International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2410227

Leveraging IoT for Enhanced National Security : A Comprehensive Review

Dr. K. V. Rukmani, Lt. Dr. D. Antony Arul Raj, Ms. Shobana N D, Ms. Sandhiya Sivanandan

Department of Software Systems, PSG College of Arts & Science, Coimbatore, Tamil Nadu, India

ARTICLEINFO

Article History:

Accepted: 15 March 2024

Published: 30 March 2024

Publication Issue

Volume 10, Issue 2

March-April-2024

Page Number

334-342

ABSTRACT

In an era marked by rapid technological advancement and evolving security threats, the integration of Internet of Things (IoT) technologies has emerged as a pivotal strategy for bolstering national security efforts. The integration of Internet of Things (IoT) technologies into national security frameworks offers unprecedented opportunities for enhancing situational awareness, proactive threat detection, and effective response mechanisms. By deploying IoT devices such as sensors, cameras, and drones across various sectors including border control, critical infrastructure protection, and emergency management, governments can achieve real-time monitoring and data-driven decision-making capabilities. This paper gives a comprehensive review of the use of IoT technologies in national security, including real-time surveillance, border control and critical infrastructure protection. It examines the challenges and propose strategies, including the development of robust regulatory frameworks.

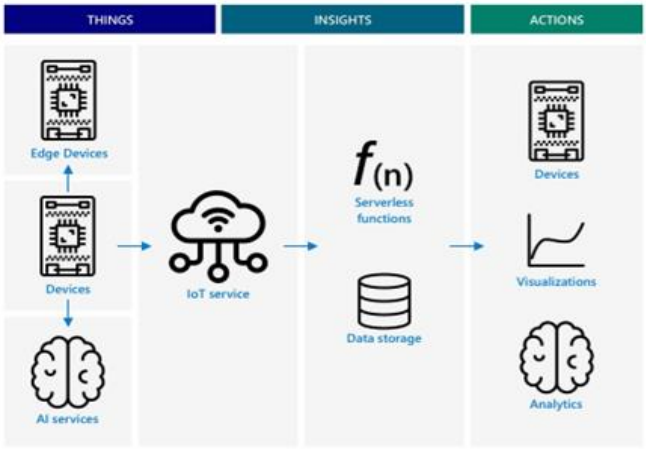
Keywords : Internet of Things (IoT), Security, Monitoring, Strategies, Decision Making, Defense

I. INTRODUCTION

IoT devices can include mechanical and digital machines, consumer objects and animals or society. IoT devices are typically rooted with technology such as sensors, software and other technologies. IoT for defence and National Security cover's themes on IoT security, automations, detecting, strategies, operations, and more, together with the up-to-date results from the foremost IoT research inventiveness of the U.S.

The Internet of Things (IoT) represents a transformative paradigm where interconnected devices autonomously collect and exchange data, shaping a hyper-connected world. At its core, IoT relies on sensors embedded in everyday objects, which communicate over networks to enable data-driven insights and actions. This intricate web of devices spans from personal gadgets like smartwatches and thermostats to industrial machinery and urban infrastructure, offering unprecedented opportunities for innovation. Leveraging cloud computing for data processing and analytics, IoT solutions empower

industries to optimize operations, enhance decision-making, and deliver personalized experiences.



This intricate web of devices spans from personal gadgets like smartwatches and thermostats to industrial machinery and urban infrastructure, offering unprecedented opportunities for innovation. Leveraging cloud computing for data processing and analytics, IoT solutions empower industries to optimize operations, enhance decision-making, and deliver personalized experiences. However, with its immense potential comes a host of challenges, including cybersecurity threats, interoperability issues, and privacy concerns. As IoT continues to evolve, addressing these complexities will be crucial to unlock its full potential and ensure a seamless integration into our lives and businesses.

II. BACKGROUND AND CONTEXT

The Paper gives a thorough examination of privacy and security issues with IoT systems, particularly in the military and national defence sectors. Subjects covered span from general talks on IoT security and privacy issues to specific frameworks designed for assessing security in military IoT devices. The application and ramifications of Internet of Things-based border security and surveillance systems are also highlighted. The analysis of particular vulnerabilities to ICT systems for national security that depend on IoT technology is noteworthy. In addition, the impact of emerging technologies on national security is examined, and the use of IoT in military settings is discussed. Comprehensive research on IoT security concerns and defence strategies are also included in the literature; these studies offer insights into current trends, difficulties, and future solutions in the field of IoT security and defence.

III.SCOPE AND FOCUS

The integration of Internet of Things (IoT) technologies in military and national defence systems presents unique security and privacy challenges that demand careful consideration. The growth of IoT devices in military infrastructures generates serious issues about protecting sensitive data, vital operations, and interests in national security. Assessment frameworks built for military IoT devices are essential for identifying and reducing security concerns, but they need to be updated periodically to reflect new threats. Likewise, IoT-based border security and surveillance systems provide greater surveillance and reaction capabilities, but their implementation raises questions around data privacy and unauthorized access. In light of the swift advancement of IoT technologies, it is crucial to scrutinize new developments and their consequences for national security. Additionally, it is necessary to fill in the gaps in the current body of literature in order to create resilient defences against ever-changing threats.

IV. METHODOLOGY

A methodical approach was used in the selection, analysis, and synthesis of pertinent literature as part of the methodology used for this literature review. Selection criteria were first set in order to guarantee that publications pertaining to national defence, military applications, and IoT security would be included while research that were deemed irrelevant would be excluded. Following that, thorough searches were carried out utilizing relevant keywords on

academic databases. Following the selection of articles that satisfied the predetermined standards, pertinent information was extracted, including security issues, assessment frameworks, and upcoming technologies. The purpose of the analysis and synthesis of this data was to find themes, patterns, and gaps in the literature. Ultimately, a discussion of the results was held in order to formulate conclusions and offer suggestions for further study and application.

V. LITERATURE REVIEW

In [1] Carsten Maple says that, the concept of connecting 'things' to the internet dates back to the early 1980s when Carnegie Melon University students fitted photosensors to a vending machine, enabling internet access to determine dispensed and remaining drinks. The number of internet-connected devices is rapidly increasing, with analysts predicting 50 billion by 2020. However, these estimates are difficult to confirm due to inconsistent data and varying interpretations of IoT, and the difference between M2M and IoT devices.M2M communication, a term used in fleet management and SCADA solutions, has a long history. It involves direct communication between devices without human intervention, over any channel, wired or wireless. Key technologies include Wi-Fi, RFID, DSRC, Bluetooth, Bluetooth Low Energy, NFC, and Zigbee. The Fourth Industrial Revolution is expected to transform the global IoT landscape, integrating cyber physical systems, automated robotics, big data analytics, and cloud computing for smarter, flexible, and lean manufacturing. IoT technologies improve logistics efficiency, automation, and automation, while RFID technology forecasts and aids in early remedial measures, enhancing asset utilization and predictive maintenance. IoT devices with low power and area processors struggle with processing information due to limited CPU, memory, and energy budget. Access control in IoT is crucial for communication between entities. Models include DAC, RBAC, and ABAC. However, scalable, manageable, and efficient mechanisms are needed. In conclusion, the Internet of Things (IoT) has the potential to revolutionize our lives and work, but challenges remain in design, implementation, and management, despite guidance from various organizations on security.

In [2] Sungyong Cha.et.al says, the Internet of Things (IoT) has revolutionized military weapon systems, but it has also increased cyberattacks, targeting military domains and even distant networks. To combat this, research using security by design concepts, such as the High-Assurance Cyber Military Systems project, is being conducted. They have proposed a new security evaluation framework that integrates RMF and Cybersecurity Test & Evaluation in the existing weapons import process with international cybersecurity standards, aiming to improve cybersecurity through detailed illustrations and italicized alphabets. The proposed framework for weapon system purchasing uses an inertial navigation system (INS) built in an unmanned aerial vehicle (UAV). The INS uses a computer, motion sensors, and magnetic sensors to calculate the position, orientation, and velocity of a moving object without external references. The INS is crucial for computing data from UAV sensors, ensuring security. A formal evaluation would be difficult due to confidentiality issues. In conclusion, the authors propose a security-enhanced framework for weapon system import, integrating international standards and facilitating communication between acquirer and provider, despite potential challenges for some nations. In conclusion, the authors propose a security-enhanced framework based on the Risk Management Framework and Cybersecurity Test & Evaluation, designed to be integrated into the import process of weapon systems. This framework ensures cybersecurity throughout the lifecycle of weapon systems, from development to operation. The framework is reinforced with reference

to NIST documents but does not recommend an evaluation methodology.

In [3] Siham Boukhalfa and Abdelmalek Amine says that, Security along the global border is a life-threatening process in security assessment. It must be exercised 24-7. With the progressions in wireless IoT technology, it has become much easier to design, develop, and deploy a cost-effective, automatic, and efficient system for intrusion detection in the setting of surveillance. The novelists propose a border surveillance system. The surveillance and security system is to sense and track intruders intruding into the monitoring area along the border which triggers warnings and estimate essential for the clasp of efficient measurements in case of a hazard. The security of borders plays a key role in the assertion of national security, organization of legal immigration, prevention of smuggling, and defense against hostile threats. Certainly, borders remain the most visible mark of a state's sovereignty over a territory, and their management of its contribution in shielding its publics from threats it defines in seclusion: smuggling, crime, irregular migration, and multifaceted trafficking. In Conclusion, the algorithm is inspired of work of researcher's biologists who discovered the links of communication between the Cockroaches and their behaviour. Acquired results are satisfactory and prove that algorithm is able of guaranteeing surveillance of borders. It gives better results in comparison with other algorithms existing in literature (k-means, tree of decision, C4.5), Validated by the measurements of valuation (recall, precision, Fr - Measure, entropy, rate of success, rate of error) We studied the impact of every parameter for the quality of performance of every algorithm to identify ideal.

In [4] Jin-Seok Yang.et.al says, they sketched original security threats on IoT based up-to-date battlefield (Network centric battlefield). DoD is converging its consideration on the growth of unmanned combat systems to formulate for future conflict. The defence ministry plans to use IoT (Internet of Things) to build an intelligent combat system, ensuring security vulnerabilities for each component. The Department of defence plans to transition to operations readiness based on IoT, which enables communication between humans and devices connected to the internet. This technology can enable real-time sharing of information between allies and enemies, and can be applied to various fields of national defence, including surveillance, reconnaissance, and logistics supply. However, IoT can pose security threats such as illegal remote control, information leakage, false information inserts and signal disturbance in modern battlefields. Information leakage involves stealing network information through sniffing or ARP spoofing attacks, allowing faster deployment of military operations. False information inserts delay friendly operations or cause confusion. Signal disturbance paralyses communication, making it difficult to obtain enemy information. These threats are particularly significant in the modern battlefield, especially when utilizing IoT technology. In Conclusion, the application of IoT in modern warfare presents new security threats in network-centric battlefields. These threats include remote control, information leakage, false information insert, and signal disturbance. Future analysis will focus on identifying and addressing these threats, with a potential to propose countermeasures. IoT is crucial in various fields of national defence.

In [5] A. Ahanger and A. Aljumah says, the Internet of Things (IoT) is a rapidly evolving trend in web-based information architecture, revolutionizing various sectors like healthcare, resource management, and knowledge processing. However, it faces numerous security and privacy challenges. They have analysed these issues using empirical research, revealing that security threats are a growing concern for IoT networks, emphasizing the need to mitigate them for its success. IoT is utilized in various applications such as domestic monitoring, healthcare, and agriculture, forming the foundation for smart objects and devices. Its application in smart living has the potential to

significantly improve the quality of life. Cyber-attacks on IoT applications include sinkhole, wormhole, selective forwarding, and sybil attacks. These can cause traffic disruption, encryption issues, packet losses, and false information, especially in embedded sensors. They can also increase traffic load and privacy loss. The IoT sector faces security threats including confidentiality breaches, data integrity issues, denial of service attacks, and authentication breaches, compromising user privacy and network access. In conclusion, it highlights security threats in the IoT environment and presents existing solutions, but the researcher believes these are insufficient for high-level security requirements. The researcher believes existing solutions need improvement due to increasing attacker potential and IoT popularity risks.

In [6] Jin-Seok Yang.et.al says about the new security threats on IoT-based modern battlefields, focusing on the development of unmanned combat systems. The technology integrates multiple components, causing new vulnerabilities such as illegal remote control, information leakage, false information inserts, and signal disturbance. The Internet of Things (IoT) connects embedded devices with electronics, software, and sensors, connecting machines, humans, and objects. With over 10 billion connected devices, the number is expected to grow by 50% by 2020, introducing new security vulnerabilities like phishing and hacking. The Department of defence (DoD) plans to transition to operations readiness based on IoT, which enables communication between humans and connected devices. This technology can enable real-time sharing of information between allies and enemies, and can be applied to various fields of national defence, including surveillance, reconnaissance, and logistics supply. However, IoT can pose security threats such as illegal remote control, information leakage, false information inserts, and signal disturbance in modern battlefields. This could lead to the degradation of enemy combat power and potential attacks on allies. In conclusion, the application of IoT in modern warfare presents new security threats in network-centric battlefields, including remote control, information leakage, false information, and signal disturbance, particularly in areas like surveillance, reconnaissance, and logistics supply.

In [7] Petrisor Patrascu says that, emerging technologies, such as IoT, are increasingly important in various sectors, including national security. However, implementing these technologies in sensitive areas is a challenge due to their inaccuracy in measuring maturity. Despite uncertainty, they present both opportunities and potential threats. New digital technologies like artificial intelligence, the Internet of Things, Big Data, Cloud Computing, blockchain, quantum computing, 5G, robotics, drones, and 3D printing meet daily needs of people and society. Critical infrastructure, essential for national security, is protected by each state. The EU approach identifies and designs these infrastructures in two directions: common for energy and transport sectors, and individual for national sectors like health, financial-banking, food, agriculture, and administration. Emerging technologies streamline functionality and protect against physical and cyber threats in critical infrastructure. Emerging technologies in defence are questionable due to concerns about vulnerabilities and risks. Manufacturers' interest in developing these technologies is increasing, but decision-makers and military experts remain cautious. IoT solutions offer benefits to military activities, both during peacetime and warfare. However, they also pose risks and vulnerabilities in the defence sector. Cyber attackers, supported by both state and non-state actors, can disable services and steal data. Therefore, cybersecurity measures are crucial to ensure the confidentiality, availability, and integrity of IoT technologies. In conclusion, emerging technologies impact critical infrastructure and defence, offering automation and optimization but also posing national security threats. Interoperability and military system architecture are crucial for IoT security, preventing cyber-attacks.

In [8] Vlada S. Sokolovic and Goran B. Markovic says that, IoT enhances efficiency and effectiveness in various business and decision-making processes by collecting and distributing data between devices and servers, improving energy monitoring, supply chain coordination, production coordination, equipment performance optimization, transportation, public health, and infrastructure monitoring. The research and development of Internet Of Battlefield Things (IoBT) technology has focused on improving military capabilities by ensuring the protection of confidential data. Blockchain technology enables secure data exchange and processing, allowing for decentralization without a trusted authority. Hybrid blockchain platforms have been developed, combining public and private blockchains in a project, allowing access to public data and limiting access to protected data. Deep neural networks are being researched for designing sensitive and safety-critical decisions. They require embedded intelligence to detect and predict enemy behaviour, respond to threats, adapt to changes, recover from attacks, and support continuous learning. IoBT is being applied in military logistics to unify functional areas such as supply, maintenance, traffic, transport, and healthcare. The network organization in the logistics system monitors individual logistics functions, ensuring data collection, analysis, and generation. IoBT also plays a crucial role in asset logistics, enabling end users to initiate actions to preserve operational capabilities or mass service for assets. In conclusion, the military is utilizing IoT technology to improve combat effectiveness and resource management, utilizing actuators and autonomous platforms for cyber interfaces. The current data transmission architecture is inadequate for data collection and processing, leading to the use of IoBT in modern defence applications. Research focuses on 6G networks for data transfer, and C2 intelligent systems for quick reconfiguration.

In [9] Paula Fraga-Lamas.et.al says that, The Internet of Things (IoT) is revolutionizing communication and organization in organizations, particularly in defence and public safety. It offers benefits similar to industry, such as increased survivability, cost reduction, and operational efficiency. The survey examines existing IoT systems, challenges, and research roadmaps for enabling affordable IoT in defence and public safety. The Internet of Things (IoT) is a distributed system that uses data to create value and improve efficiency, productivity, and profitability in the commercial sector. It transforms product development, distribution, and infrastructure management, redefining interactions between people and machines. The rapid growth of IoT is driven by four key advances: declining costs of microelectronics, rapid wireless connectivity expansion, expansion of data storage and processing capacity, and innovative software applications and analytics. These drivers are present in the IoT technology stack, enabling fault detection, control, prediction, monitoring, and optimization. Communication capabilities are crucial in challenging environments with degraded infrastructures and unplanned events like catastrophes. Large-scale natural disasters involve multiple PS organizations, and commercial communication infrastructure must be functional. Cultural differences, intellectual property, and export restrictions discourage collaboration between defence and private sector innovators. Creating affordable, high-value systems with enhanced situational awareness for the military is a proven business value, and integrating commercial IoT data with this intelligence is a compelling business model for innovative contractors and system integrators. In Conclusion, this article explores the potential of commercial IoT transformation in the defence industry, focusing on scenarios such as C4ISR, fire-control systems, logistics, smart cities operations, personal sensing, soldier healthcare, and surveillance. It also assesses the added value and risk of applying IoT technologies in these scenarios. However, commercial IoT still faces challenges such as standardization,

scalability, interoperability, and security. Defence/PS IoT and COTS IoT differ in complexity, resource constraints, and centralized cloud-based architectures.

In [10] Abdullah Alabdulatif.et.al says that, The Internet of Things (IoT) has revolutionized various aspects of life, but it has also led to a rise in cybercrimes. These attacks have not only damaged the quality of life but also pose a significant risk to human safety. A comprehensive review of over 200 articles on IoT security is crucial. This review covers technical aspects, industrial development trends, revolutionary paradigms, and updated security. It also addresses key challenges in blockchain technology, distributed denial of service attacks, electoral vote security, and forensic issues. This review aims to provide insights into possible solutions to IoT's security challenges, gaps, opportunities, foresight, and recommendations, addressing the significant divide in its adoption and actualization across various human endeavours. It has infiltrated every sphere of human life, creating new paradigms like IoFT, IoE, IoNT, IoMT, IoMCT, and IIoT. It has revamped sectors like communications, smart cities, agriculture, industry, environmental pollution monitoring, surveillance, and disaster management. The Internet of Things (IoT) is a network of interconnected devices that communicate over network systems, transforming various sectors such as communications, agriculture, and industry. Addressing pliability is a critical IoT issue that needs to be addressed. The IoT is not functioning well for Industry 4.0 due to unresolved security challenges. The US Senate introduced the IoT cybersecurity enhancement act 2017 to improve security, requiring government-procured IoT products to meet minimum security standards. Vendors must ensure IoT devices are authenticated, certified, and secure. However, this legislation could add to existing security risks due to increased connectivity among people, organizations, and governments. In Conclusion, The Internet of Things (IoT) is a revolutionary technology that has transformed various aspects of life, including smart health, homes, and cities. However, security is a critical factor in its widespread adoption, particularly at the device.

VI. FINDINGS

- The impact of the Internet of Things (IoT) is remarkable in a number of domains, such as commercial processes, military operations, and national security.
- Wi-Fi, Bluetooth, RFID, and Zigbee are some of the key technologies used in Internet of Things connectivity.
- IoT can transform sectors including manufacturing, logistics, and defence by improving productivity, automating tasks, and facilitating decision-making.
- However, IoT also come with drawbacks, like restricted processing power, problems with access control, and scalability limitations.
- Data breaches, privacy violations, and cyberattacks aimed at vital infrastructure are some of the security risks that exist in IoT contexts.
- It is determined that current security measures are insufficient, hence strong frameworks and solutions must be developed in order to reduce threats.
- IoT is used in national security for protection of key infrastructure, intrusion detection, and border surveillance.
- With the use of technology like unmanned combat systems and the Internet of Battlefield Things (IoBT), IoT improves asset monitoring, logistics management, and combat effectiveness in military operations.
- To solve cybersecurity issues in IoT applications, notably in weapon system imports and contemporary battlefields, authors suggest security-enhanced frameworks and systems.
- The potential of IoT in national security and military are predicted to be further enhanced by emerging technologies like blockchain, artificial intelligence, and 6G networks.

Overall, IoT presents enormous possibilities for innovation and efficiency advantages in a number of industries, but in order to take full advantage of this potential and protect against possible threats, security concerns must be addressed and strong frameworks must be established.

VII. CONCLUSION

The paper explores the complex environment of the Internet of Things (IoT) across several industries, highlighting both its opportunities for innovation and its drawbacks. IoT has changed industries from manufacturing to national security since its inception in the early 1980s and is expected to continue to grow in number of connected devices. In all domains, security appears as the most important concern. Scholars put forth frameworks and assessment techniques for increased security, yet the gap between current solutions and the changing threat landscape persists. Furthermore, there are potential and dangers brought about by the confluence of IoT and emerging technologies like blockchain and artificial intelligence, which calls for a strong cybersecurity strategy.

The study also emphasizes how important IoT is to military operations, national security, and key infrastructure. The research paper highlights how the Internet of Things is revolutionizing a variety of industries while also stressing how urgently robust security measures and strategic considerations are needed. Stakeholders can ensure a more secure and resilient future by tackling the design, implementation, and management problems and fully utilizing the potential of IoT while protecting against new risks.

VIII. ACKNOWLEDGEMENT

This literature review would be incomplete without dedicating our gratitude to a few people who have contributed a lot towards the victorious completion for this paper. We would like to thank Thiru L. Gopalakrishnan, Managing Trustee, PSG & Sons Charities, for providing us with the prospect and surroundings that made the work possible. We take this opportunity to express our deep sense of gratitude to Dr T. Kannaian, Secretary of PSG College of Arts & Science, Coimbatore for permitting and doing the needful towards the successful completion of this paper. We express our deep sense of gratitude and sincere thanks to our Principal Dr D. Brindha M.Sc., M.Phil., Ph.D., MA (Yoga)., for her valuable advice and concern for students. We are very thankful to Dr A. Anguraj, M.Sc., M.Phil., Ph.D., Vice Principal (Academics), Dr Jayanthi M M.Com., MBA., M.Phil., Ph.D., Vice Principal (Student Affairs), Dr M. Umarani MBA, M.Phil., Faculty-In-Charge (Student Affairs), for their support towards this paper. We owe our deepest gratitude to Dr. K. V. RUKMANI., M.C.A., M.E., Ph.D., Associate Professor & Head, Department of Software Systems, for her encouragement to pursue new goals and ideas.

I convey my heartiest thankfulness to Lt. Dr. D. ANTONY ARUL RAJ, M.Sc.,(CS).,M.Phil., PGDCE., Ph.D., Assistant Professor, Department of Software Systems, for his timely suggestion which had enabled us in completing the paper successfully.

IX. REFERENCES

[1]. Carsten Maple (2017) Security and privacy in the internet of things, Journal of Cyber Policy, 2:2, 155-184, DOI: 10.1080/23738871.2017.1366536.

[2]. Sungyong Cha , Seungsoo Baek , Sooyoung Kang, and Seungjoo Kim,"Security Evaluation Framework for Military IoT Devices",Published 3 July 2018.

[3]. Siham Boukhalfa & Abdelmalek Amine & Reda Mohamed Hamou, 2022. "Border Security and Surveillance System Using IoT," International Journal of Information Retrieval Research (IJIRR), IGI Global, vol. 12(1), pages 1-21, January.

[4]. Security Threats on National Defense ICT based on IoT,Published June 2015.

[5]. T. A. Ahanger and A. Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms," in IEEE Access, vol. 7, pp. 11020-11028, 2019, doi: 10.1109/ACCESS.2018.2876939.

[6]. Jin-Seok Yang1, Ho-Jae Lee1, Min-Woo Park1 and Jung-ho Eom 2,"Security Threats on National Defense ICT based on IoT " , Department of Computer Engineering,School of Information and Communication Engineering, Sungkyunkwan University, Suwon-si, Republic of Korea, Department of Military Studies, Daejeon University,62 Daehakro, Dong-Gu, Daejeon-si, 300-716

[7]. Petrisor Patrascu ,"Emerging Technologies And National Security: The Impact Of Iot In Critical Infrastructures Protection And Defense Sector",Vol. Xxvi, No. 4(104), 2021,“Carol I” National defense University, Bucharest, Romania.

[8]. Vlada S. Sokolovic(a), Goran B. Markovic(b),"Internet of Things in military applications", (a)University of defense in Belgrade, Military Academy, Department of Logistics, Belgrade, Republic of Serbia,(b)University of Belgrade, School of Electrical Engineering, Belgrade, Republic of Serbia

[9]. Paula Fraga-Lamas *, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo and Miguel González-López, Spain (T.M.F.-C.); (M.S.-A.); (L.C.); (M.G.-L.),Published : 5 October 2016.

[10].Abiodun Esther Omolara , Abdullah Alabdulatif , Oludare Isaac Abiodun , Moatsum Alawida , Abdulatif Alabdulatif , Wafa’ Hamdan Alshoura and Humaira Arshad, The internet of things security: A survey encompassing unexplored areas and new insights, Published 29 September 2021.