regulatory requirements and implementing measures to address compliance obligations.
12. Continuous Improvement: Continuously monitor and improve security measures based on evolving threats and technology advancements. This includes staying informed about emerging security trends, adopting new security technologies, and revising security policies and procedures as needed.

By following this methodology, organizations can effectively secure big data generated in the education field and mitigate the risks associated with handling sensitive information.

5. CONCLUSION

Here the burgeoning volume of big data generated within the education sector presents a myriad of opportunities for enhancing teaching methodologies, student learning outcomes, and institutional management. However, alongside these benefits, the extensive collection, storage, and analysis of sensitive educational data also raise significant security concerns.

Our research has underscored several key security issues inherent in big data generated within the education field. These include data privacy breaches, unauthorized access, identity theft, and the potential misuse of personal information for commercial or malicious purposes. Moreover, the interconnected nature of educational systems further amplifies the risks, as data breaches in one institution can have far-reaching consequences across networks.

Addressing these security challenges requires a multifaceted approach involving stakeholders at various levels, including policymakers, educational institutions, technology providers, and regulatory bodies. Proactive measures such as robust data encryption, stringent access controls, regular security audits, and comprehensive staff training are essential to mitigate risks and safeguard sensitive information.

Furthermore, the development and implementation of clear data protection policies and compliance frameworks are imperative to ensure accountability and transparency in handling educational data. Collaboration among stakeholders is crucial to establish industry-wide standards and best practices that prioritize data security without compromising innovation and educational advancement.

As the education sector continues to embrace big data analytics to drive insights and improvements, it is imperative that security considerations remain at the forefront of technological advancements. By fostering a culture of vigilance, responsibility, and ethical data governance, we can harness the transformative potential of big data while safeguarding the privacy and security of individuals within the education ecosystem.

ACKNOWLEDGMENT

I am thankful to Yashavantrao Chavan Institute of Science, Satara (Autonomous) for provide the facility to do research work. I also thanks my Guide Prof. Dr Bhavana Narain, MSIT, MATS University, Raipur, CG and Co guide Dr. B. T. Jadhav for continuous support for make me possible my research work easily.

REFERENCES

[1] Big Data Generated In Iot, R.P. Waghamare1 , Dr. B.T. Jadhav2, Dr. Gitanjali Sinha3, March 2023| IJIRT | Volume 9 Issue 10 | ISSN: 2349-6002, IJIRT 158677 International Journal Of Innovative Research In Technology, PN 533-536.
[2] Big Data Analytics in Education: Big Challenges and Big Opportunities Bernard Veldkamp1, Kim Schildkamp2, Merel Keijsers3, Adrie Visscher4 and Ton de Jong Book Title: International Perspectives on School Settings, Education Policy and Digital Strategies: A Transatlantic Discourse in Education Research, 2021, pp. 266-282 (17 pages) Published by: Verlag Barbara Budrich. (2021) Stable URL: https://www.jstor.org/stable/j.ctv1gbrzf4.19
[3] (Bongers/Jager/Te Velde 2015)

 https://doi.org/10.5281/zenodo.14032437

[4] Big Data In Cloud Computing Review And Opportunities , Manoj Muniswamaiah, Tilak Agerwala and Charles Tappert Seidenberg School of CSIS, Pace University, White Plains, New York, International Journal of Computer Science & Information Technology (IJCSIT) Vol 11, No 4, August 2019
[5] Big Data Security Issues: A Review Syafik Azhar1 , Noor Hidayah Mohd Yunus1, Hasya Nabilah Mohd Yusof1, Nur Aliah Hussin1, Nurizzah Zafirah Norhisham1, & Aini Juhaida Zainuddin1, Journal of Engineering Technology Vol. 11: 9-17, 2023 ISSN 2231-8798© 2021 UniKLBMI, PN 9- 17.
[6] A Review on Big Data Analytics between Security and Privacy Issue Renas Rajab Asaad1 , Nisreen Luqman Abdulnabi2 1Department of Computer Science, Nawroz University, Duhok, Kurdistan Region - Iraq 2Technical Collage of Administration, Duhok Polytechnic University, KRG – Iraq, Academic Journal of Nawroz University (AJNU), Vol.11, No.3, 2022 This is an open access article distributed under the Creative Commons Attribution License Copyright ©2017. e-ISSN: 2520-789X https://doi.org/10.25007/ajnu.v11n3a1446, PN 178- 186.
[7] The usefulness of Big Data and IoT/AI at Dubai University , 1st Author: Dr Shankar Subramanian Iyer, DBA, Faculty, Westford University College, Al Tawuun, Sharjah, UAE, shankar.s@westford.org.uk, Orcid ID: 0000-0003-0598-9543.
[8] 2nd Author: Dr Benita. K. J. Veronica, Faculty, PhD, Westford University College, Al Tawuun, Sharjah, UAE, benita.c@westford.org.uk, ORCID No. 0000-0002-5501-7382.3rd Author: Dr Amit K. Singh, Faculty, Westford University College, Al Tawuun, Sharjah, UAE, amit.k@westford.org.uk, Orcid ID: 0009-0001-4938-4135.
[9] A Review Internet of Things (IoT) Security Challenges and Issues Dr. S. Thavamani1 , Ms. C. Nandhini2 , Mr. T. Pradeep3, International Journal of Research Publication and Reviews, Vol 4, no 5, pp 87-91 May 2023, ISSN 2582-7421, PN 87-91
[10] IoT and Big Data Security Issues and Challenges: A Technological Perspective, Swati Gupta, Meenu Vijarania, Anjali Gautam, Jyoti Goel, In book: Intelligent Engineering Applications and Applied Sciences for Sustainability, November 2023
[11] IoT with Big Data and Security Challenges of Present Era Maida Insha,Tanzeela Shaheen,Turrnam Shahzadi,Muskan Khan, August 2022, publication at: https://www.researchgate.net/publication/362412128
[12] Emerging Issues in Cyber Security for Institutions of Higher Education 1 Mayieka Jared Maranga; 2 Dr. Masese Nelson, IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 4, August 2019 ISSN (Online) : 2277-5420 www.IJCSN.org
[13] A Security and Privacy Framework for e-Learning, Radwan Ali, : https://digitalcommons.kennesaw.edu/facpubs

https://doi.org/10.5281/zenodo.14032437