UWI
ST. AUGUSTINE CAMPUS
TRINIDAD & TOBAGO, WEST INDIES

IN SERVICE TO THE COMMUNITY

LATT

Big Data Security and Privacy in Libraries:

Protecting Against Cyber Attacks.

PRESENTED BY:
Ray Ganessingh, Dihanne Saul and Delise Thomas

Librarians – The Alma Jordan Library, the University of the West Indies, Trinidad and Tobago, National Library of Georgetown, Guyana and Library Association of Trinidad and Tobago.

Cloud Security

Monitoring

Hadoop Security

Auditing

Key Management

De-Identifiers

AIM:
Place data storage on cloud

Strategies

- Validation, encryption and decryption
- Identity framework
- Establish identity based encryption alogorithm

AIM:
Hadoop security & privacy

Strategies

- Trust mechanisms with user / name node
- Use encryption on data

AIM:
HDFS security

Strategies

- **Kerberos mechanism** – introduce service ticket
- **Bull eye algorithm** - keeping an eye on sensitive information
- **Name node approach** – Enhance security to tackle data issues in safe way

AIM:
Security of group transfer

Strategies

- Group transfer keys is fundamental for high levels of security

AIM:
Group sharing security

Strategies

- Relocating proxy
- Levels of re-encryption framework

AIM:
- Maintain strong passwords
- Guarantee data centres

Strategies

- **Quantum cryptography** - ensure and transmit data and prevent hacking
- Authentication is secure and geared for next generation network
- Verifies identity of based encryption
- Dismisses unauthorized entry

AIM:
Unstructured data security

Strategies

- Data analysis (classification and filtering)
- Control security standards and algorithms

AIM:
Readiness of infrastructure to detect intrusion

Strategies

- Harmful metrics – detect potential risks
- How serious it is?
- Estimate the likelihood, an incident would have

AIM:
Verification of evolving data
(transfer data to less complex forms)

Strategies

- Implement merkle hush tree - ensure verification of stored data and managing movement between computers

AIM:
Handling sensitive fields

Strategies

- Deploy k-anonymity based metrics - intruder is kept out by strong defence system
- Prevention of obtaining identity from data sets

AIM:
Preservation of data mining

Strategies

- **Adaptive utility based anonymization model** – protection of data and modifies identifiable information

AIM:
Big data privacy & preservation

Strategies

- **Two step clustering algorithm** - steps of pre-clustering
- Each data is examined
- Handles mixed field types
- Efficient in working with large data sets

Key Takeaways

- Keep updated with antivirus and malware protection
- Isolation of devices and servers with critical data
- Establish a real time security policy and relevant event management
- Train library staff to handle and identify potential cyber attacks

References

Hooper, R. (2023). Big Data: What is it and how can academic libraries use it. *Alabama Libraries, 60*(2), 3. https://jagworks.southalabama.edu/alabamalibraries_journal/vol60/iss2/3

Meng, W., Giannetsos, T., & Jensen, C. D. (2022). Information and future internet security, trust and privacy. *Future Internet, 14*(12), 372 https://doi.org/10.3390/fi14120372

Sanap, G. R. (2023). Big Data and Libraries. *International Interdisciplinary Research Journal (AIIRJ).* http://aiirjournal.com/uploads/Articles/1679562388Final%20File%20117.pdf#page=81