E-Portfolio Link: <https://fombwori.github.io/myportfolio/index.html>

**Name:** Faith Ombwori

**Student ID**: 12693221

**University of Essex Online** – Colchester

**Programme:** MSc. Cyber Security

**Department:** Computing

**Module:** Research Methods and Professional Practice

**Submission:** Individual e-Portfolio including 1000 word reflective piece

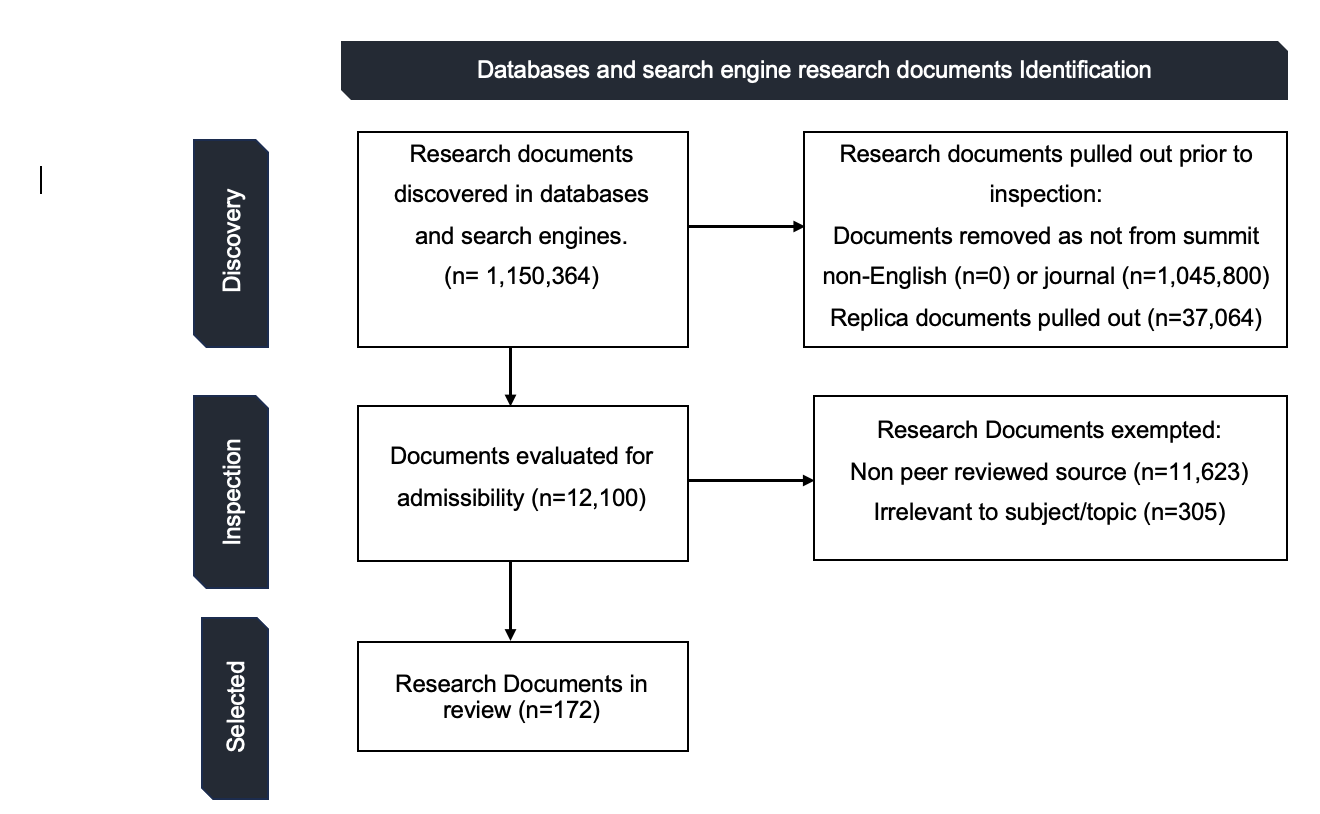
Research has numerous definitions with the most compelling being authentic analysis conducted in pursuit of substantive comprehension (RAE, 2008). Accuracy of one’s approach to delivering on their study delivers legitimacy on their subject of choice (Cryer, 2006). Thought process, is paramount as determined by topic under investigation and in my specific instance, inductive inference became appropriate in my literature review and presentation. Ethical principles (Finn et.al., 2023), of research informed both my submissions they include;

1. Respect – Consent and acknowledgement of all referenced material was sought in compliance to Global Data Protection Regulations.
2. Beneficence – No risk was posed to any party in the entirety of course submissions even as I gained from respective work.
3. Justice – adherence on equitable distribution of credits on participants work against my own analysis
4. Respect for law and public interest – highest standards of integrity, excellence and thoroughness was adhered to whilst complying to intellectual property rights to all, giving credit to all research material consulted.

Approach and methodology of application came naturally as the quantitative approach was more applicable in the topic of choice “cybersecurity threats in Internet of Things (IoT) enabled satellite networks”. Sample size extrapolated from IEEE Xplore, Google scholar and Scopus between 2011 to 2025. Years of range main determinant, was, technical significance to research topic, sector affected in this case defence and cybersecurity threat posed. In achieving my literature review’s goal, the following study questions were responded to;

1. Discovered key cybersecurity attacks on IoT enabled satellite networks
2. Found out vulnerabilities catalysing the above
3. Specified the risk mitigants to identified vulnerabilities
4. Listed the discovered highly at-risk sectors which were defence and law enforcement

The applied research approach and methodology is the Preffered Reporting Items for Systematic Reviews and Meta- Analysis (PRISMA), tabulated below;



In my literature review, I provided a summary of incorporation and debarment for reviewed literature as per table below;

|  |  |  |
| --- | --- | --- |
| **Summary of incorporated and debarment criteria for reviewed literature** | | |
| Evaluation guideline | Incorporation guideline | Debarment guideline |
| case | Peer reviewed | Non- peer reviewed |
| Subject area | Pertinent to IoT enabled satellite networks, relevant cybersecurity attacks, susceptibilities and possible solutions | Non-pertinent to IoT enabled satellite networks, relevant cybersecurity attacks, susceptibilities and possible solutions |
| Research strategy | Peer reviewed summit research documents, scientific indexed journals | Non-peer reviewed sources |
| Language | English | Other languages outside English |
| Publish date | 2011-2025 | Before 2011 |
| Geographical considerations | World wide | Too specific |

In my analysis, spoofing, satellite jamming, malware are the main cyberthreat vectors caused by risk of non-implementation of Open Worldwide Application Security Project-OWASP (Khan et.al. 2025), security framework. Vulnerabilities identified include; vulnerabilities of Commercial Off-the-Shelf (COTS), parts, non-encryption, internet of things common vulnerabilities, vulnerability assessments and penetration tests (VAPT).

**Risk Management**

The identified cybersecurity threat vectors and susceptibilities are to be mitigated through the following resolute measures;

* **Artificial Intelligence (AI), solutions** – Guided by the NIST framework through automation of routine processes (Kaur, e. al. 2023), to proactively hasten threat identification and response in threat posture enhancement. incorporation of AI in software development cycle, which incorporates security checks within workflows, static code analysis and resulting in early identity of threats, investigation and resolving of the same through release of security patches and software upgrades
* **Encryption by design** – In conjunction with the above, NIST, provides post quantum cryptography standards applicable in alleviation of risks posed by quantum computing. The algorithms presented include Crystal Kyber for protection of confidential TLS systems. Crystal Dithilium, Falcon and Sphincs (Sood, 2024), applied in validation of digital signatures.

Other mitigations to be applied include zero trust, block chain technology especially in defence and law enforcement sectors, access control paired with biometrics to mitigate the risk of multifactor authentication fatigue social engineering attacks in addition of embracing and implementing flexible policy management guided by ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection - Information security management systems Requirements.

Cybersecurity threats in IoT enabled satellite networks SWOT analysis is as per table below;

|  |  |  |  |
| --- | --- | --- | --- |
| **Strengths** | **Weaknesses** | **Opportunities** | **Threats** |
| Leveraging current set up –Satellite hardware set up are designed for a universal infrastructure that IoT leverages on for connectivity | Device Susceptibility- characterised by low computing power, IoT do not have internalised security features hence vulnerable to attacks | Modernisation of bock chain technology and zero trust, guarantees security and integrity in a wide area network | Intricacy of cyber-attacks especially targeting IoT enabled satellite networks due to interconnectedness capitalising on their supply chain vulnerabilities not to mention vulnerability to ransomware type of attacks. |
| World-wide coverage - satellite networks cover wider range geographically | lack of regularisation as there is poor compliance to governing standards and poor regulatory framework | Enhanced post quantum cryptography for the network and IoT devices | IoT are susceptible to Denial-of-service attacks especially after compromise |
|  | Vulnerable communication due to weak (or non-existent) encryption | incorporation of AI in software development cycle, which incorporates security checks within workflows, static code analysis and resulting in proactive threat identity | Poor encryption raises the risk of privacy violation during data breaches considering the large amount of data collected by IoT devices. There is also an aspect of eaves dropping |
|  | Remote physical deployment of IoT enabled satellites exposes them to network vulnerabilities for example bypassing weak security. | curbing lateral movement of cyber breaches through implementation of the zero trust | IoT enabled satellites are mainly used by defence sectors which deploy them on critical infrastructure. Consequently, the latter is at risk examples include airports, power grids, Banks, broadcasting e.t.c |
|  | low compute resource limitation that makes it extraneous enhancing requisite safety. | Security Framework - ISO/IEC 27001:2022 standard for Information security, cybersecurity and privacy protection - Information security management systems Requirements. |  |

In conclusion, I am challenged to approached cybersecurity discipline from a wider perspective applying specific use cases relevantly as this is my guide to applicable security governance and regulatory framework based on geo-location of respective jurisdiction. Additionally global standards like NIST, ISO/IEC and the GDPR are critical in deciding on foundational tenet of my research. Ethics and integrity come first in entirety of a research project.

**References**

1. ‌ Alasdair Gilchrist (2016). *Industry 4.0 The Industrial Internet of Things*. Berkeley, Ca Apress.
2. Bishop, M., 2007. About penetration testing. *IEEE Security & Privacy*, *5*(6), pp.84-87.
3. Beyrouti, M., Lounis, A., Lussier, B., Bouadallah, A. and Samhat, A.E., 2023, March. Vulnerability and threat assessment framework for internet of things systems. In *2023 6th Conference on Cloud and Internet of Things (CIoT)* (pp. 62-69). IEEE.
4. Czajkowski, M., 2021. Anti-Satellite Weapons: A Political Dimension. *Safety & Defense*, *1*, pp.107-116.
5. Crusan, J. and Galica, C., 2019. NASA's CubeSat Launch Initiative: Enabling broad access to space. *Acta Astronautica*, *157*, pp.51-60.
6. Cryer, P. (2006) The research student’s guide to success (3rd Edition), Open University Press, Maidenhead, UK
7. cybersecurity: Literature review and future research directions’, Information Fusion, 97(101804), pp. 1–29. Available at: <https://doi.org/10.1016/j.inffus.2023.101804>.
8. Dawson, C. (2015). Projects in Computing and Information Systems. 3rd Edition. [Insert Publisher Location]: Pearson International Content.
9. Ebad, S.A., 2022. Exploring how to apply secure software design principles. IEEE Access, 10, pp.128983-128993.
10. Finn, M. and Shilton, K. (2023) 'Ethics governance development: The case of the Menlo Report', Social Studies of Science, 53(3), pp. 315-340
11. Höyhtyä, M., Boumard, S., Yastrebova, A., Järvensivu, P., Kiviranta, M. and Anttonen, A., 2022. Sustainable satellite communications in the 6G era: A European view for multilayer systems and space safety. *IEEe Access*, *10*, pp.99973-100005.
12. Kathiresan, G., 2025. Trust-by-Design: embedding AI-Powered security checks into software quality workflows. Iosr Journals, 27(3).
13. Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023) ‘Artificial intelligence for
14. Khan, S.Z., Mohsin, M. and Iqbal, W., 2021. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science*, *7*, p.e507
15. Khan, S.A., Azim, N., Iqbal, A., Abbas, H. and Qureshi, S., 2025. Securing Web Applications: A Practical Approach to Mitigating OWASP Top 10 Vulnerabilities. *VFAST Transactions on Software Engineering*, *13*(2), pp.273-291.
16. Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. and Singh, S., 2022. A review on cyber crimes on the internet of things. *Deep learning for security and privacy preservation in IoT*, pp.83-98
17. Lalbakhsh, A., Pitcairn, A., Mandal, K., Alibakhshikenari, M., Esselle, K.P. and Reisenfeld, S., 2022. Darkening low-earth orbit satellite constellations: A review. *IEEE Access*, *10*, pp.24383-24394.
18. ‌ Li, Y., Li, H., Liu, W., Liu, L., Zhao, W., Chen, Y., Wu, J., Wu, Q., Liu, J., Lai, Z. and Qiu, H., 2023, July. A networking perspective on starlink's self-driving leo mega-constellation. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking* (pp. 1-16).
19. Lounis, K. and Zulkernine, M., 2020. Attacks and defenses in short-range wireless technologies for IoT. *IEEE Access*, *8*, pp.88892-88932.
20. Mayer, J., 2009. Policy space: what, for what, and where?. *Development Policy Review*, *27*(4), pp.373-395.
21. NAIR, R. (2023). *Mastering Information Security Compliance Management*. Packt Publishing Ltd.
22. Nguyen, H.P.D. and Nguyen, D.D., 2021. Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication. *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, pp.185-210.
23. Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E. and Chou, R., 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, *372*.‌
24. Pasdar, A., Koroniotis, N., Keshk, M., Moustafa, N. and Tari, Z., 2024. Cybersecurity solutions and techniques for internet of things integration in combat systems. *IEEE Transactions on Sustainable Computing*.
25. RAE (2008) Research assessment exercise, <http://www.rae.ac.uk/> (3 June 2014)
26. Rausch, H., 2006, April. Jamming commercial satellite communications during wartime an empirical study. In *Fourth IEEE International Workshop on Information Assurance (IWIA'06)* (pp. 8-pp). IEEE.
27. Rampini, G.H.S., Takia, H. and Berssaneti, F.T., 2019. Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. *Procedia Manufacturing*, *39*, pp.894-903.
28. Sood, N., 2024. Cryptography in post quantum computing era. Available at SSRN 4705470.
29. Sedhupathy, P., Shavkatov, N., Bostani, A., Srinivasan, A. and Mathew, C., 2025. Quantum-Resilient Antenna-Assisted Communication Protocols for Satellite-Based Secure IoT Networks. *National Journal of Antennas and Propagation*, *7*(1), pp.262-269.
30. Stojnic, T., Kayes, A.S.M., Rahayu, W. and Chowdhury, M.J.M. (2025). A comprehensive literature review of cyber threats and vulnerabilities in IoT-driven satellite networks: Research challenges and future directions. *Computer Networks*, [online] 272, p.111678. ‌
31. Schuckers, S.A., 2002. Spoofing and anti-spoofing measures. *Information Security technical report*, *7*(4), pp.56-62.
32. Team, I.G.P., 2020. *EU general data protection regulation (gdpr)–an implementation and compliance guide*. IT Governance Ltd.
33. *Weerackody, V., 2021, June. Satellite diversity to mitigate jamming in LEO satellite mega-constellations. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE.*
34. Yahuza, M., Idris, M.Y.I., Ahmedy, I.B., Wahab, A.W.A., Nandy, T., Noor, N.M. and Bala, A., 2021. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access*, *9*, pp.57243-57270.