Name: Faith Ombwori

Student ID: 12693221

University of Essex Online – Colchester

Programme: MSc. Cyber Security

Department: Computing

Module: Research Methods and Professional Practice

Submission: Literature Review

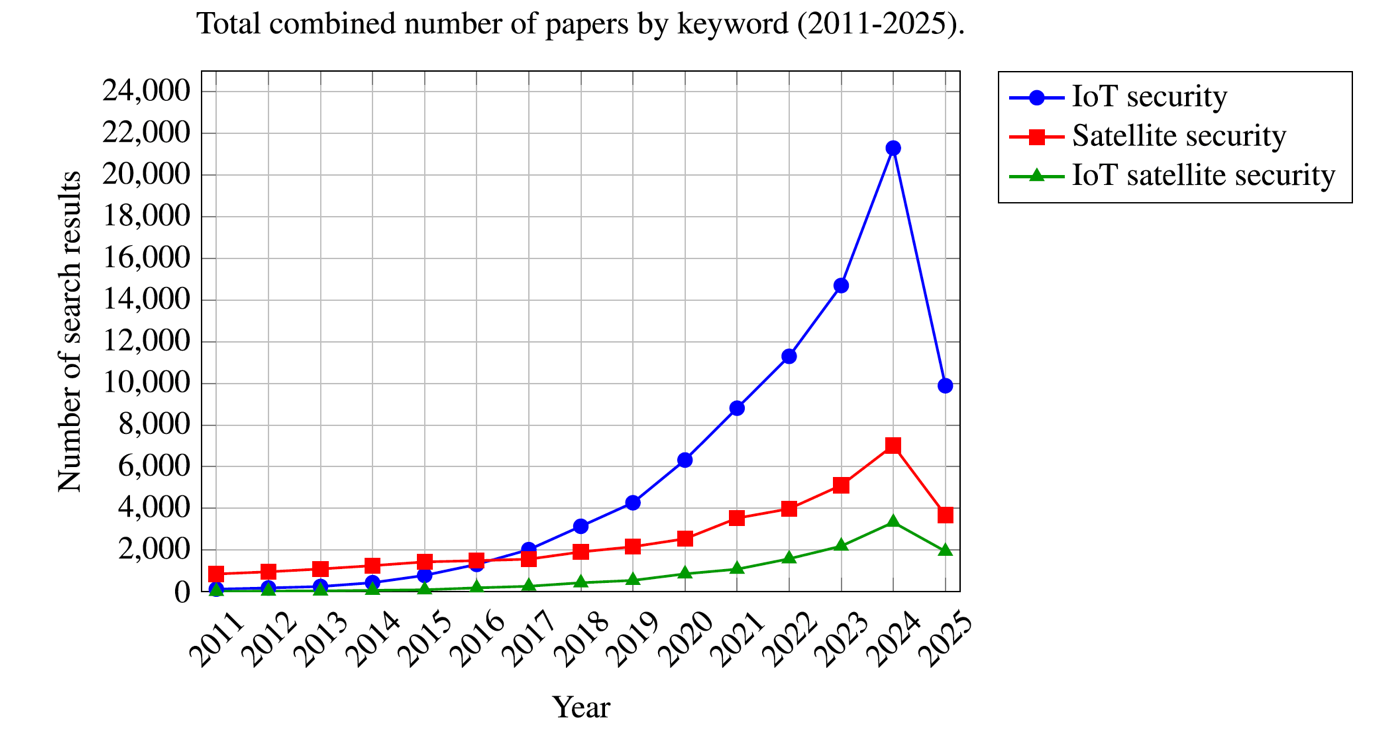
**Introduction**

This literature review focuses on cybersecurity threats in Internet of Things (IoT) enabled satellite networks. IoT, accelerated the realisation of industry 4.0 revolution (A. Gilchrist, 2016), catalysed connectivity in the form of intelligent and super-efficient cyber physical systems. The latter brings about criticality of data security (Nair, 2023) and privacy (I.T.G., 2020) in IoT technologies.

The Satellite networks enabled by IoT, suffer numerous susceptibilities exposing them to common cyberattacks including but not limited to malware, commercial off the shelf (COTS), denial of Service (DoS), jamming and spoofing. Additionally, threat vectors explored in IoT enabled satellite networks are access control, poor and or lack of encryption including commercial off the shelf (COTS), part vulnerabilities.

Applying the preferred reporting items for systematic literature reviews and meta-analysis (PRISMA) methodology (Page et. al. 2020), consideration has been taken to allow for structured review of appropriate sources through relevant research databases[[1]](#footnote-1). In this submission exploration of the IoT powered Satellite network vulnerabilities and threat vectors is based on recent technical papers and existing literature, despite limitation in statistical documentation addressing the same. This paper proposes the need for further research on subject matter in contributing to the designing of a cybersecurity framework to mitigate IoT driven satellite network vulnerabilities and subsequent cyber-attacks.

Commercialisation of satellite technology has taken prevalence with conglomerates like Space X, taking centre stage in provision of high-speed broadband internet connectivity services through Starlink. Statistically, there were over 500 Starlink satellites as at August 2023, (Li. et.al 2023), with a set target of reaching 42,000 in Low Earth Orbit (LEO) (Lalbakhsh et.al 2022). This industry providing high speed internet, used by national defence and GPS navigation systems, has experienced an exponentially rapid growth rate. The latter, provides justification to prioritise satellite networks security against cyber-attacks as it generates a record $366 billion (three hundred and sixty-six billion dollars) as per 2019 - 2020 Satellite Industry Association report (Czajkowski, 2021).



Source: (Stojnic. et.al.2025)

Figure 1. colour coded key depicting respective search terms well defined in different colour. The table gives summation of IoT satellite security papers by year in Scopus, IEEE Xplore, and Google scholar (2011-2025)

Figure one above, shows the totality of peer reviewed documents from searched databases with topic “IoT enabled satellite security” in contrast with “satellite Security” and “IoT security”. The past decade, saw search frequency for “IoT satellite security” has increased as “IoT security” quests remain common. It is noteworthy, that in the last half a decade, investigative papers on subject matter topics/texts, increased as follows; 2016 – 184, 2024 – 3330 and 2025 to date – 1940.

Comparatively, lack of IoT satellite networks and an over emphasis on IoT security and or Satellite topics, as stand-alone perspectives, with commensurate results on enhancing security on the same, that also, focus mainly on satellite technology topology, is evidence of a lacuna in available studies and assessments. Results presented by the surveys, focused on security improvement.

**Review structure**

* Review Methodology
* Outline of IoT enabled satellite networks
* IoT enabled satellite networks cybersecurity threat vectors and vulnerabilities
* Evolving and current methods to mitigate security risks in the these IoT aided satellite networks,
* Research limitations in subject matter i.e. cybersecurity threats in Internet of Things, enabled satellite networks
* Future research projections to mitigate IoT-Satellite network cyber threat risks

**Review Methodology**

Applying quantitative approach, research questions were developed as per figure 2, below to achieve main objectives of this paper i.e.

1. Find main kind of cyber-attacks on IoT enabled satellite networks,
2. Discover susceptibilities enabling the above
3. Provide propositions to mitigate identified susceptibilities as per above
4. Discover most exposed industries/sectors to identified cyber-attacks with possible pragmatic solutions.

Sample size was selected and retrieved from Scopus, IEEE Xplore, and Google scholar between 2011-2025. Selection range was informed by technical relevance to subject matter, sector of application and of course with key consideration to type of cybersecurity threat posed.

Figure 2 Review Methodology Research Questions

Research Documents exempted:

Non peer reviewed source (n=11,623)

Irrelevant to subject/topic (n=305)

Databases and search engine research documents Identification

Research documents pulled out prior to inspection:

Documents removed as not from summit non-English (n=0) or journal (n=1,045,800)

Replica documents pulled out (n=37,064)

Research Documents in review (n=172)

Documents evaluated for admissibility (n=12,100)

Research documents discovered in databases and search engines. (n= 1,150,364)

Selected

Inspection

Discovery

Figure 3 PRISMA Work flow diagram listing research document incorporation and debarring protocol and number of research studies in review

Table 1 Summary of incorporation and debarment for literature reviewed

|  |  |  |
| --- | --- | --- |
| **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 |

**Outline of IoT enabled satellite networks**

In the advent of cyberwarfare, defence sector invested heavily in intelligence, Global Positioning System (GPS) to bolster artificial intelligence-based weaponry including drones that are part of IoT. The later exudes the security role played at national level by IoT enabled satellite networks (Pasdar et.al. 2024). Long-range and short-range wave transmission across remote areas is made possible through IoT enabled satellite networks. Role of short and long-range waves in IoT enabled satellite networks, introduces unique vulnerabilities and an increased attack surface, that have long been ignored by researchers, unlike the commonly studied and researched short-range IoT wireless network technologies (Lounis, et.al. 2020)

IoT enabled satellite networks are formulated by large constellations at various altitudes and connections to a myriad of IoT devices as they are manufactured with scalability at the core.

**IoT enabled satellite networks cybersecurity threat vectors and Susceptibilities**

* **Spoofing:** attackers target authentication faults creating parallel access inlet gaining network access whilst purporting to be a genuine user. In the process network packets interception provide requisite data facilitating impersonation actual user(s), and sharing of disguised malicious traffic (Schuckers, 2002). This type of attack is seen in prevarication of GPS data (GPS spoofing), (Khan, et.al. 2021). To ensure smooth data flow, drones were produced without encrypted serial ports exposing them to spoofing distorting their flight path (Nguyen,et.al. 2021).
* **Satellite jamming:** This simply a deployment of a denial-of-service attack on the network through emission of radio wave at same frequency as satellite signal confusing the transponder on the genuine wave (Rausch, 2006). LEO networks commonly suffer such attacks too (*Weerackody, 2021).*
* **Malware:** This occurs through download of malicious software on unsecured networks creating threat vectors for denial of service and exfiltration. In this research study, this specific type of attack was not prevalent. Though, attackers commonly target unmanned aerial vehicles with keylogger type of malware (Yahuza,2021).

OWASP (Khan, et.al.2025), security framework remains unenforced as concentration remain on IoT devices and not IoT enabled satellite networks. Also, through this literature review it has become apparent that lack of security policies and standards focusing on lowering of vulnerabilities

**IoT Satellite Networks Susceptibilities**

* **Susceptibilities COTS parts:** unregulated over commercialised satellite market, with complicated supply chain creating a quality assurance risk (especially on quality of hardware used to produce the satellites) and threat vector, has made satellites readily available and affordable to cyber criminals that purchase, dismantle and study them and understand how to create backdoors and exploits. Examples used are CubeSats built using COTS parts (Crusan, 2019). Use of open source software is also a major vulnerability exploited by cyber attackers
* **Poor encryption vulnerability:** this remains the leading cause of cyber-attacks in IoT enabled satellite networks prevalent in the form of spoofing, man in the middle attack as secure by design is not a policy embraced by the satellite communication manufacturers. In keeping production costs low, manufacturers avoid implementation of strong encryption to avoid computational increased expenses consequently. On this front we recommend strengthening of encryption and applying the latest protocols i.e. lattice-based: kyber -1024 (Sedhupathy, 2025).
* **Common IoT device vulnerabilities:** according to this literature review it is evident that there are shared vulnerabilities between IoT devices, cyber-physical systems and IoT enabled satellite networks due to sharing of wireless communications and cloud overdependence.
* **Poor policy standards and governance vulnerabilities:** critically low levels of IoT enabled satellite network cybersecurity awareness (Kagita,2022), lack of proper governance structures targeting these networks and if at all any, enforcement and compliance remain poor, lack of satellite supply chain regulatory framework and poor-quality assurance compromising on quality of hardware released on to the market full of vulnerabilities exposing end users to high-risk threat vectors ready for exploitation. Though various jurisdictions have developed robust legal and policy frameworks regulating their cyberspace and critical infrastructure, more needs to be done pertaining to protection of space cybersecurity policies more so in developing countries even if it their space technology is yet to be developed. This is because Space market conglomerates are taking advantage and exploiting them since space governance is only for big players (Mayer, 2009).
* **Vulnerability Assessment and Penetration testing (VAPT):** this exercise is conducted to exploit present vulnerabilities (Bishop,2007) however a risk assessment is required to identify the vulnerabilities. To date, there are no set VAPT protocols for IoT enabled satellite networks and this is a critical area for further research.

Numerous propositions have been listed on best way to mitigate identified vulnerabilities above including but not limited to AI-based resolutions, encryption by design, zero trust, blockchain technology, robust access control through identity-based authentication, embracing software defined networks, tunnelling and cryptographic key controlling, flexible policy management. Use of IoT enabled satellite networks by defence and national security raises the critical need for compliance to the principle of confidentiality, integrity and privacy (CIA Triad) which must be embedded to governance policy.

**Research limitations in subject matter i.e. cybersecurity threats in Internet of Things, enabled satellite networks**

Critical limitation is lack of governance and standardised regulatory framework (Höyhtyä, et.al. 2022), in developing countries who comprise of the biggest consumer market of IoT enabled satellite network market serviced by large manufacturers based in USA e.g. Star Link.

Security measures remain unenforced (Beyrouti, et.al. 2023), since available frameworks are IoT device and legacy network centric and silent on IoT enabled Satellite networks

Theres a clear lack of change management especially in the migration to newer technologies like block chain and zero trust. Risk management standards (Rampini, et.al. 2019) need to be applied across the entire supply chain and governance of IoT enabled satellite network industry.

**Summary**

**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. 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.
7. 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
8. 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.
9. 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
10. 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.
11. ‌ 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).
12. Lounis, K. and Zulkernine, M., 2020. Attacks and defenses in short-range wireless technologies for IoT. *IEEE Access*, *8*, pp.88892-88932.
13. Mayer, J., 2009. Policy space: what, for what, and where?. *Development Policy Review*, *27*(4), pp.373-395.
14. NAIR, R. (2023). *Mastering Information Security Compliance Management*. Packt Publishing Ltd.
15. 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.
16. 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*.‌
17. 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*.
18. 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.
19. 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.
20. 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.
21. 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. ‌
22. Schuckers, S.A., 2002. Spoofing and anti-spoofing measures. *Information Security technical report*, *7*(4), pp.56-62.
23. Team, I.G.P., 2020. *EU general data protection regulation (gdpr)–an implementation and compliance guide*. IT Governance Ltd.
24. *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.*
25. 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.

1. <https://www.sciencedirect.com> [↑](#footnote-ref-1)