Review

A Systematic Literature Review of Zero Trust Architecture for UAV Security Systems in IoBT

Alanoud Abdullah Alquwayzani * and Abdullah Abdulrahman Albuali *

Posted Date: 6 March 2024

doi: 10.20944/preprints202403.0349.v1

Keywords: Security; Zero Trust Architecture (ZTA); Drone; UAV, UAV Security; Internet of Battlefield Things (IoBT); Cybersecurity; Suspicious Behavior

 doi:10.20944/preprints202403.0349.v1

Review

A Systematic Literature Review of Zero Trust Architecture for UAV Security Systems in IoBT

Alanoud Abdullah Alquwayzani * and Abdullah Abdulrahman Albuali *

Dept. of Computer Networks and Communications, CCSIT, King Faisal University, Al Hassa 31982, Saudi Arabia
* Correspondence: 222402679@student.kfu.edu.sa (A.Q), aabuali@kfu.edu.sa (A.A)

Abstract: Over the years, the need for autonomous systems such as drones, also known as unmanned aerial vehicles (UAVs), has significantly increased in popularity across several industries, including the military. The Internet of Battlefield Things (IoBT) represents a modern technological advancement that significantly enhances the operational efficacy of defense systems. It establishes an integrated military force by connecting individuals to intelligent technology in drones, radios, equipment, antennas and ground stations. This is achieved through the utilization of cloud and edge computing, sensors, mobile devices, embedded systems, and IoT-based systems. However, IoBT security is significantly compromised by enemies that exploit the vulnerabilities and malicious intrusions that specifically target the external environment or to obtain sensitive data. In addition, a comprehensive understanding of cyberattacks and countermeasures is essential for assuring the security of IoBT. On the other hand, as cyber threats get more complicated, trust becomes increasingly important for the security of digital systems. Within this context, the zero trust architecture contends that the security of a complex network is inherently vulnerable to internal and external threats. In defense, UAV security system applications, for example, the primary purpose of the zero trust architecture is to limit the vulnerability of military UAV systems to cyberattacks, hence reducing the possibility of data breaches and illegal entry. This study conducts a systematic review aimed at identifying different aspects of cybersecurity strategies for protecting UAV systems within the IoBT domain. Furthermore, zero trust architecture is presented in the study as an effective prospective solution to the security issues that develop in defense UAV systems.

Keywords: security; zero trust architecture (ZTA); drone; UAV; UAV security; Internet of Battlefield Things (IoBT); cybersecurity; suspicious behavior

1. Introduction

Zero Trust Architecture (ZTA) is a security model that requires all devices, users, and applications to be authorized and authenticated. Before accessing resources, validation is required [1]. The model operates on the principle of "Never trust, always verify," recognizing trust as a vulnerability that can be exploited by malicious insiders or external attackers [2]. In the military UAV Security, the implementation of zero trust can play a crucial role in detecting suspicious behavior and potential threats. By applying a zero trust approach, military UAV operators can ensure that only authorized and authenticated devices and applications have access to the UAV's systems, minimizing the risk of unauthorized access and data breaches. The importance of zero trust in military UAV Security cannot be overstated. UAVs are increasingly being used for military purposes, including reconnaissance, surveillance, and combat operations [3]. As such, they are valuable targets for cyberattacks, and any security breach can have severe consequences.

Implementing zero trust can help to mitigate this risk by providing a comprehensive security framework that covers every aspect of the UAV's operation [4]. By identifying sensitive or valuable data, and defining access controls, zero trust can minimize the attack surface and reduce the risk of data breaches. Furthermore, by continuously validating user and device behavior, zero trust can respond and detect suspicious activity in real-time, enabling operators to take immediate action to mitigate the threat [5].

Machine Learning (ML) has the capability to be utilized to implement zero trust in military UAV Security. By analyzing large number of logs and data generated by the UAV's systems, ML algorithms

 doi:10.20944/preprints202403.0349.v1

can detect trends and anomalies that may indicate potentially suspicious activity. These algorithms can be trained to recognize specific threat vectors and take appropriate action to mitigate them. For example, if an ML algorithm detects unusual network traffic or unauthorized access attempts, it can trigger an alert and isolate the compromised device or application [6]. The use of ML in zero trust can significantly enhance the security of military UAVs, providing operators with real-time threat detection and response capabilities [4]. Unauthorized access, data breaches, and the possibility of drone hijacking are all important issues that must be addressed to ensure the integrity and security of these systems. To mitigate these threats, robust security measures and solid architecture are essential and needed.

This survey paper explores the application of the zero trust security model in the military UAV to detect any suspicious behavior and ensure that these vital assets remain resilient and secure in general, particularly in battlefield environments. UAVs, commonly called drones has become an integral part of military operations worldwide. With the increasing reliance on UAVs, ensuring their security against potential threats has become paramount. The concept of ZTA, which emphasizes the principle of "never trust, always verify," offers a promising approach to detect and counteract suspicious behaviors in military UAVs. This survey aims to provide an in-depth understanding of the implementation of ZTA in military UAVs.

The survey is divided into sections that discuss an overview of ZTA, related work, architecture's components, its benefits, with a focus on military UAV security. It covers the requirements, threats, and ZTA applications in UAVs, future direction, and conclusion. A detailed breakdown of these sections is presented in Figure 1. Each section provides insights and analyses based on existing research and industry practices. The rest of the paper is organized as follows: Section 2 presents the details of zero trust model in IoBT. Section 3 presents related studies based on a systematic literature review (SLR). Section 4 describes the implementation techniques of this security framework. Section 5 covers IoBT attacks. Section 6 discusses the integration of zero trust within the Internet of Battlefield Things, emphasizing authentication and access control systems. Section 7 looks ahead to the future directions for using ZTA in UAVs. Section 8 concludes the paper by showing the key findings of the promising of ZTA in military UAV security and the potential future research and industrial applications.

 doi:10.20944/preprints202403.0349.v1

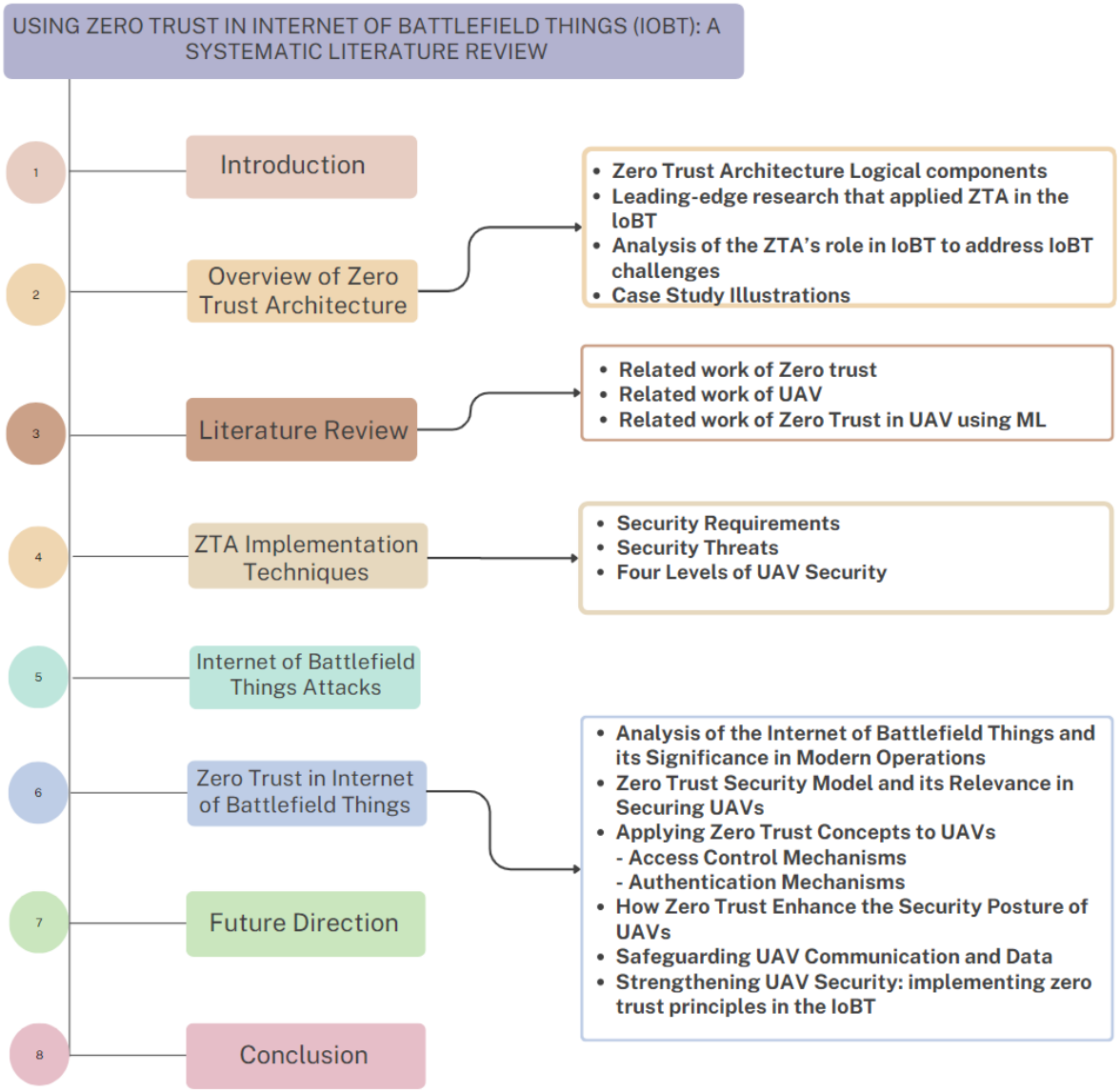

Figure 1. Structural Overview of the Paper.

2. Overview of ZTA

ZTA is a revolutionary security concept that questions the effectiveness of the conventional perimeter-based security model [1]. It operates on the principle that no device or user should be inherently trusted, irrespective of their location or origin. By implementing zero trust principles and components, drone systems can significantly enhance their security posture and protect against potential risks. Table 1 presented a comparison between the traditional security model and zero-trust model.

 doi:10.20944/preprints202403.0349.v1

Table 1. Contrasting the conventional security model with the zero trust model

Features	Traditional Security Model	Zero Trust Model
Approach	Verify with trust.	Verify everything without trusting anything.
Trust Boundary	No trust for external devices and users but trust for internal devices and users.	Not trust for internal and external devices and users.
Access Control	Process of regulating and managing access to resources or systems, such as IP (Port, Protocol) based access control.	Data-centric access control approach, which focuses on controlling access to specific data or information.
Communication Encryption	External traffic is Encryption but Internal traffic is not Encryption.	All traffics are encryption.
Authentication	Occurs during the initial access and involves verification.	Requires before access and involves constant verification.
Security Policy	Pre-defined rules and common policies are in place.	Fine-grained rules and adaptive policies can be implemented after a thorough Security Assessment.
Security Managements	Involves the monitoring and visibility of individuals	Involves visibility, devices, automation, and security of behavior, orchestration, services, and systems.

The first fundamental principle of ZTA is eliminating implicit Trust. Every user and device, including drones, must undergo strict authentication and authorization processes before accessing any resources or data. Instead of relying on a single trust point, zero trust employs multiple layers of verification to ensure the legitimacy and integrity of each interaction.

The second principle revolves around the concept of least privilege [7]. Zero Trust promotes the idea that users and devices should be allocated only the essential privileges required for their designated tasks. This principle restricts access rights to specific resources, limiting the potential damage from a compromised account or device.

Another crucial principle of ZTA is continuous monitoring and analysis. Instead of assuming that users and devices remain trustworthy indefinitely once granted access, zero trust advocates for constantly monitoring their activities. This includes scrutinizing network traffic, user behavior, and device characteristics in real-time to detect any suspicious or anomalous patterns that may indicate a security breach. In terms of components, ZTA comprises of several key elements. Identity and access management (IAM) solutions are vital in enforcing strict authentication and authorization processes. These system authenticate the identity of users and devices, validate their credentials, and grant access based on predetermined policies [8].

Network segmentation is another critical component. Zero Trust limits the lateral movement of potential threats by dividing the network into smaller, isolated segments. Each component has its own security controls and authentication requirements, reducing the impact of a potential breach and containing it within a confined area.

Furthermore, encryption plays a significant role in ZTA. Encrypting data at rest and in transit protects sensitive information even if intercepted by unauthorized entities. Data confidentiality and integrity are guaranteed through encryption, limiting the risk of unwanted access or data alteration[4].

ZTA has key components that assist secure the IoBT network and protect the UAVs. The IoBT sensors collect and analyze a large amount of data, such as aerial photography and environmental information. These data are stored and protected by the PE (of the ZTA), which uses Least Privilege Access Control to provide UAVs authorized access to certain resources (the collected data). Any access not authorized by this PE control is denied to the UAVs. The UAVs ensure that they only access resources provided by the PE of the ZTA and so remain secure. The Policy Administrator (PA) Component of the ZTA grants drones access to a resource after the PE has authorized it [9]. With this component, UAVs can only access the IOBT's network resources to which the PE has authorized

 doi:10.20944/preprints202403.0349.v1

access. This prohibits the drone from accessing network resources that he has not been granted access to, hence protecting the IOBT's network.

Furthermore, Identity and Access Management (IAM) is a vital component of the ZTA that uses robust authentication and authorization methods to verify user and device identity before granting access. It accomplishes this by accessing the user's device and determining whether it is connected to the network, updated, and equipped with the necessary antivirus software. This prevents cyber criminals from bugging the network and safeguards UAVs while they are in operation.

Real-time monitoring and analysis of user and device behaviour is critical. The ZTA's Policy Enforcement Point (PEP) control monitors the connection between the user, their device, and the IoBT's network resources. When the PEP detects a compromised device connecting to the network, it notifies the network, disconnects the compromised device from the network, and prevents any attempted assault on the network. This alerts the IoBT to any attacks and safeguards the UAVs from adversary manipulations during missions.

The micro-segmentation control partitions networks into small, isolated zones. This minimizes attacks on the IoBT network by ensuring that it does not spread to other microsegments if security is exploited. This allows the UAVs to remain operational because they can be commanded from various microsegments of the IoBT without jeopardizing their mission [10].

2.1. ZTA Logical Components

The architecture is made up of various services that have multiple logical components. These components are operated through the cloud, either onsite or offsite. National Institute of Standards and Technology (NIST) [10] has defined three of these components as core: Policy Engine (PE) in the control plane, Policy Administrator (PA) in the control plane, and Policy Enforcement Point (PEP) in the data plane. These three components are displayed in the Figure 2. Their functions include the following:

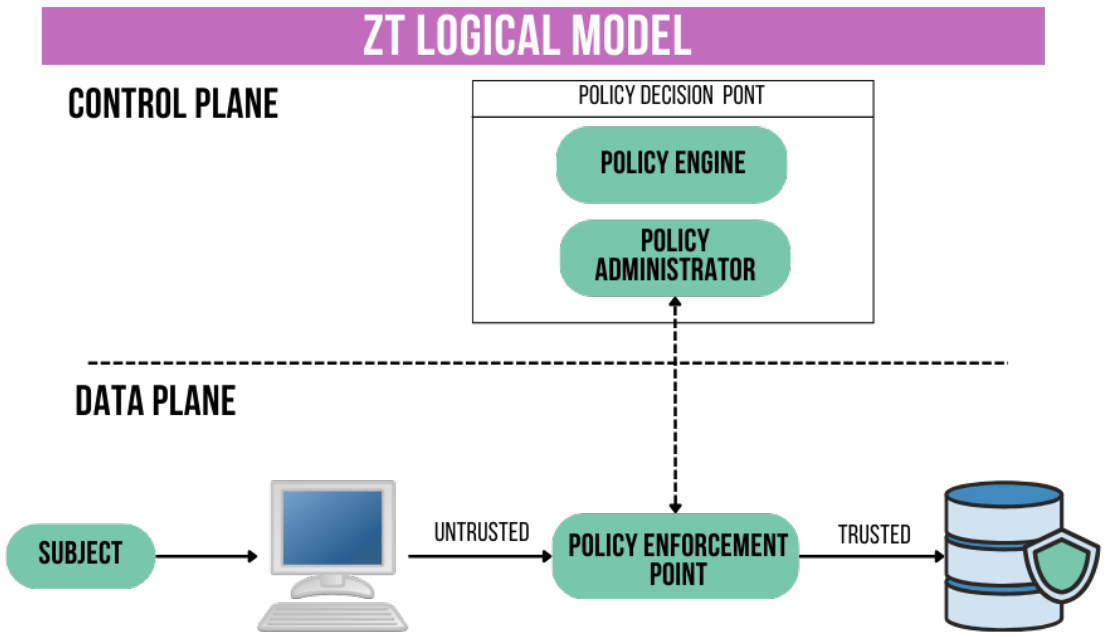

Figure 2. Core logical components of ZT [9]

- PE: makes access decisions according to the policies of the company. The system achieves this by utilizing external inputs and employing a TA as its cognitive mechanism.

 doi:10.20944/preprints202403.0349.v1

- PA: works along with the PE to provide or refuse access depending on the PE's decision. This system may be seamlessly included with PE and establishes communication with PEP for the purpose of enforcing policies.
- PEP is responsible for facilitating, overseeing, and terminating the connection between the subject and the resource. The system consists of two sub components: the client (such as an agent installed on a device) and the resource (such as a gateway). The trust-zone is typically located beyond the PEP. Apart from the core components, [9] mentions several additional components that help achieve zero trust security, including continuous monitoring. The decision to allow access is made by the PE using Trust. This utilizes various measures such as diagnostics, mitigation, data access policies, identity management, Security Information and Event Management (SIEM) alongside activity logs.

Table 2. ZTA components for IoBT.

ZTA Component	Component Description
Access Management: – Identity Access Management – Privilege Access Management – Whitelisting	Defines and manages the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. Access management is the process of controlling and monitoring access to resources within the IoBT (Internet of Battlefield Things) network. Access management guarantees that only authorized people or devices can interact with an unmanned aerial vehicle (UAV), lowering the danger of unauthorized access, data breaches, or tampering.
Segmentation: – Micro segmentation – Macro segmentation	An approach in computer networking that is the act or practice of splitting a computer network into sub-networks, each being a network segment. Micro-segmentation involves dividing networks into logical units and applying policies to control access to data and applications within these segments. By segmenting the network and restricting traffic between segments, organisations can significantly enhance security. Micro-segmentation for UAV security in IoBT networks aids in establishing of discrete zones or compartments within the network, hence limiting the attack surface and preventing lateral threat movement.
Encryption: – Data-at-Rest – Data-in-Transit – Data-in-Use	The process of encoding information. Keeps data encrypted while in transit between the enterprise server and the device itself. In the context of UAV security in IoBT networks, data encryption ensures that sensitive information exchanged between the UAV and ground stations or other network components is secure and confidential.

2.2. Leading-Edge Research That Applied ZTA in the IoBT Context, Particularly for UAVs Security

UAVs and IoBT are vulnerable to cyberattacks because of their wireless connectivity and remote operation. This leaves them vulnerable to hijacking by cybercriminals. To address this challenge, Anthony Moffa [11] investigated how ZTA intends to protect sensitive data and the network by implementing strict access control, authentication mechanisms, and monitoring techniques on devices connected to the IoBT, regardless of location or network. Furthermore, HikVision's [12] "Securing a New Digital World with Zero Trust" explains that network segmentation, which divides IoBT networks into smaller, isolated segments, limits the lateral movement of threats within the network and reduces the damage that a compromised IoBT device can cause to the network.

Sairath Bhattacharjya [13] has also stated that because to the heterogeneous ecosystem of smart devices and the massive increase in the number of connected endpoints, it is difficult to trust a request or answer arriving from an unknown source via an untrusted medium. As a result, the ZTA technique was adopted to develop a robust authentication mechanism in which every request may be checked and access determined before proceeding with any further operation.

 doi:10.20944/preprints202403.0349.v1

2.3. Analysis of the ZTA's Role in IoBT and Refinement of ZTA Protocols to Address IoBT Challenges

The ZTA has been able to secure the IoBT network and protect the operations of the UAVs with strong authentication and authorisation methods, continued verification, continued monitoring, micro-segemtation and strict access control. However, the IoBT experiences some challenges that may influence the refinement of the ZTA protocols. One of the challenges experiences by the IoBT is security vulnerability associated with those battlefield devices. Many IoBT devices lack proper configuration of encryption and authentication mechanisms and the diversity of these IoBT devices makes them easy targets to cyber criminals who can exploit the weak security measures of these devices to gain unauthorized access to the battlefield network and manipulate the data there. To overcome this challenge, there must be strict adherence of the ZTA principle of "never trust, only verify" to ensure all loBT devices are properly configured before given access. Additionally, the absence of standardization in the IoBT is a difficulty. Without uniform standards, interoperability of IoBT devices suffers greatly, and with unstandardized security procedures across IoBT devices, cyber thieves can infiltrate the network's weakest link. This might lead to serious breaches involving vast amounts of data, with severe consequences for privacy and financial loss. ZTA would need to strike a compromise between standardization and guaranteeing that all IoBT devices are uniformly standardized. Furthermore, the IoBT is concerned with privacy hazards since sensitive data may slip into the wrong hands. This emphasizes the importance of the ZTA implementing strong security measures as well as thorough privacy legislation. Moreover, the rapid rate at which IoBT data is generated exacerbates these management problems, necessitating real-time or near-real-time processing to extract timely insights and enable swift decision-making. This demonstrates that ZTA's network access advantages for UAVs must be balanced against the operational speed required in IoBT, which promotes real-time or near-real-time processing to extract timely insights and enable rapid decision-making.

Table 3. Challenges in implementing ZTA for UAV security in IoBT.

Challenges	Possible Solutions
Cultural Barriers and Organizational Resistance: Organizational culture must change to implement Zero Trust in place of conventional security paradigms. The zero trust concepts of least privilege access and constant verification may not sit well with team members used to perimeter-based trust models.	Providing tangible evidence of successful UAV deployments in IoBT, including improved operational efficiency, enhanced situational awareness, and reduced risks to personnel, can help overcome skepticism and build trust in the technology. Also through implementing change management strategies, comprehensive training.
Problems with integration and technical complexity prevent UAVs from being fully utilized in the Internet of Battlefield Things (IoBT). Advanced technology is needed for UAV systems in order to integrate payloads, operate autonomously, and maintain cybersecurity.	Collaborative development activities are crucial to addressing the issues given by technical complexity and integration when introducing UAVs into the Internet of Battlefield Things (IoBT). Promoting standardization projects and allocating resources towards continuous improvement techniques can effectively optimize integration procedures and guarantee smooth interoperability throughout the IoBT network.
One of the biggest challenges in using UAVs in the Internet of Battlefield Things (IoBT) is striking a balance between security and usability. Robust cybersecurity protections are vital to fend against threats like jamming and hacking, but in order to maintain smooth and productive operation in dynamic battlefield conditions, they must be balanced with usability needs. Comprehensive risk assessment, user-friendly security protocol implementation, continuous monitoring, and adaptation to changing threats and operational requirements are all necessary to achieve this balance.	Balancing security and usability in UAV implementation within IoBT necessitates creating intuitive interfaces and speeding authentication processes to ensure user productivity while improving security safeguards. Optimising procedures enables efficient operation while maintaining the effectiveness of security upgrades.

Continued on next page

 doi:10.20944/preprints202403.0349.v1

Table 3. *Cont.*

Challenges	Possible Solutions
Financial considerations are important in the deployment of UAVs within the Internet of Battlefield Things (IoBT). UAV system procurement, maintenance, and operation incur significant expenditures, including initial hardware, software, and infrastructure investments, as well as continuous fees for training, support, and upgrades.	To mitigate the financial impact, strategies such as leveraging economies of scale through centralized procurement, prioritizing cost-effective UAV models with long-term viability, and exploring public-private partnerships for shared investment and resource allocation can help optimize budget utilization and ensure UAV deployment affordability within IoBT.
Data privacy and regulatory compliance are key barriers to the deployment of UAVs in the Internet of Battlefield Things (IoBT). Strict rules govern the collection, storage, and transmission of sensitive data recorded by UAVs, requiring compliance with privacy laws and security requirements to prevent unauthorized access and misuse of information.	To solve these issues, employing strong data encryption techniques, anonymizing personally identifiable information, and developing explicit standards for data management and sharing can assure regulatory compliance while protecting privacy in UAV operations under IoBT.
Organizational scalability has a substantial impact on UAV implementation within the Internet of Battlefield Things (IoBT). As demand for UAV capabilities develops and mission requirements change, organizations must ensure that their structures, processes, and people can expand to meet increasing operational demands.	Implementing flexible organizational structures, engaging in ongoing training and development programs, and developing relationships with industry and academics can improve organizational scalability, allowing for effective use of UAVs in a variety of operational scenarios within IoBT.

2.4. Case Study Illustrations

Alicia Morel et al.'s article on Enhancing Network-Edge Connectivity and Computational Security in Drone Video Analytics explains how ZTA protects UAV military operations by preventing unauthorized data access and allowing only valid system requests to be authorized via the PDP and PEP functionalities [14]. According to Yuan Feng et al, battlefield real-time data sharing and cooperative decision-making among commanders rely heavily on network connectivity between different combat units and UAVs. However, due to the wireless nature of communication, a huge number of communication links are immediately exposed in the complex battlefield environment, and various cyber or physical attacks represent a threat to network connectivity. As a result, the capacity to retain network connectivity in the face of adversary attacks, as well as safeguard the network and ensure that UAV operations are not hampered by cyber attacks, requires the implementation of zero-trust [15].

3. Literature Review

SLR is a method employed to choose a concise set of studies from an extensive range. This is a crucial rationale for its application in this paper. The initial phase involves querying the JSTOR, Google Scholar, IEEE, ScienceDirect, and Scopus databases using a combination of keywords. In the first stage, databases were searched using the following query: (zero trust) AND (UAVs OR Drone OR Military) AND (Machine learning). The literature is limited only to studies published in English between 2014 and 2023. Database searches revealed 27,570 papers that specifically discuss zero trust and how it might be applied in various sectors. After registering the initial papers, 18,000 duplicate were removed, 500 papers were marked as ineligible by automation tool, and 1,500 papers for other reasons. We have 2,380 papers remaining; after screening, 2000 papers have been excluded for type of study and 300 papers for other reasons. Additionally, 45 reports could not be retrieved, and 12 publications have been excluded for having vague titles and abstracts. Finally, after reviewing and studying these papers, we selected 23 papers from the databases and 3 from Studies included in the previous version of the review. This selection process of papers by PRISMA 2020 is shown in Figure 3.

 doi:10.20944/preprints202403.0349.v1

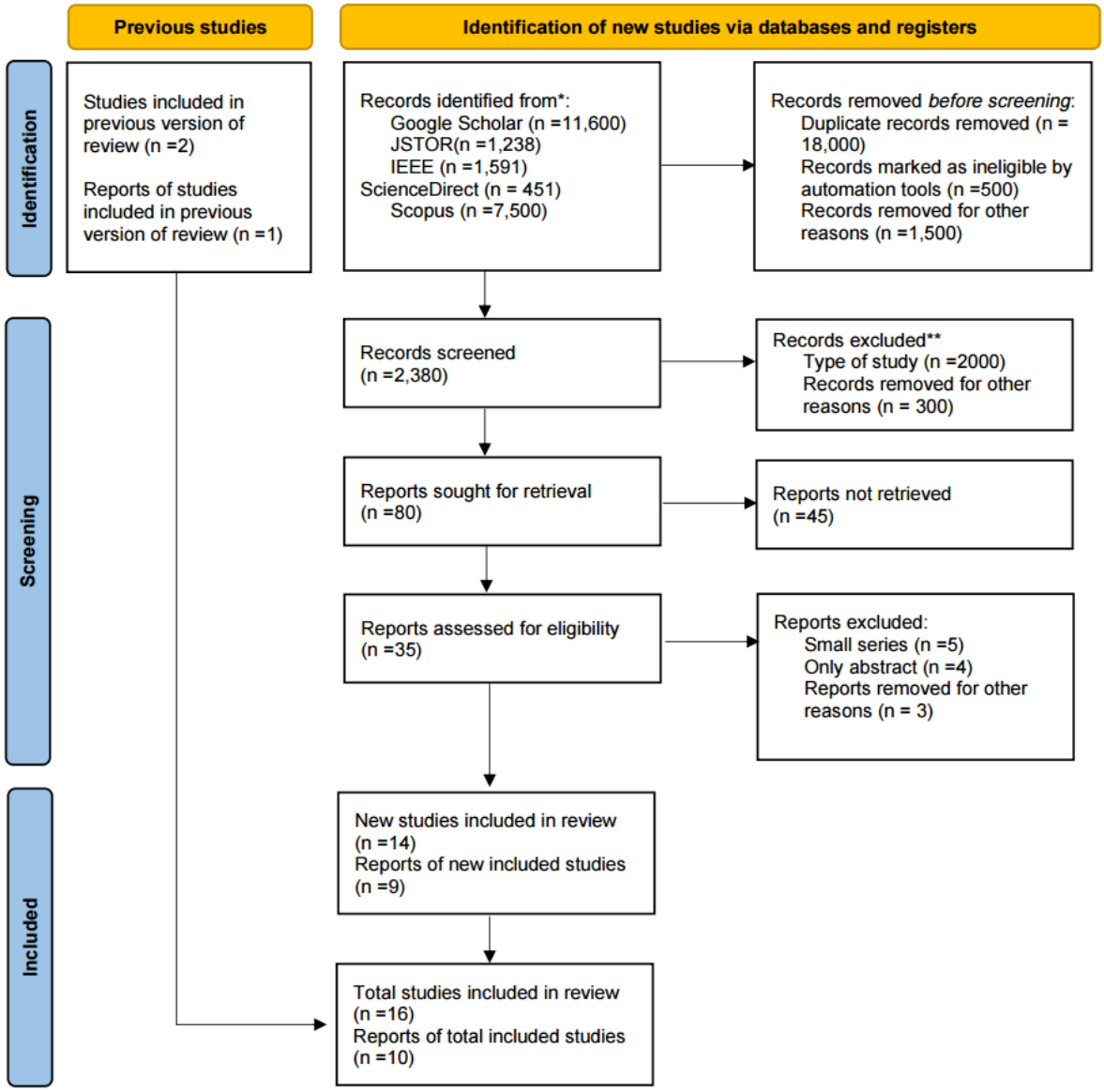

Figure 3. Selection of papers for Literature Review using PRISMA.

This survey explores the future trajectory of incorporating ZTA into the security framework of UAVs in the dynamic landscape of IoBT. As UAVs continue to play a pivotal role in modern warfare, the need to strengthen their security becomes increasingly urgent. This study investigates prospective avenues in ZTA application, including addressing the evolving nature of threats in the military domain, optimizing network segmentation strategies for enhanced protection, advancing authentication and authorization mechanisms, ensuring comprehensive data protection in IoBT scenarios, and bolstering ZTA resilience against potential UAV compromises. By synthesizing existing literature and considering emerging trends, the research aims to not only provide a comprehensive analysis of the current state of ZTA integration in UAV security within IoBT but also to identify research gaps and propose innovative directions for future developments. The goal is to contribute insights that can guide the design and implementation of robust security measures, aligning with the anticipated challenges and advancements in the evolving landscape of UAVs operating in the IoBT.

3.1. Related Work of Zero Trust

In 2010, Kindervag [16] introduced a zero trust architectural model and provided a practical implementation methodology. Their publication proposed a ZTA, emphasizing the "Data Acquisition

 doi:10.20944/preprints202403.0349.v1

Network" (DAN). The DAN system streamlines the extraction of network data to the management center, enabling real-time inspection and analysis. This, in turn, results in the implementation of the zero trust concept. However, this progress accompanied by challenges, such as heightened network complexity and increased user communication delays.

Subsequently, in the year 2016, DeCusatis et al. [17] introduced a zero trust approach that relies on transport access control. The suggested method is based on the principles of stenography and overwriting. Specifically, the authentication token is hidden in the TCP request packet and the initial authentication packet. This approach strengthens enterprise security in cloud computing environments by adhering to the zero trust concept and efficiently reducing the risk of unauthorized fingerprinting of protected resources. It is crucial to highlight that while this strategy protects layer 3/4, it does not extend its security measures to layer 7.

In a further study conducted in, 2020, Rose et al. [18] provided a comprehensive summary of the prevailing fundamental ZTA schemes. Additionally, they put forth the essential logical components that constitute the ZTA. Furthermore, the authors emphasized the practical implementation of ZTA. Instead of implementing a comprehensive overhaul of infrastructure or procedures, this approach entails systematically implementing specific measures, for example, robust identity and access management (IAM) protocols, to apply ZTA in a network. currently built on a perimeter-centric architecture.

Zero trust promotes a host-based monitoring approach, allowing each device owner to define the methods and criteria to access it. This indicates that the host can dictate the target audience while prohibiting unauthorized users from accessing the restricted data [19]. Zero Trust security guarantees that no item within the system limits can stray out of scope. As a result, every component is treated as a potential target for either accidental or adversarial effects [20]. According to the US Department of Defense, zero trust (ZT) embeds security throughout a defined and limited framework, preventing malicious actors from accessing essential resources. This works in the sense that every device, application, user and network are managed and monitored within the defined security perimeters. This mitigates the risk of unverified trust that can lead to serious security breaches [21]. For already established entities with traditional cybersecurity implementations, migrating and adopting ZTA can involve various principles and stages.

NIST advises that an organization can pursue the adoption of the ZTA from an incremental perspective. This means that enterprises can choose to adopt the new security framework from a hybrid standpoint, involving both the zero trust and perimeter-based mode for an indefinite period. The Canadian Government suggests that the implementation of zero trust security systems can also leverage software-defined approaches which can help in building security environments that allow context-based and logical access in various application systems. Using such approaches can limit access to application assets in public visibility since the trust broker must validate the identity, context, and policy adherence of the specified users [22]. ZTA thrives on creating a paradigm that relies on the "never Trust, always verify" principles. The deployment of a zero trust system within a given system can restrict access to resources by only permitting "trusted agents". The validation of every access by the trusted agents is necessary and continuous [23]. This approach aims to eliminate unauthorized access to the system's data and services, thus security enforcement becomes more granular by breaking down privileged access to resources into little pieces.

In order to address the issue of trust deficit, the researchers in [24] utilized ZTA framework to create a trust model customized for cloud environments. The research introduces a comprehensive model aimed at enhancing trust within an organization's information system. The model's design integrates reference components sourced from the National Institute of Standards and Technology. The researchers conducted a performance analysis to evaluate the effectiveness of the proposed model. The results clearly demonstrated that the distribution of trust-based nodes can effectively mitigate intrusions. Due to the existing shortcomings of cybersecurity measures in virtual power plants, the authors in [25] implemented ZTA as a means to improve privacy and data protection within the energy sector. Their approach was based on the fundamental principles of ZTA and demonstrated satisfactory

 doi:10.20944/preprints202403.0349.v1

performance, offering a viable solution to mitigate the risks of data theft and breaches. Since the beginning of the pandemic, there has been a considerable increase in the use of zero trust, resulting in significant shifts in workplace dynamics.

Organizations have implemented remote working arrangements in an effort to mitigate the spread of viral infections. However, this approach has inadvertently made networks and systems more vulnerable to intrusion. To address this issue, the zero trust model has gained popularity as a means to bridge the gap in network security and prevent hacking incidents. As a result, various organizations, including prominent institutions such as the United States government's Department of Defense, Department of Health and Services, and Department of Homeland Security, have adopted this model [26]. In order to facilitate the widespread implementation and utilization of the model, some information technology companies have devised a functional prototype that aligns with the principles outlined in the NIST policy. One notable organization that has made significant contributions in this regard is Microsoft [27]. Table 4 represent summary of articles for zero trust.

Table 4. Summary of Articles Table for Zero Trust.

Paper	Year	Key Findings	Description
Kindervag [16]	2010	Proposed a ZTA, emphasizing the "Data Acquisition Network" (DAN)	This report paper is a deep dive into how you can potentially use and implement the Zero Trust model concepts in the real world. One of the most important goals is to improve security architectures and technologies for future usage. This paper can benefit you in starting to design infrastructure using zero trust. Their publication proposed a ZTA, emphasizing the "Data Acquisition Network" (DAN). The DAN system streamlines the extraction of network data to the management center, enabling real-time inspection and analysis.
DeCusatis et al. [17]	2016	Principles of steganography and overwriting. In particular	This paper introduced a zero trust approach that relies on transport access control. The suggested method is based on the principles of steganography and overwriting. In particular, the authentication token is hidden in both the TCP request packet and the initial authentication packet. By adhering to the zero trust principle, this approach strengthens the security of enterprises functioning in cloud computing environments and efficiently reduces the risk of unauthorized fingerprinting of protected resources.
Rose et al. [18]	2020	Authors placed greater emphasis on the execution of ZTA, with a particular focus on achieving the realization of ZTA	Authors put forth the essential logical components that constitute the ZTA. Furthermore, the author placed greater emphasis on the execution of ZTA, with a particular focus on achieving the realization of ZTA. Instead of implementing a comprehensive overhaul of infrastructure or procedures, this approach entails a systematic implementation of specific measures to apply ZTA in a network that is currently built on a perimeter centric architecture.
[23]	2023	Implementation of the zero trust system can reduce access to resources by only allowing "trusted agents".	This paper advices to use ZTA for creating a paradigm that relies on the "never Trust, always verify" principles. Within in a given system, the implementation of the zero trust system can reduce access to resources by only allowing "trusted agents". The validation of every access by the trusted agents is necessary and continuous. This approach targets eliminating unauthorized access to data and services of the system and so, the security enforcement becomes granular through dividing up privileged access to resources into small pieces.

 doi:10.20944/preprints202403.0349.v1

Table 4. *Cont.*

Paper	Year	Key Findings	Description
[24]	2021	ZTA framework is utilized to create a trust model customized for cloud environments.	The research introduces a comprehensive model aimed at enhancing trust within an organization's information system. The model's design integrates reference components sourced from the National Institute of Standards and Technology. The researchers conducted a performance analysis to evaluate the effectiveness of the proposed model. The results clearly demonstrated that the distribution of trust-based nodes can effectively mitigate intrusions.
[25]	2022	Implemented ZTA as a means to improve privacy and data protection within the energy sector.	Their approach was based on the fundamental principles of ZTA and demonstrated satisfactory performance, offering a viable solution to mitigate the risks of data theft and breaches. The adoption of zero trust has experienced a notable increase in usage scenarios since the onset of the pandemic, resulting in significant shifts in the dynamics of the workplace setting.

3.2. Related work of UAV

Paper Finn et al. [28] utilization of UAVs for surveillance and civilian assignments has increased significantly in recent years. Moreover, UAVs will have an increasing number of uses in the future. The accelerated development of technology permits the diminution of device size and price. All of this makes it possible to utilize UAVs in ways that ten years ago were unimaginable. UAVs have a variety of social applications, including search and rescue operations [29], automatic forest fire surveillance and measurement [30] and disaster management [31]. Commercial tasks are also found in the agriculture [32], construction [33], surveying and geology [34], surveillance [35], and film industries [36] industries.

Compared to alternative choices, the affordability of new UAVs and their applicability across diverse fields have generated significant attention for this technology. The widespread use of UAVs has reached a point where regulations are necessary to curb illicit activities and mitigate accidents. Numerous studies have explored the legal implications of utilizing robots and autonomous systems, particularly in sectors like video surveillance, image rights, and defense. Addressing these intricate matters is already a central focus in managing the deployment and operation of UAVs. Finn and Scheduling [37] conducted among the initial comprehensive analyses of these legal and ethical issues. However, an analysis of the vast array of UAV capabilities is insufficient for the development of a platform to monitor UAV flights. When developing the platform, security and legal considerations must be taken into account, as all laws governing the utilization of these vehicles should be incorporated into the platform, and the UAV must be protected from attacks that could compromise its operation or cause of loss sensitive data, the issue can be fixed by implementing the zero trust in UAVs. Table 5 represent summary of articles for UAV.

Table 5. Summary of Articles Table for UAV.

Authors	Key Findings	Research Type
U.S. Department of Defense	zero trust (ZT) enhances security by embedding it throughout the framework, limiting unauthorized access.	Government Report
NIST	Organizations can adopt zero trust incrementally, combining it with perimeter- based security for a period.	Government Report
Canadian Government	zero trust security can leverage software- defined approaches, enhancing context-based access control.	Government Report

 doi:10.20944/preprints202403.0349.v1

Table 5. *Cont.*

Authors	Key Findings	Research Type
Unnamed Paper (Finn et.)	Unmanned Aerial Vehicles (UAVs) have diverse applications, spanning surveillance, search and rescue agriculture, and more.	Academic Paper
R. L. Finn and D. Wright (2012)	UAVs raise legal and ethical issues related to surveillance, privacy, and civil applications.	Academic Paper
S. Waharte and N. Trigoni (2010)	UAVs can support search and rescue operations.	Conference Paper
Merino et al. (2012)	UAVs can be used for automatic forest fire monitoring.	Academic Paper
M. Quaritsch et al. (2010)	Networked UAVs have the capability to operate as an aerial sensor network dedicated to disaster management.	Academic Paper
D. Gómez-Candón et al. (2014)	UAV imagery is accurate for precision agriculture purposes.	Academic Paper
Y. Ham et al. (2016)	UAVs can visually monitor civil infrastructure systems.	Academic Paper
S. P. Bemis et al. (2014)	Photogrammetry, whether ground-based or UAV-based, serves as a high-resolution mapping tool for structural geology	Academic Paper
C. Bracken et al. (2014)	UAVs raise privacy implications in Canada due to surveillance.	Report
J. Fleureau et al. (2016)	An all-encompassing drone control platform can independently capture cinematic scenes	Conference Paper
A. Finn and S. Scheding (2010)	Advancements and obstacles are present in autonomous unmanned vehicles.	Academic Paper

3.3. Related Work of Zero Trust in UAV Using ML

Nour [38] provides an in-depth study of Internet of Things (IoT) security vulnerabilities and highlights the limitations of limited power capacity, which compromises encryption and timely updates. The study highlights the importance of a zero trust model for IoT and the risks of not applying such strong authentication and authorization measures. Using 5G's low latency potential, Nour proposes an ML-based intrusion detection system (IDS) within a zero trust framework optimized for real-time threat detection in power-constrained 5G edge environments.

Notably, after evaluating multiple ML models, decision trees and extreme gradient boosting classifiers were the most effective Ramezanpour and Jagannath [39] studied the integration of zero trust (ZT) principles into new 5G/6G communication networks and discovered significant vulnerabilities associated with such large and complex systems. By introducing Intelligent zero trust architecture (i-ZTA), they highlight its novelty in effectively handling network security with untrusted components. Their approach uniquely integrates artificial intelligence and focuses on the MED (monitoring, evaluation, and decision-making) component as critical for dynamic trust assessment. Similar to the current project, while focusing on 5G/6G networks, the overall principles used by i-ZTA and AI can provide useful insights when applied to detect suspicious behavior in military drones under a zero trust framework.

Keshavarz et al. [40] addressed critical security vulnerabilities faced by drones and highlighted notable threats such as Global Positioning System (GPS) spoofing, distributed denial-of-service (DDoS), and man-in-the-middle (MITM) attacks. They emphasized the urgency of ensuring the safety of drones, not only to protect their integrity, but also to protect the wider operational environment and human safety. Their core proposal is a trust monitoring mechanism, controlled by a central entity such as a ground station, that measures the trustworthiness of a drone by assessing its actions and behavior in real time. This approach can effectively identify drones that are vulnerable to

 doi:10.20944/preprints202403.0349.v1

cyberattacks. Kulunathan et al. [41] provided a comprehensive overview of integrating ML methods into unmanned aerial vehicle (UAV) operations and communications. The study highlights the growing synergies between ML and drones, demonstrating their joint potential to improve drone intelligence and autonomy. Their research examined four main operational components of drones where ML can make significant advances: perception, feature interpretation, trajectory planning, and aerodynamic control. A basic understanding of ML applications in drones is established, but the overarching need to increase reliability and trust in line with the goals of the future project is emphasized. The study [42] discusses the rapid development of Internet of Vehicles (IoV) technology, as well as the security threats associated with it, especially hacker attacks that could target user devices and identities. To prevent tampering attacks, the authors suggest a multi-factor authentication approach that involves device fingerprinting and Public Key Infrastructure (PKI). They utilize algorithms classified as state secrets for data encryption and blockchain technology to protect and ensure the security and integrity of data collection and transmission. The zero trust security network architecture is used to improve the system's security during data transmission, perform dynamic access control, monitor user behavior in real-time, and eliminate malicious nodes. The paper introduces an evaluation system for vehicles based on various pass rates for authentication and acceptance rates for packet transmission.

Table 6. Summary of Articles Table for zero trust in UAV using ML.

Authors	Year	Key Focus	Methodology/Technique	Key Findings
Nour [38]	2023	IoT security vulnerabilities in 5G-based networks.	ML-based Intrusion Detection System (IDS) in a zero trust framework.	Decision Tree and Extreme Gradient Boosting were the most efficient models for real-time detection.
Ramezanpour & Jagannath. [39]	2022	zero trust in 5G/6G networks.	i-ZTA with AI, focusing on the MED components.	i-ZTA principles and AI might offer insights for detecting suspicious behavior in military UAVs.
Keshavarz et al. [40]	2020	UAV security threats like GPS spoofing, DDoS.	Real-time trust monitoring mechanism assessing UAV behaviors via a centralized unit.	Identified UAVs undergoing cyber-attacks, emphasizing real-time monitoring.
Kurunathan et al. [41]	2023	ML in UAV operations and communications.	Comprehensive review on ML methodologies within UAV operations.	Identified gaps in ML applications for UAVs, emphasizing the need for enhanced reliability and trust.

4. ZTA Implementation Techniques

ZT principles that may be recognized and considered appropriate to a given context should be described, particularly the methods used to implement them. Although some organizations support defining the ZTA principles and logical components, defining Critical Infrastructure (CI) implementation strategy remains uncertain. The ambiguity is also due to the extensive endpoints, which include IoT devices, CPS devices, or even conventional network-end CNs, as well as varied technologies implemented in different types of implants, ranging from new frameworks to obsolete systems. However, these factors cause numerous difficulties in successful implementation.

4.1. Security Requirements

Authorization and authentication play pivotal roles in ensuring the security of UAVs. Authentication establishes the identity of users or systems interacting with the UAV, safeguarding against unauthorized access and data manipulation. Meanwhile, authorization determines the level of access and privileges granted to authenticated entities, ensuring that only authorized personnel or systems can perform specific actions or access particular resources within the UAV ecosystem. These

 doi:10.20944/preprints202403.0349.v1

mechanisms collectively form a crucial layer of defense against potential security threats, such as sensor spoofing, data interception, and unauthorized control. By implementing robust authentication and authorization protocols, UAV operators and developers enhance the overall security posture of UAV systems, contributing to safe and reliable operations [43]. Authentication and authorization are indispensable requirements in ensuring the security and reliability of UAVs. Authentication involves verifying the identity of users or systems interacting with the UAV, preventing unauthorized access and ensuring that commands and data originate from trusted sources. Authorization, on the other hand, regulates the access and permissions granted to authenticated entities, guaranteeing that only authorized personnel can carry out specific actions and access defined resources. However, these pre-requirements are critical in addressing potential threats such as sensor spoofing, blocked data encryption, and unauthorized control that may threaten UAV operation, thus endangering security. The study's resulting segments take into account a variety of validation attributes, such as multiple verifications and secure reinstatement processes, as well as approval norms such as role-based privileged access controls or security technical implementation guides, and granular permissions grants. These initiatives contribute to establishing a solid foundation for the UAV mission, mitigating potential vulnerabilities, and ensuring careful implementation with responsible use depending on different applications.

4.2. Security Threats

UAVs have a complex biological system that includes four specific levels: sensor level, hardware level, software level, and communication level [44]. A sensor-level design for UAVs relies on a variety of sensors, including cameras and inertial estimation units, to be able to see their surrounding elements. This is because sensor data must be reliable and intact to avoid acts of deception, which can result in navigational errors or compromised mission outcomes. The physical parts of the UAV, such as propulsion systems and control units, give hardware. The initial point of activity to preclude unauthorized modifications, alteration, or portion failures that could compromise flight safety would be through a secure equipment plan and access controls.

In the software level, UAVs operate on software and firmware, determining their behavior and functionality. Robust software security measures are essential to thwart potential cyber threats, unauthorized access, and software vulnerabilities. The communication level pertains to wireless data exchange between UAVs and ground control stations (GCS) and among UAVs in collaborative missions. Authentication and authorization are paramount in safeguarding UAVs and their levels from various potential threats [45]. Threats to authentication include unauthorized access to UAV systems, leading to the compromise of control and sensitive data. Additionally, attackers might exploit vulnerabilities in authentication protocols to impersonate legitimate users or devices, potentially gaining unauthorized control over UAVs. Authorization threats involve unauthorized entities accessing restricted functionalities or resources, potentially disrupting UAV operations. These threats can lead to unauthorized commands, sensor data manipulation, or even physical damage to the UAV. The research underscores the importance of countering these threats, with studies proposing solutions such as secure authentication mechanisms and fine-grained access control to mitigate potential risks. Figure 4 shows the attacks targeting UAVs for each level.

 doi:10.20944/preprints202403.0349.v1

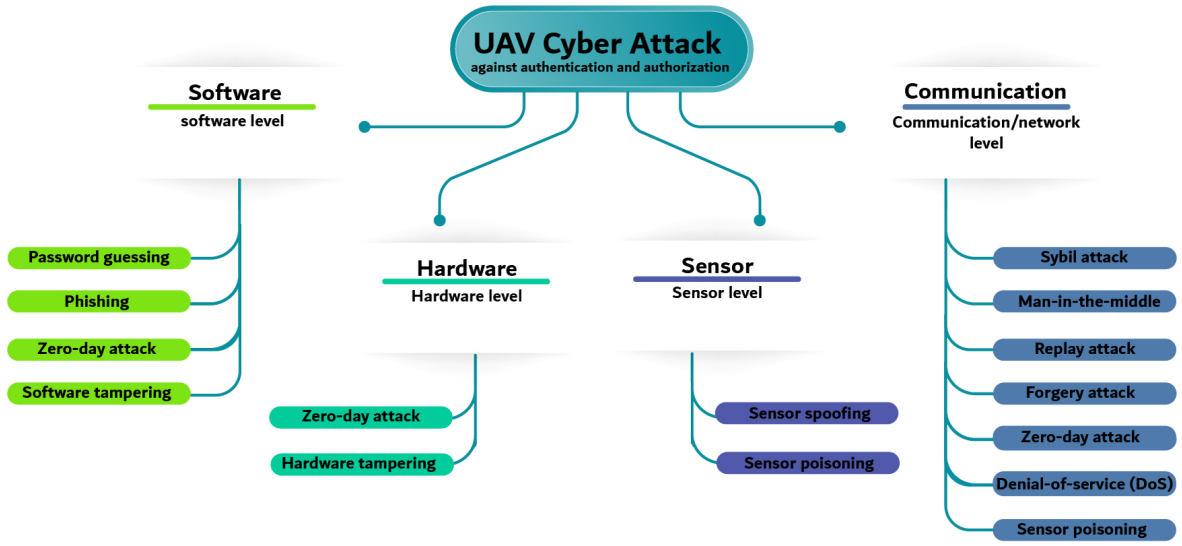

Figure 4. Attacks targeting UAVs for each level

4.3. Four Levels of UAV Security

In UAVs, security is an all encompassing mission. It extends far beyond the skies, delving into every facet of these autonomous flying machines. UAV security is typically categorized into four levels, each with priorities and measures. Let us embark on a comprehensive journey through these four levels, unveiling the intricacies and importance of each [44].

4.3.1. Hardware Security

For UAVs, physical security is their first line of protection. It has a variety of safeguards to protect the actual UAV and its parts from dangers like theft, tampering, or unauthorized access [46]. Imagine physical security as the fortress that houses the UAV, complete with moats, drawbridges, and impenetrable walls.

4.3.2. Software Security

Software security ensures that UAV missions are executed with the utmost security and precision. It's like the strategic planning and coordination required for a military campaign, ensuring that the UAV operates only in authorized airspace, follows predefined flight paths, and communicates securely with ground stations.

4.3.3. Communication/Network Security

Communication and network security are the guardian of the virtual pathways that connect the UAV to the GCS via antenna. It is concerned with securing the data transmitted between these two vital nodes in the UAV ecosystem. Think of it as the invisible shield that envelops the fortress, ensuring that no message or data is intercepted or tampered with during its journey [47].

4.3.4. Sensor Security

UAVs depend on utilizing sensors to collect data about their immediate environment, this information is critical and requires protection from malicious attackers. Compromised UAV sensors might result in the failure and malfunction of the UAV system. Table 7 outlines countermeasures at the UAVs levels, focusing on current approaches that can be employed to safeguard against assaults on UAVs.

 doi:10.20944/preprints202403.0349.v1

Table 7. Features of four UAV levels.

Level	Paper	Feature	Description
Hardware	[46]	Secure Storage	Protects UAV during non-operation. Fortified storage areas with surveillance and alarm systems to prevent hardware theft and unauthorized access.
	[46]	Biometric Locks	Restricts access to UAV hardware components. Only individuals with authorized biometric data (fingerprints or retinal scans) can interact with the UAV.
	[48]	Tamper-Evident Seals	Applied to critical components, similar to fortress drawbridges. Reveals signs of interference, alerting security personnel to potential breaches during storage or transport.
Software	[49]	Authorized Airspace	Ensures UAV adherence to designated airspace regulations and restrictions. Software security plans missions within authorized zones, preventing unintentional or intentional incursions.
	[50]	Predefined Flight Paths	UAV routes during missions are predefined, and software security ensures strict adherence to these paths, minimizing the risk of deviation or intrusion into unauthorized areas [50].
	[51]	Secure Communication with Ground Stations	Vital for UAV operations, software security ensures safe communication channels between the UAV and Ground Control Stations (GCS). Encryption, secure protocols, and frequency-hopping techniques protect data in transit [51].
Communication	[52]	Encryption	Foundation of communication security, transforms data into an unreadable format decipherable only by authorized recipients. End-to-end encryption ensures data security, even if intercepted [53].
	[53]	Secure Protocols	Utilizes secure communication protocols (e.g., TLS) for UAV and ground station data exchanges. Establishes secure connections to prevent eavesdropping or data manipulation [54].
	[54]	Frequency-Hopping Techniques	Involves rapidly and unpredictably changing communication frequencies. Enhances difficulty for malicious entities to intercept or jam UAV communication signals, ensuring data confidentiality [55].
Sensor	[55]	Detecting Unusual Signals	To detect GPS spoofing, observes anomalous signal power fluctuations, indicating a potential spoofing attempt. Cooperative data attestation method suggested for multiple UAV situations, validating shared data precision [56].
	[56]	Enable Autonomous Navigation	Mitigates jamming attempts by implementing a system facilitating autonomous navigation and self-directed movement in the absence of signal reception by the flight controller. Proposal presented by authors in [57].
	[57] [58].	Use of Machine Learning (ML)	Utilizes Intrusion Detection Systems (IDS) with ML algorithms to identify sensor-based attacks, whether familiar or unfamiliar [58] [59]. IDS systems gather training data from UAV onboard components, considering challenges related to energy and compute resources [59].

5. Internet of Battlefield Things Attacks

IoBT plays an important role in the military field, especially if integrated into UAV devices. Through it, commanders and soldiers benefit from obtaining important intelligence about the enemy. Drones first appeared in 1849, when Austrians assaulted Venice, Italy, with bombs containing unmanned balloons. Similar attacks occurred even during the American Civil War. Military drones were also utilized in the Cold War, World War I, World War II, the American Civil War, the Vietnam War, and the Balkans War [59]. The first aircraft drone was deployed for tactical reconnaissance during the

 doi:10.20944/preprints202403.0349.v1

Vietnam War. According to Armour and Ross [60], the employment of military drones in conflicts such as Iraq, Afghanistan, and Kosovo increased their effectiveness.

IoBT plays an important role in the military field, especially if integrated into UAV devices. Through it, commanders and soldiers benefit from obtaining important intelligence about the enemy. UAVs have been an essential component of military operations for several years, providing reconnaissance, surveillance, and, in some cases, offensive capabilities. Although useful, it is exposed to many attacks that make it vulnerable. Table 8 showing a number of real attacks that occurred on the Internet of Things on the battlefield with using ML/DL to mitigate the attacks. Implementing zero trust in military UAVs is critical for safeguarding sensitive data, maintaining operational integrity, and avoiding adversarial takeovers [59]. ZTA ensures that if a malicious actor successfully infiltrates the network, they would not be able to move laterally or access critical systems without the appropriate credentials and permissions [60].

Table 8. Table of Attacks on Military UAVs and IoBT.

Attack	Technology	Paper	Description
Black hole attack	IoBT Network	[61]	The paper used ML to analyze KmCtrust model, it is compination between ML and trust managment by trust in IoBT network to remove attack from the network
Inject false information attack	IoBT Network	[62]	Attacker try to inject false data in the IoBT nodes. The paper used ML algorithms based on the forward backward sweep method to increase in the quality of information
Impersonation and spectrum sensing data falsification attacks	IoBT Device	[63]	The paper used ML/DL with SpecForce, a security framework for IoBT spectrum sensors
Spoofing and jamming attacks	Military UAV	[64]	The paper reviews the methods of spoofing and how it can affect on IoBT and ways of preventing it by using ML.

6. Zero Trust in Internet of Battlefield Things

UAVs have revolutionized modern warfare, enabling military forces to perform reconnaissance, surveillance, and strike operations with unprecedented efficiency and precision. As military operations increasingly embrace network centric approaches, the Internet of Battlefield Things (IoBT) emerges as a transformative framework connecting UAVs and other military assets to enhance situational awareness and decision-making capabilities. However, integrating UAVs into the IoBT landscape brings new and sophisticated cybersecurity challenges, demanding innovative solutions to secure these critical assets. The zero trust model operates on a core principle: default distrust of any device or user, irrespective of their location or network. Instead, it requires continuous verification and authorization of entities trying to access resources, preventing potential cyber threats from exploiting trust assumptions and unauthorized access to sensitive data.

6.1. Analysis of the Internet of Battlefield Things and its Significance in Modern Operations

In the thrilling realm of modern military operations, a technological marvel has emerged to revolutionize the battlefield like never before; IoBT, a vast network connecting numerous intelligent devices, such as UAVs, seamlessly communicating with each other and sharing vital information [65].

At its core, IoBT is an interconnected web of intelligent sensors, actuators, and devices that operate with remarkable synergy. Their ingenuity lies in their ability to collect, analyze, and share

 doi:10.20944/preprints202403.0349.v1

real-time data, creating unparalleled situational awareness. IoBT allows military forces to make swift and informed decisions in the heat of combat.

Imagine the smooth moving of drones high above, surveilling the battlefield with unwavering focus. They feed critical intelligence back to the central command, forming a seamless data flow that empowers soldiers on the ground [66]. The significance of IoBT cannot be overstated. The golden key unlocks the doors to enhanced military capabilities, providing a tactical edge that was previously thought to be impossible.

Now, commanders have a panoramic view, which allows them to strategize and adapt with unparalleled precision. IoBT enables real-time decision-making that is agile, accurate, and effective, turning the tide of battles in favor of those who harness its potential. IoBT's reach extends far beyond the traditional realms of warfare. It embodies the spirit of innovation that continues to define the modern era. This transformative technology inspires those in the military and countless brilliant minds in the tech industry [67]. The most important point remains how this technology can be protected from enemy attacks, which is what we will explore in the following parts.

6.2. Zero Trust Security Model and Its Relevance in Securing UAVs

The zero trust security concept is a contemporary cybersecurity strategy that does away with conventional perimeter-based protections. Unlike older models that assumed trust within the network, zero trust treats every user, device, or application as potentially untrusted, regardless of location [68]. It continuously verifies identities and devices, granting access only per request. This dynamic and multi-layered approach ensures enhanced security by reducing the attack surface and preventing unauthorized access. UAVs operating in IoBT scenarios face unique security challenges due to their dynamic and distributed nature:

- Dynamic Networks: UAVs interact with various edge devices in fast changing environments. Zero Trust's continuous verification ensures that UAVs are granted access only to authorized resources in real time, reducing the risk of unauthorized infiltration [69].
- Protecting Sensitive Data: UAVs collect and transmit critical data, making them attractive cyberattack targets. Zero Trust prevents unauthorized access to this data, safeguarding its confidentiality and integrity during transmission and storage [70].
- Defense against hardware attacks: In IoBT environments, UAVs may be physically intercepted by adversaries. Zero Trust's continuous verification reduces the chances of attackers exploiting a captured UAV to gain unauthorized network access [68].
- Mitigating Insider Threats: Continuous monitoring in zero trust opens itself to detecting insider threats. Any abnormal behavior is seen and responded to quickly, resulting in interception of the activities plotted by malicious insiders that could violate security [69].
- Compliance and Auditing: zero trust provides comprehensive logs and auditing capabilities, essential in military and defense contexts, to ensure compliance with regulations and facilitate post-incident investigations.

6.3. Applying Zero Trust Concepts to UAVs

Incorporating zero trust concepts into UAV systems necessitates a robust framework for access control, ensuring that sensitive operations and data are shielded from unauthorized access. This paper contains three types of access control. of Role-Based Access Control (RBAC) serves as a foundational layer, restricting system privileges based on predefined roles within the UAV's operational protocol. Complementing RBAC, Attribute-Based Access Control (ABAC) adds a nuanced layer of security by considering a multitude of attributes, such as the context of access, the sensitivity of the data, and the state of the UAV, to make real-time access decisions. For mission-critical applications like battlefield surveillance, an access control protocol specifically tailored for Surveillance-IoT can be integrated, leveraging zero trust's rigorous verification processes to ensure that every access request is continuously validated, thus fortifying UAV networks against the evolving threats in dynamic and adversarial environments.

 doi:10.20944/preprints202403.0349.v1

6.3.1. Access Control Mechanisms

- **Role-based Access Control (RBAC)**

RBAC is a popular access control model vital in enhancing security and managing user privileges. When integrated into zero trust drone architecture, RBAC enables fine-grained control over user permissions, ensuring that only authorized individuals can access sensitive drone systems and data.

RBAC operates on the principle of assigning permissions based on predefined roles [71]. Each role represents a set of responsibilities and tasks within an organization or system. Users are then transferred to specific parts based on their job functions or duties. RBAC simplifies access management by associating permissions with roles rather than individual users, streamlining the process and reducing administrative overhead. When integrated into ZTA, RBAC strengthens the security posture of drone systems by enforcing strict access controls. The concept of least privilege allocates rights to users and correctly defines user roles. This means users are granted only the minimum privileges necessary to perform their functions and tasks. By limiting access rights, RBAC minimizes the potential impact of a compromised user account or device, mitigating the risks associated with unauthorized access or malicious activities.

RBAC within ZTA also enables efficient and centralized access control management. The defined roles and associated permissions are managed centrally, allowing administrators to easily add, modify, or revoke access privileges based on changes in user responsibilities or organizational requirements. This centralized management ensures consistency and reduces the likelihood of access control errors or unauthorized access.

Moreover, RBAC supports the segregation of duties, which is crucial for maintaining a separation of responsibilities and preventing conflicts of interest. RBAC enables the assignment of complementary roles to different individuals, ensuring that critical tasks require multiple authorized individuals to collaborate [72]. This segregation enhances accountability and reduces the likelihood of insider threats or unauthorized actions. Integrating RBAC into ZTA for drones also enhances audibility and accountability. RBAC provides a clear audit trail by associating user actions with their assigned roles and permissions. This traceability facilitates the identification of any security breaches or policy violations, enabling swift investigation and response.

- **Attribute-based Access Control (ABAC)**

ABAC is an advanced access control model that provides a flexible and dynamic approach to managing resource access. When integrated into ZTA for drones, ABAC enables access decisions based on various attributes, including user location, time, device characteristics, and other contextual factors. This attribute centric approach enhances the security of drone operations by providing dynamic and context-aware access control [73].

ABAC takes into consideration multiple attributes to make access decisions. These attributes can include user attributes (such as role, department, or clearance level), environmental attributes (such as location, time, or network status), and object attributes (such as the sensitivity or classification of the resource being accessed). The attributes define the ABAC policies because of their accurate and fine-tuned access permissions. Drone systems can implement context-aware access control by leveraging ABAC within ZTA. For example, access to sensitive drone control systems or data can be restricted based on the user's location. Access can be denied if a user attempts to access the drone system from an unauthorized area, preventing potential security breaches. Similarly, access permissions can be dynamically adjusted based on other attributes, such as the time of day or device type.

ABAC enhances security by providing dynamic access control mechanisms that adapt to changing circumstances. For instance, if a user's clearance level or the sensitivity of specific resources changes, access policies can be automatically adjusted. This ensures that access permissions align with the current security requirements, reducing the risk of unauthorized access or data breaches. Furthermore, ABAC enables attribute-based risk assessments. By considering attributes such as user behavior

 doi:10.20944/preprints202403.0349.v1

patterns or device health status, access decisions can be influenced by the perceived risk level associated with a specific attribute value. For example, if a user's behavior deviates from their usual patterns or a device is detected as compromised, access can be restricted, or additional authentication measures can be required to prevent potential security threats [74]. ABAC integration into ZTA also promotes interoperability and scalability. ABAC policies can be defined in a standardized format, such as the XACML (extensible Access Control Markup Language), allowing for interoperability across different systems and applications. Additionally, ABAC's flexible nature enables the scalability of access control policies as the drone ecosystem expands, accommodating new attributes and adapting to evolving security requirements [75].

Table 9. Access Control Mechanism.

Mechanisms	Feature	Description
Role-Based Access Control (RBAC)	Least privilege access: Evaluates and reevaluates a user's access based on context and adapts permissions accordingly	RBAC assigns permissions based on predefined roles, streamlining access management. In battlefield surveillance, roles could include operators, commanders, and analysts. For example, an operator may have access to live feeds, while an analyst may access historical data.
Attribute-Based Access Control (ABAC)	Evaluate several attributes for authorization decisions.	ABAC considers attributes such as user characteristics, environmental conditions, and resource properties for access decisions. In battlefield surveillance, ABAC can dynamically control access based on factors like location, mission status, and security clearance. For instance, an agent's access may change based on their location and the nature of the ongoing mission and system will look for any unusual or anomalous behavior.

- **Access Control Protocol for Battlefield Surveillance-IoT**

  ACPBS-IoT is an access control protocol specifically designed for battlefield surveillance within drone-assisted IoT environments. Zhang et al. [76] introduced this protocol in their article published in 2022, titled "Ac-cess Control Protocol for Battlefield Surveillance in Drone-Assisted IoT Environment" The primary aim of ACPBS-IoT is to mitigate several security challenges by employing several robust security techniques:

  - Symmetric encryption: all messages between the drones and the GCSs are encrypted using symmetric encryption, which makes it difficult for an adversary to eavesdrop on the communication.
  - Message authentication codes: message authentication codes are used to verify the authenticity of messages, which makes it difficult for an adversary to impersonate a legitimate drone or GSS.
  - Key freshness: the keys used for encryption and message authentication are refreshed periodically, which makes it difficult for an adversary to crack the keys.
  - Replay protection: a replay protection mechanism is used to detect and prevent replay attacks.

  ACPBS-IoT has undergone extensive security evaluations, both formal and informal. The formal analysis confirms the protocol's resilience against various potential attacks, including eavesdropping, impersonation, drone hijacking, and replay attacks. The informal analysis supports the protocol's defense against numerous practical attacks. ACPBS-IoT presents a promising solution for enhancing security in drone-assisted IoT environments for battlefield surveillance. It incorporates multiple security features to defend against diverse threats. Nonetheless, further real-world evaluations are necessary to fully validate the effectiveness of ACPBS-IoT in actual deployment scenarios.

 doi:10.20944/preprints202403.0349.v1

6.3.2. Authentication Mechanisms

- **Multi-Factor Authentication (MFA)**

MFA is a robust authentication mechanism that enhances the security of access to drone systems by requiring users to provide multiple authentication factors. When integrated into ZTA for drones, MFA ensures that only authenticated and authorized individuals can interact with the drone systems, adding an extra layer of protection to sensitive operations [4]. MFA combines two or more authentication factors to verify the identity of a user. These factors typically fall into knowledge, possession, and inherence. Knowledge factors include the user's ability, such as a password or PIN. Possession factors involve something the user possesses, such as a physical token or a mobile device. Inheritance factors are based on distinctive biological characteristics, such as fingerprints, iris scans, or facial recognition.

Drone systems can establish a robust authentication process by utilizing MFA within ZTA. Passwords, the most common used knowledge factor, are strengthened by requiring additional factors for authentication. For example, after entering a password, the user may need to provide a one-time password (OTP) generated by an authentication app on their mobile device or a physical token. This combination of factors significantly reduces the risk of unauthorized access, as an attacker must possess both the password and the additional authentication factor. Biometric factors add an extra layer of security to MFA. Drones can incorporate biometric authentication methods such as fingerprint, iris scans, or facial recognition. These unique biological traits provide a high level of assurance in verifying the user's identity. Integrating biometric authentication into MFA ensures that only authorized individuals with the correct biometric attributes can access the drone systems, further strengthening security [77].

Physical tokens, such as smart cards or hardware tokens, are possession factors that can be integrated into MFA for drones. These tokens generate dynamic authentication codes or digital signatures used with other elements to verify the user's identity. Physical tokens offer an additional layer of protection as they are not easily replicated or compromised. The integration of MFA into ZTA for drones brings several benefits. Firstly, it significantly increases the difficulty for attackers to gain unauthorized access, as they must possess multiple factors simultaneously. Secondly, MFA reduces the reliance on passwords alone, addressing the vulnerability of password-based authentication and minimizing the risk of password related security breaches. Moreover, MFA enhances the overall security posture of drone systems by adding a layer of defense against credential theft, phishing attacks, and social engineering attempts. Even if an attacker obtains one authentication factor, they would still be unable to access the system without the other required factors.

Table 10. Different authentication approaches and their various attacks.

Authentication Approach	Brute-Force Attack	Guess Attack	Phishing Attack	Spoofing Attack	Impersonation Attack	Apply on drone	Using zero trust	Ref.
Face Recognition	No	No	No	Yes	No	✓	✓	[78,79]
Fingerprint Scanner	No	No	No	Yes	No	✓	✓	[80,81]
Geographical Location	No	No	No	No	No		✓	[80]
Ocular-based Methods	No	No	No	No (retina) & Yes (iris)	No		✓	[78]
OTPs	No	No	Yes	No	Yes	✓	✓	[82,83]
Password/PIN	Yes	Yes	Yes	No	Yes	✓	✓	[81,84]
SmartPhone Applications	No	No	Yes	No	Yes	✓	✓	[84,85]
SmartCards	No	No	No	Yes	Yes	✓	✓	[85]
Thermal Image Recognition	No	No	No	No	No		✓	[78]
Vein Recognition	No	No	No	Yes	No		✓	[80,81]
Voice Recognition	No	No	No	Yes	No		✓	[80]

- **Certificate-based Authentication**

Certificate-based authentication is a robust method that utilizes digital certificates to verify the identities of devices and users. Certificate-based authentication can be used in ZTA for drones to provide secure communication channels while preventing unauthorized access to drone systems. Certificate-based authentication relies on X.509 certificates, widely adopted in PKI systems. These

 doi:10.20944/preprints202403.0349.v1

certificates contain the entity's public key, digital signature, and other identifying details. They are a dependable way to confirm the legitimacy and integrity of the communicating parties and are issued by a reputable certificate authority (CA) [86].

In the case of drone systems, certificate-based authentication ensures that only trusted and authorized devices and users can access and interact with the drone systems. Each user or device is issued a unique digital certificate as a digital credential. When attempting to connect with the drone system, the machine or user presents their certificate as proof of identity [87]. The drone system, acting as the verifier, checks the presented certificate against a trusted CA's certificate store. If the presented certificate is valid and trusted, the authentication process proceeds, allowing the device or user to access the drone system. This authentication mechanism ensures that only entities with valid and recognized certificates can communicate with the drone system, mitigating the risk of unauthorized access. Certificate-based authentication offers several advantages within the zero trust framework for drones. Firstly, it provides a strong level of assurance regarding the identity of the communicating parties. The use of digital certificates, coupled with the rigorous validation process against trusted CAS, ensures that the entities interacting with the drone system are indeed whom they claim to be.

Furthermore, certificate-based authentication enables secure communication channels between the drone system and other devices or users [86]. Public-key cryptography within the certificates facilitates establishing encrypted connections, protecting the confidentiality and integrity of the data transmitted between the entities. This ensures that sensitive information, such as control commands or telemetry data, remains protected from unauthorized interception or tampering. Additionally, certificate-based authentication supports the scalability and manageability of authentication in large-scale drone deployments. By relying on standardized digital certificates, issuing, revoking, and managing credentials becomes more streamlined. Certificates can be centrally managed and easily updated or withdrawn as needed, enabling for effective access control management in dynamic and evolving drone environments.

Table 11. Authentication Factor.

Authentication Factor	**MFA (Multi-Factor Authentication)**	**Certificate-Based Authentication**
Description	Enhances security by requiring users to provide multiple authentication factors before gaining access.	Relies on digital certificates issued to users or devices, utilizing Public Key Infrastructure (PKI) for secure communication.
Factors Used	- Something You Know (Password or PIN) - Something You Have (Temporary code from a mobile app or hardware token) - Something You Are (Biometric data like fingerprints or facial recognition)	- Something You Have (Digital certificate issued by a Certificate Authority) - Something You Are (Authentication based on cryptographic keys)
Security Strength	Provides a high level of security by adding layers of verification, reducing the risk of unauthorized access.	Offers robust security, especially in environments where strong identity verification is essential.
Suitability	Well-suited for environments requiring strong user authentication, such as military systems or confidential databases.	Highly suitable for secure communication channels, military networks, or any context where rigorous identity validation is critical.
Ease of Use	Depending on factors used, may involve additional steps for users, but advancements like biometrics improve user experience.	Requires the management and deployment of digital certificates, which can be seamless once set up but may involve initial configuration complexities.

 doi:10.20944/preprints202403.0349.v1

6.4. How Zero Trust Enhance the Security Posture of UAVs

The trust security model is effective in helping solve the issues of UAV security. The significance of zero trust in assuring battlefield effectiveness and resilience is explored below, including UAV attacks by hostile actors, attacks via unauthorized access accounts, and data breaches.

1. **Preventing Malicious Actors:** It is like military operations, coupled with the fact that in combat, every second counts; one hundred seconds can spell disaster or even death, being half a minute away. The zero trust narrative of "never trust, always verify" provides proactive protection against such attacks. Through continuous verification of personal users and device identities, zero trust guarantees that only authorized individuals can initiate connections with UAV networks. Using robust authentication approaches such as biometrics and MFA, which prevent access attempts by intruders or unauthorized persons nefariously trying to break in, provides the zero trust policy with insights into improving UAV security. In addition, anomaly detection and behavioral analysis increase the effectiveness of its early identification function to create a barrier against malicious intruders that would jeopardize UAV operational reliability [47].
2. **Mitigating Unauthorized Access:** In fighting conditions, the unauthorized network surrounds everywhere. In fight circumstances, the UAVs are often based and connected to robust and unfettered system segments that increase accessibility toward unauthorized consumers. Zero Trust's identification-based access controls play a significant role in mitigating this risk. All entrance requests are continuously surveyed to ensure that users and devices are checked out and verified so that legitimate owners can access UAV services. Moreover, the "least privilege" aspect of zero trust protects only those resources required to complete certain operations. This approach minimizes potential attack surfaces, making it significantly harder for adversaries to move laterally within UAV networks. By enforcing the principle of least privilege, zero trust mitigates the risk of unauthorized users gaining undue access to critical resources [88].
3. **Safeguarding Against Data Breaches:** UAVs capture and transmit a wealth of sensitive information; making data breaches a significant concern. Zero Trust's continuous verification and dynamic policy enforcement significantly reduce the likelihood of data breaches. Real-time monitoring and context-aware access controls ensure that data is only accessible to authorized recipients and protected from unauthorized interception. Dynamic policy enforcement also adapts to changing conditions, adjusting access privileges based on real-time context. This responsiveness ensures that UAV networks maintain optimal security even in rapidly evolving battlefield scenarios. With zero trust's strong emphasis on data protection, UAVs can confidently execute missions, knowing their valuable data remains secure [89].

6.5. Safeguarding UAV Communication and Data

Secure communication becomes paramount as UAVs integrate into the IoBT.

1. Protecting Sensitive Data: UAVs are deployed to gather and transmit sensitive information, including real-time video feeds, aerial imagery, and strategic intelligence. The security of this data is of utmost importance as it could contain classified information that, if intercepted, may jeopardize military operations or compromise national security. Secure communication channels, implemented through encryption and robust cryptographic protocols, are vital in safeguarding the integrity and confidentiality of data during transmission. By encrypting the data, UAVs can ensure that it remains indecipherable to unauthorized entities even if intercepted. This proactive measure minimizes the risk of data breaches and ensures that sensitive information remains accessible only to authorized recipients [90].
2. Ensuring Data Integrity: UAVs often transmit data through dynamic and interconnected networks, exposing them to potential risks such as data tampering and man-in-the-middle attacks. Only authorized data manipulation can lead to accurate decision-making and critical mission failures. To mitigate such threats, secure communication channels utilize digital signatures and

 doi:10.20944/preprints202403.0349.v1

integrity checks to verify data's authenticity and unaltered nature during transmission. By ensuring data integrity, UAVs can confidently rely on the accuracy and trustworthiness of received information, enhancing the effectiveness of their missions in dynamic and hostile environments [87].

3. Securing Mission-Critical Commands: UAVs receive mission-critical commands from remote operators or automated systems. The consequences of unauthorized access or interception of these commands can be catastrophic, potentially leading to the loss of control or manipulation of UAVs. Secure communication ensures the confidentiality and authenticity of mission-critical commands, preventing unauthorized access or tampering. More importantly, a security protocol, that serves in securing the communication between UAVs and GCS, is proposed. Strong authentication and access controls guarantee that only authorized entities can issue orders, bolstering the UAVs' reliability and trustworthiness in executing critical tasks.

6.6. Strengthening UAV Security: Implementing Zero Trust Principles in the IoBT

A comprehensive zero trust approach is essential to safeguard against attacks and unauthorized access. This article delves into the critical components of securing UAVs in the IoBT using the zero trust model.

1. Device Authentication: Implementing robust device authentication mechanisms is fundamental to establishing trust within the IoBT network. Each drone must be equipped with unique digital certificates and device identifiers, making it possible to identify and validate its authenticity during the connection process. Secure boot processes ensure that only genuine and untampered software can run on the UAV, mitigating the risk of compromised firmware or software [91].
2. Data Encryption: Data transmitted between drones and GCS must be encrypted using robust encryption protocols to prevent unauthorized interception and tampering. End-to-end encryption guarantees that intercepted data remains unintelligible unless accompanied by the requisite decryption keys. protecting sensitive information from falling into the wrong hands [92].
3. Continuous Monitoring: Real-time monitoring is indispensable in detecting anomalies and suspicious activities in the IoBT network. By constantly analyzing drone activities and network traffic, security teams can swiftly respond to potential threats, unauthorized access attempts, abnormal data transfers, and deviations from expected flight patterns. Early detection allows for proactive mitigation measures [93].
4. Segmentation and Micro-segmentation: Dividing the network into logical segments and applying granular access controls significantly reduces the attack surface and minimizes the lateral movement of attackers in case of a breach. Micro-segmentation ensures that each piece is fortified with its access permissions, limiting the scope of any potential infringement and containing it effectively [94].
5. Identity and Access Management (IAM): A robust IAM strategy is vital for managing user and device identities within the IoBT. Implementing rigorous password policies, RBAC, and MFA ensures that only authorized personnel can control or interact with drones, significantly reducing the risk of unauthorized access [95].
6. Secure Communication Protocols: Secure communication protocols such as Secure Shell (SSH) or TLS should be employed to exchange commands, telemetry, and other data between drones and GCS. Encrypting communication channels prevents eavesdropping and ensures that transmitted data remains confidential and unchanged during transmission [96].
7. Secure Firmware and Software Updates: Establishing a secure process for applying firmware and software updates is critical to prevent potentially malicious code injection. Verifying the integrity and authenticity of updates before deployment minimizes the risk of compromising drone systems with malware or unauthorized modifications [97].
8. Incident Response and Recovery: A comprehensive incident response plan is essential to swiftly and efficiently address security breaches or compromises. This plan should outline clear steps

 doi:10.20944/preprints202403.0349.v1

for isolating compromised drones, conducting forensics to identify the source of the attack, and safely returning operations to normalcy [98].

9. Compliance and Regulations: Compliance with relevant regulations, guidelines, and standards is crucial for UAV operations and security. The IoBT network can maintain a strong security posture and protect itself from potential legal and operational repercussions by aligning its zero trust implementation with aviation authorities' regulations and industry organizations' best practices.

Table 12. Comparison of Selected Papers in Drone.

Features	Our paper	Dong et al. [4]	Nour [38]	Ramezanpour et al. [39]	Keshavarz et al. [40]	Kurunathan et al. [41]	Fang at al.[42]
Model or Framework	✓	✓	✓	✓	✓	✓	✓
Security and Privacy	✓	✓	✓	✓	✓	✓	✓
Challenges	✓	✓	✓	✓	✓	✓	✓
Components	✓	✗	✗	✗	✗	✓	✗
Internet of Things	✓	✓	✓	✓	✗	✓	✓
Military sector	✓	✗	✗	✗	✗	✗	✗
Mechanism	✓	✗	✓	✓	✓	✓	✓

7. Future Direction

This section provides a concise overview of our results about the effective implementation of ZTA and highlights the areas where there is a lack of knowledge in the current state-of-the-art approaches. Zero Trust requires a detailed and context-aware access restriction. Usage-based access control is a method that can fulfill these access control needs, as indicated by the literature. Nevertheless, diverse IoT-enabled environments exhibit distinct access control prerequisites, necessitating varied configurations of access control components. Blockchain is increasingly being considered as a potential solution for distributed access control. Nevertheless, the usage of blockchain in this field is still in its early stages due to its reliance on a consensus mechanism, which makes it less appealing compared to conventional centralized systems. It is advisable to use a risk-aware access control system that combines the features of fine-grained access control schemes like (RBAC) and (ABAC) .

Although authentication technologies have been widely adopted and utilized, there are still certain aspects of authentication that have not been entirely achieved. The majority of user authentication systems, including passwords, fingerprints, facial recognition, and iris scans, possess weaknesses. Multi-factor authentication (MFA) is widely supported, although most MFA solutions require a secondary device, such as a cell phone, and demand significant of user effort. The presence of these criteria hinders the extensive use of MFA solutions. Therefore, it is necessary to find solutions that need minimal user involvement. Hence, there is a need for MFA solutions that do not rely on a secondary device and demand minimal user interaction. Consequently, novel approaches to authentication are currently being sought.

Increased security and resilience of IoBT devices and networks is a major expected outcome of using the zero trust Model in the IoBT industry. The traditional perimeter-based security approach is no longer sufficient in the face of emerging technologies such as 5G, IoT, and blockchain, which are transforming the battlefield environment [99]. By adopting a zero trust strategy, which asserts that no entity—user, app, service, or device—should be trusted by default, IoBT systems can benefit from a more robust and adaptive security posture. This approach includes network micro-segmentation, which can be seamlessly integrated into existing environments, and sophisticated reputation-based trust models for detecting malicious nodes. As a result, IoBT networks will be better equipped to withstand a variety of threats, ensuring the integrity and availability of critical battlefield assets [100].

Expected outcome of using the zero trust Model in the IoBT industry is the improved protection of sensitive data and information. In data-sensitive applications such as IoBT and IoMT, securing data, systems, and devices while safeguarding the privacy of both the data and data subjects, is of paramount importance. These procedures remain tiring for users, but give more protection to the system, especially when we talk about the military field. A trust model crafted to determine the

 doi:10.20944/preprints202403.0349.v1

level of trust and whether sharing data can significantly enhance data protection in IoBT networks [101]. Furthermore, deception-based schemes can be employed to enhance the location information security of IoBT nodes, as well as novel encryption methods for securing sensitive data [102]. By implementing these advanced security measures, the IoBT industry can effectively safeguard mission-critical information, ultimately contributing to the success of military operations [103].

Enhanced trust and confidence in IoBT industry products and services is another anticipated outcome of integrating the zero trust Model into IoBT systems. As the Internet of Battlefield Things continues to evolve, delivering intelligence services on the battlefield to commanders and soldiers, it is crucial that users have faith in the reliability and security of these advanced technologies [104]. By adhering to the principle of zero trust, which states that no entity—user, app, service, or device—should be trusted by default, the IoBT industry can build and maintain trust among its stakeholders.This covers the integration of multi-tier security mechanisms beyond traditional perimeter-oriented methods and Cisco's zero trust platform, which is renowned for securing hybrid work environments, easing compliance, and minimizing ransomware danger. By creating an environment of trust and openness by improving the IoBT industry, we can provide a more comprehensive adoption nature for its innovative products or services so that it will help enhance overall military capabilities.

8. Conclusion

In conclusion, the deployment of this novel approach is revolutionary for UAVs and allows it to improve the security and resilience of these priceless entities' sentiments towards a range industry, including the public sector, commercial military, and private sector, with the use of ZTA. Such dangerous threats, such as potential malicious attacks, unauthorized access, or data breaches, can be substantially reduced with the use of zero trust's core principles, which are the elimination of implicit trust, enforcement of least privilege, and ongoing actual monitoring & analytics to develop highly secured UAV. No matter where a user is located or the source of that per-son's authority. A multi-layered security strategy applies strict identification requirements and lots every User Client Device Application before authorizing them access. The following strategy is crucial in the widespread and dynamic operating environment in which UAVs can be employed, such as IoBT. ZTA allows granular control of access permissions due to security mechanisms such as ABAC, RBAC, and ACPBS-IoT. It does so because the system's architecture can adapt to the needs and pointers of unpiloted air vehicles as they continue developing. Additional authentication types, including certificate-based, MFA and grant access, allow only authorized users with the required characteristics to communicate with UAV systems. This paper presents a comprehensive description of zero trust and how it can help to protect IoBT environment. To ensure confidentiality of sensitive data and mission-critical orders, UAV operations require secure channels between communication points and their data processing integrity by using ZTA.

Acknowledgments: This work was made possible in part by a grant from the university, which allowed us to conduct the research and collect the necessary data. This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT ...].

Conflicts of Interest: All authors declare no conflict of interest.

Nomenclature

ZTA	Zero Trust Architecture
UAV	Unmanned Aerial Vehicle
IoBT	Internet of Battlefield Things
SLR	Systematic Literature Review
GCS	Ground Control Station
ML	Machine Learning
IAM	Identity and Access Management
DDoS	Distributed Denial-of-Service

 doi:10.20944/preprints202403.0349.v1

NIST	National Institute of Standards and Technology
IDS	Intrusion detection system
PE	Policy Engine
PA	Policy Administrator
PEP	Policy Enforcement Point
SIEM	Security Information and Event Management
TA	Trust Algorithm
i-ZTA	Intelligent zero trust architecture
MFA	Multifactor Authentication
DDoS	Distributed Denial-of-Service
MITM	Man-In-The-Middle
GPS	Global Positioning System
PKI	Public Key Infrastructure
IoT	Internet of Things
TLS	Transport Layer Security
RBAC	Role-Based Access Control
ABAC	Attribute-Based Access Control
ACPBS-IoT	Access Control Protocol for Battlefield Surveillance-IoT
CA	Certificate Authority
SSI	Self-Sovereign Identity

References

1. Yang, D.; Zhao, Y.; Wu, K.; Guo, X.; Peng, H. An efficient authentication scheme based on Zero Trust for UAV swarm. *2021 International Conference on Networking and Network Applications (NaNA)* **2021**. doi:10.1109/nana53684.2021.00068.
2. Keshavarz, M.; Shamsoshoara, A.; Afghah, F.; Ashdown, J. A real-time framework for trust monitoring in a network of unmanned aerial vehicles. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* **2020**. doi:10.1109/infocomwkshps50562.2020.9162761.
3. Rani, C.; Modares, H.; Sriram, R.; Mikulski, D.; Lewis, F.L. Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* **2015**, *13*, 331–342. doi:10.1177/1548512915617252.
4. Dong, C.; Jiang, F.; Chen, S.; Liu, X. Continuous authentication for UAV delivery systems under Zero-Trust Security Framework. *2022 IEEE International Conference on Edge Computing and Communications (EDGE)* **2022**. doi:10.1109/edge55608.2022.00027.
5. Shafique, A.; Mehmood, A.; Elhadef, M. Survey of security protocols and vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 46927–46948. doi:10.1109/access.2021.3066778.
6. Penmetsa, S.; Minhuj, F.; Singh, A.; Omkar, S. Autonomous UAV for suspicious action detection using pictorial human pose estimation and classification. *ELCVIA Electronic Letters on Computer Vision and Image Analysis* **2014**, *13*, 18. doi:10.5565/rev/elcvia.582.
7. Mad'ar, T. STIENNON, Richard. There Will Be Cyberwar: How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar. *Obrana A Strategie (defence and Strategy)* **2017**, *17*, 161–163.
8. Mukhandi, M.; Damião, F.; Granjal, J.; Vilela, J.P. Blockchain-based Device Identity Management with Consensus Authentication for IoT Devices. *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)* **2022**, pp. 433–436.
9. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access* **2022**, *10*, 57143–57179. doi:10.1109/access.2022.3174679.
10. Zero Trust Architecture: NIST Publishes SP 800-207. National Institute of Standards and Technology, 2020.
11. Moffa, A. Implementing zero-trust to IOT solutions, 2024.
12. Canada, H. Securing a new Digital World with Zero trust, 2021.
13. Bhattacharjya, S. A novel zero-trust framework to secure IOT Communications, 2020.
14. Morel, A.E.; Kavzak Ufuktepe, D.; Ignatowicz, R.; Riddle, A.; Qu, C.; Calyam, P.; Palaniappan, K. Enhancing network-edge connectivity and computation security in drone video analytics. *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)* **2020**. doi:10.1109/aipr50011.2020.9425341.

15. Feng, Y.; Li, M.; Zeng, C.; Liu, H. Robustness of internet of battlefield things (IoBT): A directed network perspective. *Entropy* **2020**, *22*, 1166. doi:10.3390/e22101166.
16. Kindervag, J. Build security into your network's DNA: The Zero Trust Network Architecture, 2010.
17. DeCusatis, C.M.; Liengtiraphan, P.; Sager, A.; Pinelli, M. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. *2016 IEEE International Conference on Smart Cloud (SmartCloud)* **2016**, pp. 5–10.
18. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero trust architecture* **2020**. doi:10.6028/nist.sp.800-207-draft2.
19. Solodov, A.A.; Williams, A.D.; Hanaei, S.A.; Goddard, B. Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities. *Security Journal* **2018**, *31*, 305–324.
20. Awan, S.M.; Azad, M.A.; Arshad, J.; Waheed, U.; Sharif, T. A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. *Inf.* **2023**, *14*, 129.
21. Hale, B.; Van Bossuyt, D.L.; Papakonstantinou, N.; O'Halloran, B. A zero-trust methodology for security of Complex Systems with machine learning components. *Volume 2: 41st Computers and Information in Engineering Conference (CIE)* **2021**. doi:10.1115/detc2021-70442.
22. Phiayura, P.; Teerakanok, S. A comprehensive framework for migrating to zero trust architecture. *IEEE Access* **2023**, *11*, 19487–19511. doi:10.1109/access.2023.3248622.
23. Kerman, A. Zero trust cybersecurity: "never trust, always verify", 2023.
24. Ferretti, L.; Magnanini, F.; Andreolini, M.; Colajanni, M. Survivable zero trust for cloud computing environments. *Computers & Security* **2021**, *110*, 102419. doi:10.1016/j.cose.2021.102419.
25. Alagappan, A.; Venkatachary, S.K.; Andrews, L.J. Augmenting Zero trust network architecture to enhance security in virtual power plants. *Energy Reports* **2022**, *8*, 1309–1320. doi:10.1016/j.egyr.2021.11.272.
26. Macri, K. What is Zero trust? Federal Agencies Embrace Cybersecurity Innovation, 2021.
27. Embrace proactive security with Zero Trust.
28. Finn, R.L.; Wright, D. Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Comput. Law Secur. Rev.* **2012**, *28*, 184–194.
29. Waharte, S.; Trigoni, A. Supporting Search and Rescue Operations with UAVs. *2010 International Conference on Emerging Security Technologies* **2010**, pp. 142–147.
30. Journal of Intelligent & Robotic Systems manuscript No. (will be inserted by the editor) An Unmanned Aircraft System for Automatic Forest Fire Monitoring and Measurement.
31. Quaritsch, M.; Kruggl, K.; Wischounig-Strucl, D.; Bhattacharya, S.; Shah, M.; Rinner, B. Networked UAVs as aerial sensor network for disaster management applications. *e & i Elektrotechnik und Informationstechnik* **2010**, *127*, 56–63.
32. Gómez-Candón, D.; Castro, A.I.; López-Granados, F. Assessing the accuracy of mosaics from unmanned aerial vehicle (UAV) imagery for precision agriculture purposes in wheat. *Precision Agriculture* **2014**, *15*, 44–56.
33. Ham, Y.; Han, K.K.; Lin, J.J.; Golparvar-Fard, M. Visual monitoring of civil infrastructure systems via camera-equipped Unmanned Aerial Vehicles (UAVs): a review of related works. *Visualization in Engineering* **2016**, *4*, 1–8.
34. Bemis, S.P.; Micklethwaite, S.; Turner, D.; James, M.R.; Akciz, S.O.; Thiele, S.T.; Bangash, H.A. Ground-based and UAV-Based photogrammetry: A multi-scale, high-resolution mapping tool for structural geology and paleoseismology. *Journal of Structural Geology* **2014**, *69*, 163–178.
35. Bracken-Roche, C.; Lyon, D.H.; Mansour, M.; Molnar, A.; Saulnier, A.; Thompson, S. Surveillance drones: privacy implications of the spread of unmanned aerial vehicles (UAVs) in Canada. 2014.
36. Fleureau, J.; Galvane, Q.; Tariolle, F.L.; Guillotel, P. Generic Drone Control Platform for Autonomous Capture of Cinema Scenes. *Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use* **2016**.
37. Finn, A.; Scheding, S. Developments and Challenges for Autonomous Unmanned Vehicles - A Compendium. Intelligent Systems Reference Library, 2010.
38. Nour, M.G. Implementing Machine Learning to Achieve Dynamic Zero-Trust Intrusion Detection Systems (ZT-IDS) in 5G Based IoT Networks. PhD thesis, The George Washington University, 2023.
39. Ramezanpour, K.; Jagannath, J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks* **2022**, *217*, 109358.

40. Keshavarz, M.; Shamsoshoara, A.; Afghah, F.; Ashdown, J. A real-time framework for trust monitoring in a network of unmanned aerial vehicles. IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2020, pp. 677–682.
41. Kurunathan, H.; Huang, H.; Li, K.; Ni, W.; Hossain, E. Machine learning-aided operations and communications of unmanned aerial vehicles: A contemporary survey. *IEEE Communications Surveys & Tutorials* **2023**.
42. Fang, L.; Wu, C.; Kang, Y.; Ou, W.; Zhou, D.; Ye, J. Zero-Trust-Based Protection Scheme for Users in Internet of Vehicles. *Security and Communication Networks* **2022**.
43. Ko, Y.; Kim, J.; Duguma, D.G.; Astillo, P.V.; You, I.; Pau, G. Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone. *Sensors (Basel, Switzerland)* **2021**, *21*.
44. Mekdad, Y.; Aris, A.; Babun, L.; Fergougui, A.E.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A survey on security and privacy issues of uavs. *Computer Networks* **2023**, *224*, 109626. doi:10.1016/j.comnet.2023.109626.
45. Abro, G.E.M.; Zulkifli, S.A.; Masood, R.J.; Asirvadam, V.S.; Laouti, A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones* **2022**.
46. Pirker, D.; Fischer, T.; Lesjak, C.H.; Steger, C. Global and Secured UAV Authentication System based on Hardware-Security. *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* **2020**, pp. 84–89.
47. Krichen, L.; Fourati, M.; Fourati, L.C. Communication Architecture for Unmanned Aerial Vehicle System. *Ad-hoc, Mobile, and Wireless Networks* **2018**, p. 213–225. doi:10.1007/978-3-030-00247-3_20.
48. Allan, B.M.; Ierodiaconou, D.; Hoskins, A.J.; Arnould, J.P.Y. A Rapid UAV Method for Assessing Body Condition in Fur Seals. *Drones* **2019**.
49. LaFlamme, M. Traffic: Authorizing Airspace, Appifying Governance. 2020.
50. Nguyen, D.D.; Rohacs, J.; Rohacs, D. Autonomous flight trajectory control system for drones in Smart City Traffic Management. *ISPRS International Journal of Geo-Information* **2021**, *10*, 338. doi:10.3390/ijgi10050338.
51. Agron, D.J.; Ramli, M.R.; Lee, J.M.; Kim, D.S. Secure Ground Control Station-based routing protocol for UAV Networks. *2019 International Conference on Information and Communication Technology Convergence (ICTC)* **2019**. doi:10.1109/ictc46691.2019.8939885.
52. Cecchinato, N.; Toma, A.; Drioli, C.; Oliva, G.; Sechi, G.; Foresti, G.L. A Secure Real-time Multimedia Streaming through Robust and Lightweight AES Encryption in UAV Networks for Operational Scenarios in Military Domain. *Procedia Computer Science* **2022**.
53. Vadlamudi, S.R.; Bharathy, D.A.M.V.; Rani, S.; Vadlamudi. DESIGN AND DEVELOPMENT OF A SECURE DATA TRANSMISSION PROTOCOL FOR UAV. *europeanchemicalbulletin* **2023**.
54. Ye, J.; Zou, J.; Gao, J.; Zhang, G.; Kong, M.; Pei, Z.; Cui, K. A New Frequency Hopping Signal Detection of Civil UAV Based on Improved K-Means Clustering Algorithm. *IEEE Access* **2021**, *9*, 53190–53204.
55. Abera, T.; Bahmani, R.; Brasser, F.; Ibrahim, A.; Sadeghi, A.R.; Schunter, M. DIAT: Data Integrity Attestation for Resilient Collaboration of Autonomous Systems. *Proceedings 2019 Network and Distributed System Security Symposium* **2019**.
56. Wu, A.; Johnson, E.N.; Kaess, M.; Dellaert, F.; Chowdhary, G.V. Autonomous Flight in GPS-Denied Environments Using Monocular Vision and Inertial Sensors. *J. Aerosp. Inf. Syst.* **2010**, *10*, 172–186.
57. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. Novelty-based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles. *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks* **2020**.
58. Arthur, M.P. Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS. *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)* **2019**, pp. 1–5.
59. Glade, D. Unmanned Aerial Vehicles: Implications for Military Operations. 2012.
60. Xiaoning, Z. Analysis of military application of UAV swarm technology. *2020 3rd International Conference on Unmanned Systems (ICUS)* **2020**, pp. 1200–1204.
61. Rutravigneshwaran, P.; Anitha, G. Security model to mitigate black hole attack on internet of battlefield things (IoBT) using trust and K-means clustering algorithm. *International Journal of Computer Networks and Applications* **2023**, *10*, 95. doi:10.22247/ijcna/2023/218514.
62. Abuzainab, N.; Saad, W. Misinformation Control in the Internet of Battlefield Things: A Multiclass Mean-Field Game. 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–7. doi:10.1109/GLOCOM.2018.8647236.

63. Sánchez, P.M.; Celdrán, A.H.; Bovet, G.; Pérez, G.M.; Stiller, B. SpecForce: A Framework to secure IOT spectrum sensors in the internet of battlefield things. *IEEE Communications Magazine* **2023**, *61*, 174–180. doi:10.1109/mcom.001.2200349.
64. Tugsad Seferoglu, K.; Serdar Turk, A. Review of Spoofing and Jamming Attack on the Global Navigation Systems Band and Countermeasure. 2019 9th International Conference on Recent Advances in Space Technologies (RAST), 2019, pp. 513–520. doi:10.1109/RAST.2019.8767871.
65. Cavender, C. The internet of battlefield things is changing connector designs, 2019.
66. Miller, K.; O'Halloran, B.; Pollman, A. Securing the Internet of Battlefield Things While Maintaining Value to the Warfighter, 2019.
67. Popescu, F.C. From the IoT to the IoBT. The Path to Superior Situational Understanding. *Land Forces Academy Review* **2019**, *24*, 276 – 282.
68. Alawneh, M.; Abbadi, I.M. Integrating Trusted Computing Mechanisms with Trust Models to Achieve Zero Trust Principles. *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* **2022**, pp. 1–6.
69. Zeng, R.; Li, N.; Zhou, X.; Ma, Y. Building A Zero-trust Security Protection System in The Environment of The Power Internet of Things. *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)* **2021**, pp. 557–560.
70. Gao, P.; Yan, L.; Chen, Z.; Wei, X.; Guo, L.; Shi, R. Research on Zero-Trust Based Network Security Protection for Power Internet of Things. *2021 IEEE 4th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)* **2021**, pp. 458–461.
71. Gofman, M.I.; Luo, R.; Solomon, A.C.; Zhang, Y.; Yang, P.; Stoller, S.D. RBAC-PAT: A Policy Analysis Tool for Role Based Access Control. International Conference on Tools and Algorithms for Construction and Analysis of Systems, 2009.
72. Jeong, H.J.; guk Ha, Y. RBAC-Based UAV Control System for Multiple Operator Environments. 2012.
73. Hu, V.C.; Ferraiolo, D.F.; Kuhn, R.; Schnitzer, A.; Sandlin, K.; Miller, R.; Scarfone, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. 2014.
74. Alohaly, M.; Balogun, O.; Takabi, D. Integrating Cyber Deception Into Attribute-Based Access Control (ABAC) for Insider Threat Detection. *IEEE Access* **2022**, *10*, 108965–108978.
75. Zhang, Y.; Zhang, B. A new testing method for XACML 3.0 policy based on ABAC and data flow. *2017 13th IEEE International Conference on Control & Automation (ICCA)* **2017**, pp. 160–164.
76. Bera, B.; Das, A.K.; Garg, S.; Piran, M.J.; Hossain, M.S. Access Control Protocol for Battlefield Surveillance in Drone-Assisted IoT Environment. *IEEE Internet of Things Journal* **2021**, *9*, 2708–2721.
77. Patel, S.B.; Kheruwala, H.A.; Alazab, M.; Patel, N.S.; Damani, R.; Bhattacharya, P.; Tanwar, S.; Kumar, N. BioUAV: blockchain-envisioned framework for digital identification to secure access in next-generation UAVs. *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond* **2020**.
78. Otta, S.P.; Panda, S.; Gupta, M.; Hota, C. A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet* **2023**, *15*. doi:10.3390/fi15040146.
79. Liu, S.; Song, Y.; Zhang, M.; Zhao, J.; Yang, S.; Hou, K. An Identity Authentication Method Combining Liveness Detection and Face Recognition. *Sensors* **2019**, *19*. doi:10.3390/s19214733.
80. Jaikla, T.; Pichetjamroen, S.; Vorakulpipat, C.; Pichetjamroen, A. A Secure Four-factor Attendance System for Smartphone Device. 2020, pp. 65–68. doi:10.23919/ICACT48636.2020.9061431.
81. Adiraju, R.V.; Masanipalli, K.K.; Reddy, T.D.; Pedapalli, R.; Chundru, S.; Panigrahy, A.K. An extensive survey on finger and palm vein recognition system. *Materials Today: Proceedings* **2021**, *45*, 1804–1808. International Conference on Advances in Materials Research - 2019, doi:https://doi.org/10.1016/j.matpr.2020.08.742.
82. Mujeye, S. An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity. 2016.
83. Erdem, E.; Sandıkkaya, M.T. OTPaaS—One Time Password as a Service. *IEEE Transactions on Information Forensics and Security* **2019**, *14*, 743–756. doi:10.1109/TIFS.2018.2866025.
84. Wang, C.; Wang, Y.; Chen, Y.; Liu, H.; Liu, J. User authentication on mobile devices: Approaches, threats and trends. *Computer Networks* **2020**, *170*, 107118. doi:https://doi.org/10.1016/j.comnet.2020.107118.
85. Gordin, I.; Graur, A.; Potorac, A. Two-factor authentication framework for private cloud. 2019, pp. 255–259. doi:10.1109/ICSTCC.2019.8885460.

86. Das, A.K.; Bera, B.; Wazid, M.; Jamal, S.S.; Park, Y. iGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment. *IEEE Access* **2021**, *9*, 87024–87048.
87. Semal, B.; Markantonakis, K.; Akram, R.N. A Certificateless Group Authenticated Key Agreement Protocol for Secure Communication in Untrusted UAV Networks. *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)* **2018**, pp. 1–8.
88. Bera, B.; Das, A.K.; Sutrala, A.K. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Comput. Commun.* **2021**, *166*, 91–109.
89. Wei, Z.; Liu, F.; Ng, D.W.K.; Schober, R. Safeguarding UAV Networks through Integrated Sensing, Jamming, and Communications. *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* **2021**, pp. 8737–8741.
90. Sharma, G.; Sharma, D.K.; Kumar, A. Role of cybersecurity and Blockchain in battlefield of things. *Internet Technology Letters* **2022**, *6*.
91. Rodrigues, M.; Amaro, J.; Osorio, F.S.; Kalinka. R. L. J. C., B. Authentication methods for UAV communication. *2019 IEEE Symposium on Computers and Communications (ISCC)* **2019**. doi:10.1109/iscc47284.2019.8969732.
92. Kim, K.; Kang, Y. Drone security module for UAV data encryption. *2020 International Conference on Information and Communication Technology Convergence (ICTC)* **2020**, pp. 1672–1674.
93. Birnbaum, Z.; Dolgikh, A.; Skormin, V.; O'Brien, E.; Muller, D.; Stracquodaine, C. Unmanned Aerial Vehicle Security using behavioral profiling. *2015 International Conference on Unmanned Aircraft Systems (ICUAS)* **2015**. doi:10.1109/icuas.2015.7152425.
94. Klein, D. Micro-segmentation: securing complex cloud environments. *Netw. Secur.* **2019**, *2019*, 6–10.
95. Han, P.H.; Sui, A.; Wu, J. Identity Management and Authentication of a UAV Swarm Based on a Blockchain. *Applied Sciences* **2022**.
96. Khan, N.A.; Jhanjhi, N.Z.; Brohi, S.N.; Almazroi, A.A.; Almazroi, A.A. A Secure Communication Protocol for Unmanned Aerial Vehicles. *Cmc-computers Materials & Continua* **2022**, *70*, 601–618.
97. Catuogno, L.; Galdi, C. Secure Firmware Update: Challenges and Solutions. *Cryptogr.* **2023**, *7*, 30.
98. Zhang, K.; Zheng, J.; Fu, J.; Zhang, Y.; Ji, W. Research and application of zero trust based secure access to the power Internet of Things. *2023 IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC)* **2023**, *7*, 2356–2360.
99. Li, S.; Iqbal, M.; Saxena, N. Future Industry Internet of Things with Zero-trust Security. *Information Systems Frontiers* **2022**.
100. Feng, Y.; Li, M.L.; Zeng, C.; Liu, H. Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective. *Entropy* **2020**, *22*.
101. Banerjee, M.; Lee, J.; Choo, K.K.R. A blockchain future for internet of things security: a position paper. *Digit. Commun. Networks* **2017**, *4*, 149–160.
102. Alkanjr, B.; Mahgoub, I. A Novel Deception-Based Scheme to Secure the Location Information for IoBT Entities. *IEEE Access* **2023**, *11*, 15540–15554.
103. Federici, F.; Martintoni, D.; Senni, V. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics* **2023**.
104. Rutravigneshwaran, P.; Anitha, G. Security Model to Mitigate Black Hole Attack on Internet of Battlefield Things (IoBT) Using Trust and K-Means Clustering Algorithm. *International Journal of Computer Networks and Applications* **2023**.