Proceedings of the INMM & ESARDA Joint Annual Meeting
22 - 26 May, 2023, Vienna, Austria

Unmanned Aerial Vehicles (UAVs) for Small Modular Reactor (SMR) Security in Remote Sites

Ankur Chaudhuri, Jelena Vucicevic, Karthik Thiyagarajan
Canadian Nuclear Laboratories, Chalk River, ON, Canada

ABSTRACT

In Canada and around the world, interest in the potential deployment of small modular reactors (SMRs) has been gaining momentum as a low-carbon footprint energy solution to meet climate change goals. One of the possible applications of SMRs will be to address the need for energy in remote locations such as Canada's northern region. The deployment of SMRs in remote sites will have logistical challenges; however, it will be essential to maintain the nuclear security and physical protection of these sites.

Unmanned aerial vehicles (UAVs) could be a potential solution for SMR security in remote sites. UAVs would reduce the security costs significantly by reducing the number of on-site security personnel, as well as reduce the potential for insider threats in the remote sites. Although the use of UAVs is considered to be a cost-effective and safer means to verify the condition of any remote site, it is important to consider its limiting factors such as constraints on operational capability in harsh weather conditions, battery life, etc. In addition, UAV is a cyber-physical system in which the digital components collaborate to control and monitor the physical parts. Like other cyber-physical systems (industrial control systems, automobiles, etc.), UAVs have vulnerabilities that could be exploited by attackers. The evaluation criteria of the UAV-based solutions for SMR security in remote sites is discussed in this paper.

INTRODUCTION

According to the International Atomic Energy Agency, SMRs are a type of nuclear reactor with power output less than 300 MWe [1]. While conventional nuclear power plants contribute to the electric power production within centralised and interconnected power grid systems, SMRs can be deployed in a remote area which is either not connected to the grid, or connected with a small electricity grid, or in a region with limited suitable sites for large nuclear power plants [2]. Three potential applications for SMRs in Canada are identified as: on-grid; heavy industry; and remote communities, each of these with different energy demands [3]. A new class of SMRs (micro-reactors) with power outputs ranging up to 20 MWe designed primarily to replace diesel use in remote communities and mines are being proposed in Canada [4]. It is expected that SMRs with very low power output will be appropriate for remote communities (~ 3-10 MWe), and mining sites (~20 MWe) [3].

The remote northern region of Canada will pose unique logistics challenges for SMR deployment. According to the Remote Communities Energy Database published by Natural Resources Canada

[5], there are approximately 240 remote communities in Canada with their total population just over 196,100. These communities are small, and distant from each other.
The map in Figure 1 shows the locations of these remote communities and the extent of electric grid lines above 65 kV [6]. Green dots show Aboriginal communities while yellow dots show non-Aboriginal sites. Many of these communities are only connected by air, or do not have year round road access.

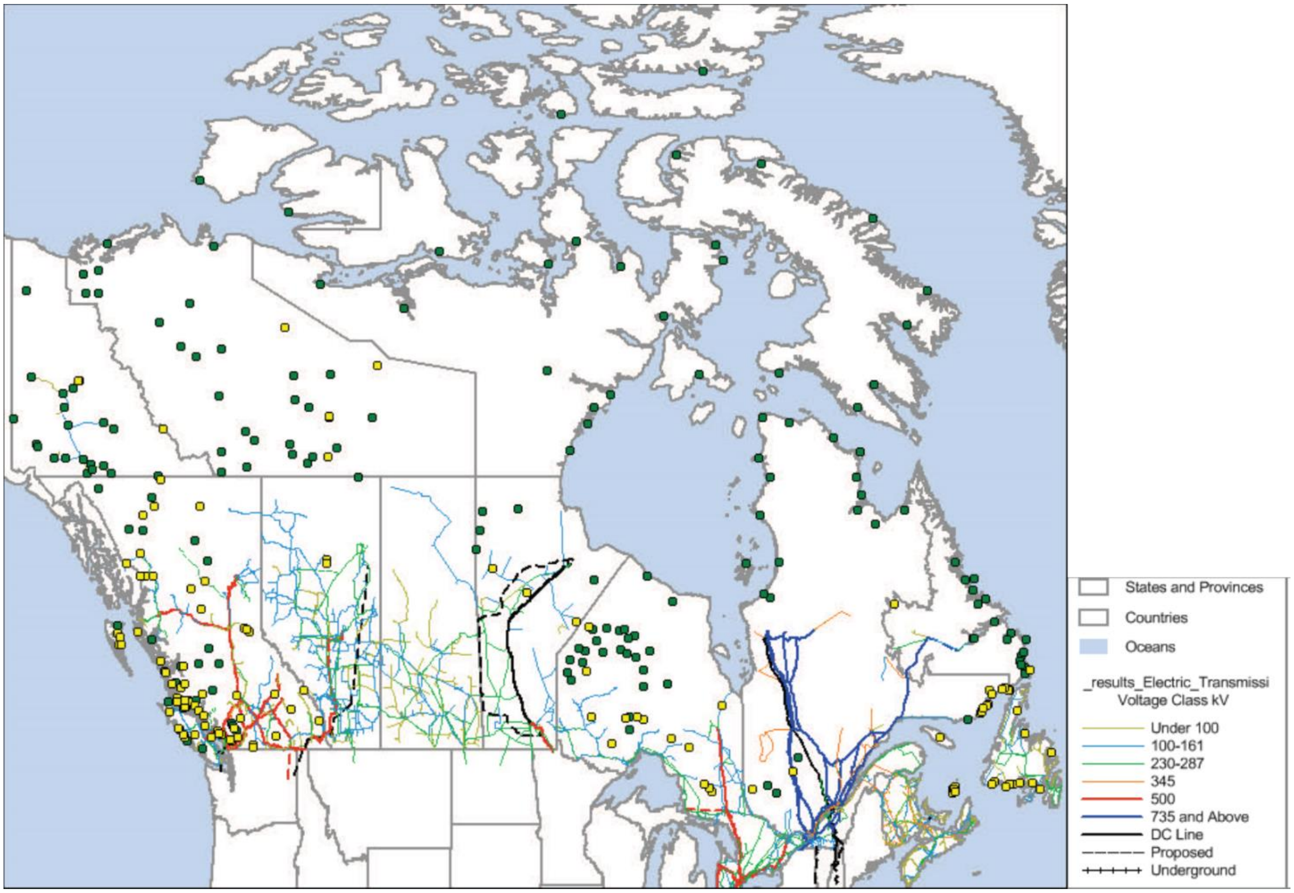

Figure 1 Remote communities in Canada: Green dots show Aboriginal communities while yellow dots show non-Aboriginal sites *[6]*.

Despite the remote and disconnected locations, it is very important to maintain the safety and security of the remote SMR sites, and ensure that emergency management and response provisions are in place. The remote siting of SMRs with limited physical access can have counterbalancing security benefits and challenges [7]. It will be harder for the adversaries to reach and access the sites for theft, sabotage, or unauthorised access of nuclear materials. However, staffing of SMRs in remote sites is likely to be very small for economic reasons, hence it may be difficult to have sufficient security personnel present at the SMR site to fully protect against external adversaries [8]. Any offsite response force will also have difficulty to access the site in a timely manner due to the remote location. It is expected that UAVs could verify the reactor sites from a central operations center allowing a timely response by offsite security forces without increasing the cost of security [9].

UNMANNED AERIAL VEHICLEs (UAVs) FOR SMR SECURITY

The primary use cases of UAVs, when they were first introduced, were for aerial photography. Over the past few decades, the number of applications for UAV technologies in critical infrastructure has increased exponentially, particularly for monitoring and surveillance purposes. In the case of surveillance and physical security, UAVs may act as perimeter security to watch over the facility. In the case of moving objects in a critical area, an UAV can aim its camera at the moving object, magnify (zoom in), and transmit its image to a central monitoring station.

The current UAV market is very diverse and provides technological solutions for different purposes. Most often UAVs are used for creating high quality photographs and videos, but recently they have been adjusted to respond to other challenges. Many UAVs are now being built with capacities to enable response to different scenarios related to public safety (firefighting, law enforcement, rescue services). They are also finding use in industries (oil, gas, electricity) for inspections, construction management, environmental management, and power grid management to enhance personnel safety. At the same time, using UAVs can significantly save time on certain tasks, which leads to improved efficiency and reduces costs. Due to constant improvement and adjustment of the features, UAVs are increasingly utilized in the security sector as one of the important tools in surveillance.

SMRs are envisioned to utilize a smaller complement of staff compared to today’s conventional larger-scale nuclear power plants. UAVs deployed for security purposes can serve as potentially useful tools for ensuring the effectiveness of reduced SMR security staffing. Key advantages of UAVs include their fast technology development, adjustability, and intelligent features which allow some tasks to be completed with minimum involvement of the security officer. However, when deploying UAVs for SMR security in remote locations, some physical limitations should be considered, such as limited capability in severe weather conditions, battery life, etc.

EVALUATION OF UAVs FOR SMR SECURITY

When considering UAVs for SMR security it is important to choose the best option for the security needs. Some manufacturers build UAVs for specific operation; these are often supplied with specialized equipment for conducting aerial inspection and survey. These UAVs have some specific functions which allow them to fly in different weather conditions, at high speed, and they have sensors and cameras adjusted for the purpose (for example thermal cameras). Other UAVs are built with no specific task in mind, and are mainly used for photography and videography; therefore they have very high quality cameras, but their use is not limited to only these operations. As UAV technology develops they are becoming a multipurpose tool, since they can be highly adjustable, with different payloads that can be tailored to meet the user’s needs.

The UAV features can be divided in five groups for assessing their suitability in remote site security operation.

Group I: weather condition tolerance: operable in low temperatures, waterproof, wind speed resistance
Group II: characteristics of the UAV: battery life, flight speed, distance
Group III: image and video quality, intelligent features, obstacle sensing
Group IV: cyber security
Group V: price

Group I weather condition tolerance is considered a very important assessment criteria, since it is essential for successful operation in the area of interest. The most important characteristics for Group I is the operating temperature since it is certain that temperature in the remote northern areas of Canada can be very low. Irrespective of features, ability to operate in the expected temperature range becomes the first criterion in UAV selection for a security application. The next criteria is wind resistance, since it is most certain that remote areas where SMRs might be located will not have additional wind protection (no high buildings, or natural wind protection such as high mountains). The final criteria for this group is whether the UAVs are waterproof or not and if yes, to what level. Waterproof and dustproof levels are defined through IP (ingress protection) ratings introduced by the International Electrotechnical Commission (IEC). The IP code is composed of two numerals: The first numeral refers to the protection against solid objects and is rated on a scale from 0 (no protection) to 6 (dust-tight). The second numeral rates the enclosure’s protection against liquids and uses a scale from 0 (no protection) to 9 (high-pressure hot water from different angles) [10]. An UAV with IP rating 68 will be signifantly more robust to weather conditions than an UAV with IP rating 45, for example.

Group II parameters for UAV categorization would include characteristics of the UAV itself. This includes battery life, since the UAV should be able to fly for a certain amount of time and/or carry a payload, for which a certain battery capacity is needed. Flight speed is very important since the UAVs may be required to follow a vehicle during a security breach.

Group III ranking is based on intelligent features, photo and video characteristics, and obstacle sensing. For most UAV models, standard cameras are high quality, providing high resolution images. For the purpose of security operation, cameras should have high quality photo and video, and it is important that the UAV has a thermographic/infra-red camera as well, so the night imaging is possible. An intelligent features which allows autonomous tracking of the target will be very beneficial for security operations. In addition to these characteristics, the safe maneuverability of UAVs to avoid obstacles in their surroundings is important also. In particular, the UAV should be able to sense obstacles and avoid them when flying out of line of sight, or on a programmed route.

Group IV ranking is based on cyber security of UAV based solutions. A cyber security evaluation of UAVs is discussed in next section which can be used to assess the suitability of any particular UAV model for remote SMR security.

Finally, the price could be one of the decision points when ranking UAVs, as some might have very high price but none of the equipment is needed for security. However, this will be the least important characteristic, if all other characteristics are met.

CYBER SECURITY OF UAV BASED SOLUTIONS

Security issues, vulnerabilities, and threats are constantly arising, including the malicious misuse of UAVs via cyber-attack [11]. Reported cyber security breaches include: GPS jamming and spoofing, video interception, hijack attacks via communication, sensor spoofing, etc. By exploiting these vulnerabilities, an adversary could disturb the normal operation or take over control of the system for malicious objectives, including injuring people on the ground, violating personal privacy, damaging infrastructure, etc.

Hence, cyber security capabilities of UAV based security solutions should be an important consideration when assessing the suitability of an UAV for the security of remote SMRs. In order to assess the capability of the UAVs to protect from, detect and respond to a cyber-attack, both field system (UAV) and remote system (controller) need to be evaluated with respect to the identified cyber security controls. The field system (UAV) has a complex computer system that can be controlled by a remote controller and can be programmed to carry out a series of complex automation functions. A field system can operate alone but may also need to maintain interactions with operators on the ground. The remote system or a controller can be hardware or software used by operators to control the field system. The remote controller could also be a target for cyber-attack.

A cyber-attack on a UAV based system can be executed by the adversaries using any of the following five attack pathways mentioned in CSA N290.7, Cyber Security for Nuclear Facilities [12]:

a. wired
b. wireless
c. direct physical access
d. removable media
e. supply chain

The cyber security controls (bolded) which can be used for assessment of the suitability of any particular UAV based security system for remote SMR deployment have been identified and listed below. The list of controls was developed in the context of NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline [13]. The attack pathways impacted by these cyber security controls are mapped in square brackets next to the bolded heading. However, supply chain attacks are difficult to detect, as they rely on software that has already been trusted and can be widely distributed, therefore controls for supply chain attacks are not addressed in this paper.

1. External physical communication ports [(a) (c) (d)]: Unprotected external physical ports can serve as an entry point for attackers in physical proximity to perform a variety of attacks. For example, an attacker could plug in a USB stick with malware and infect the device. If the USB port was disabled when not in use, it would be difficult for an attacker to use this attack pathway.

2. Accessibility of hardware components [(c) (d)]: Directly accessible hardware components could be physically damaged, stolen, tampered with, removed, or completely disabled causing the system to misbehave or completely fail. An obvious example is the removal of critical sensors for the behavior of the system.

3. Capability to monitor component changes [(c) (d)]: Having no verification or log of whether hardware or software components of the system are accessed or updated could mean attackers could tamper with components or install malicious software unnoticed. Monitoring/logging capability can be helpful by identifying unscheduled access to internal components.

4. Physical identification [(c) (d)]: A unique physical identifier (e.g. a product tag number) can be used to distinguish each system from all other similar systems.

5. Encryption - Data [(a) (b)]: Encryption is a method that uses mathematical algorithms to encode sensitive information at rest and/or in transfer. Encryption protects information by making it indecipherable to unauthorized personnel. In the context of the above technologies, sensitive information could be sensor data or images being exposed to less secured communication paths/access points.

6. Encryption - remote maintenance [(a) (b)]: The aforementioned systems at remote sites require maintenance such as software updates and configuration changes. Because remote sites by definition are not easily accessible the UAVs require remote maintenance capability. Remote maintenance activity can be vulnerable to session hijack cyber-attacks. A session hijack could allow an attacker to misconfigure the system, leading to unintended operation and potential damage. The encryption of remote maintenance communication would block illegitimate users from hijacking the session between the remote maintainer and the remote asset.

7. Device authentication [(a) (b) (c) (d)]: Authentication is verifying the identity of the device trying to access the system, often as a prerequisite to allowing access to resources in the system [14]. Authentication protects against unauthorized devices trying to start communicating with the UAVs. This is the starting point for most cyber-crime activities.

8. User authentication [(a) (b) (c) (d)]: Authentication is verifying the identity of a user trying to access the system, often as a prerequisite to allowing the user to access the system resources [14]. This feature manages user authentication when attempting to access the remote and/or the field system. (e.g., for maintenance purposes). Authentication establishes the identity of the user accessing the system.

9. Access control [(a) (b) (c) (d)]: Access control adds an extra layer of security to the authentication process. It specifies the access rights and privileges an entry should be granted access to data or make a specific configuration change.

10. Communication protocol vulnerability [(a) (b)]: Vulnerabilities of communication protocols can allow attackers to gain unauthorized access to the internal network and intercept or modify transmitted data.

11. Wireless radio frequency [(b)]: Wireless communication uses radio frequency bands to transmit information to and from devices. Specific frequency bands can be licensed where no others can use those frequencies, or they can be unlicensed and freely available for use by the general public. Because wireless signals flow through un-protected media (air) they are prone to jamming. An attacker could simply use a jamming device to inject signal waves similar to those the system uses for communication. This could degrade or fail the operational performance of the system.

12. Logical identification [(a) (b)]: The remote system needs to have a logical identifier as does the field system connected to it. A unique logical identifier distinguishes one asset from all others, usually for automated asset management and monitoring.

13. Anti-jamming capabilities [(b)]: Jamming refers to the creation of interference within a radio channel to disrupt its normal operation. Attackers may use interference generators or signal suppressors to disturb radio channels leaving them unavailable for normal data transfer.

14. Replay protection [(a) (b)]: A replay attack occurs when attackers record legitimate encrypted packets and then arbitrarily replay them to achieve malicious actions. Replay attacks can be prevented by incorporating replay prevention mechanisms into communication. For example, the encrypted packets can be tagged with a session ID and a packet number to authenticate that the packet is valid.

15. Update mechanism [(a) (b)]: Updates are important for vulnerability management. Updates can address known vulnerabilities, which lowers the likelihood of an attacker compromising the device. Updates can correct device operational problems, which can improve device availability, reliability, performance, and other aspects of device operation. Some users may need automatic update capabilities to meet cyber security goals and requirements, while others require more direct control over updates and their applications.

16. Logging and alerting [(a) (b) (c) (d)]: Logs provide information about a wide array of activities that could take place in UAV and remote controller. Logs can be configured to capture cyber events such as deviations from expected activity, configuration changes, log on/off activities, hardware or network runtime issues, etc. Logs from UAVs and remote controllers could be forwarded to a centralized cyber security tool to automatically parse for anomalous behaviors.

17. Security configuration management [(a) (b) (c)]: Security configuration management is a process that involves adjusting any default settings of a system that would increase/harden its security, mitigate risk and create a secure baseline configuration.

18. Performance monitoring [(a) (b)]: Performance monitoring improves security by constant monitoring of the performance levels of the system. Performance levels are indicators of normal operation such as CPU load, memory consumption, etc. Asset performance monitoring helps protect the asset by identifying warning signs (e.g., high memory consumption leading to Denial of Service) that could indicate a security breach or threat.

19. Secure user interface [(a) (b) (c)]: A secure user configuration is required to manage the asset. For example, some devices host a Hypertext Transfer Protocol (HTTP) server that the maintainer can access to modify the configuration. However, HTTP servers are vulnerable and can be easily compromised, further compromising the asset. Therefore, it is recommended to use either Hypertext Transfer Protocol Secure (HTTPS)-based access or the command line to modify asset configuration.

20. Configuration management, backup and disaster recovery [(a) (b) (c) (d)]: Configuration management is used for configuration controlled Original Equipment Manufacturer (OEM) and user-defined software / configuration data. Backups are used for operational data (data that changes during the operation of the system) whose persistent storage is important. Disaster recovery is the process of re-establishing vital system operations following a natural disaster or human-induced cyber-attack.

21. Internet connectivity [(a) (b)]: Internet connectivity may be required for updating or upgrading device software or firmware. Because the internet increases the exposure to potential attackers, the system should have features to control this communication flow. For example, the system could be configured to access and receive updates strictly and only from a single vendor website.

22. Open network service ports [(a) (b)]: A great number of open service ports e.g. File Transfer Protocol (FTP), HTTP results in a larger attack surface and therefore the number of open service ports should be as low as possible. Services that are exposed should have no known vulnerabilities due to the ease of their exploitation.

DISCUSSION

The evaluation characteristics presented in this paper can be used for assessing the usefulness of any UAV system for SMR security in remote sites. However, this assessments should follow a risk-based methodology. For example, an UAV responsible for the surveillance of critical areas in the SMR should be more secure than an UAV responsible for surveillance of less critical areas.

Overall findings from this evaluation is that the security operations in remote SMR sites may benefit from using advanced technologies such as a UAV system. The current state of UAV technology may not be made specifically for SMR security purposes, but they have a number of characteristics which allow them to conduct many tasks regarding surveillance or response to an adversary attack. It is important to note that UAV technology develops quickly, and in the future they might be more suitable for specific security tasks.

CONCLUSIONS

An evaluation of UAV-based solutions for SMR security in remote sites is discussed in this paper. The UAV features were divided in five groups for this evaluation purpose, which are: (i) weather condition tolerance, (ii) characteristics of the UAV (e.g. battery life, flight speed, and distance), (iii) image and video quality, intelligent features, obstacle sensing, (iv) cyber security, and (v) price. It has been emphasized that irrespective of the advanced features present in the UAV, their ability to withstand the harsh weather condition of Canadian north is the first criteria for the UAV selection for SMR security in remote sites. The UAV-based security system for physical security of SMR sites must also be resilient towards any cyber-attack attempts.

ACKNOWLEDGMENT

Authors acknowledge the funding received from the Federal Nuclear Science and Technology Work Plan of Atomic Energy of Canada Limited for the study described in this paper.

REFERENCES

[1] International Atomic Energy Agency, "Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends," IAEA-TECDOC-1451, 2004.

[2] Nuclear Energy Agency, "Small Modular Reactors: Challenges and Opportunities," OECD, 2021. [Online]. Available: https://www.oecd-nea.org/jcms/pl_57979/small-modular-reactors-challenges-and-opportunities?details=true. [Accessed 01 03 2023].

[3] Canadian Small Modular Reactor Roadmap Steering Committee, "A Call to Action: A Canadian Roadmap for Small Modular Reactors," 2018. [Online]. Available: https://smrroadmap.ca/. [Accessed 01 03 2023].

[4] Governments of Ontario, New Brunswick, Saskatchewan and Alberta, "A Strategic Plan for the Deployment of Small Modular Reactors," 2022. [Online]. Available: https://www.ontario.ca/page/strategic-plan-deployment-small-modular-reactors. [Accessed 01 03 2023].

[5] Natural Resources Canada, "The Atlas of Canada - Remote Communities Energy Database," 2018. [Online]. Available: https://atlas.gc.ca/rced-bdece/en/index.html. [Accessed 01 03 2023].

[6] Government of Canada, "Status of Remote/Off-grid Communities in Canada," 2011. [Online]. Available: https://natural-resources.canada.ca/sites/www.nrcan.gc.ca/files/canmetenergy/files/pubs/2013-118_en.pdf. [Accessed 01 03 2023].

[7] "WINS Special Report Series- Security of Advanced Reactors," World Institute for Nuclear Security (WINS), Vienna, Austria, August 2020.

[8] G. Bentoumi, A. Chaudhuri, B. van der Ende, B. Sur and D. Trask, "Safety and Security for Small Modular Reactors in Canada," in *International Conference on Nuclear Security,* Vienna, Austria, 2020.

[9] F. Dimayuga, A. Chaudhuri, D. Rowan, D. Trudell, B. van der Ende, S. K. Yang and G. Xu, "Mobile Microreactors for Deployment in Canada's North," in *Technical Meeting on the Status, Design Features, Technology Challenges and Deployment Models of Microreactors*, Vienna, Austria, 2021.

[10] "IP ratings," International Electrotechnical Commission, 2023. [Online]. Available: https://www.iec.ch/ip-ratings. [Accessed 10 03 2023].

[11] M. Haider, I. Ahmed and D. B. Rawat, "Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems," in *Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, Barcelona, Spain, 2022, doi: 10.1109/ICUFN55119.2022.9829584.

[12] "CSA N290.7:21 Cyber Security for Nuclear Facilities," [Online]. Available: https://www.csagroup.org/store/product/CSA%20N290.7:21/. [Accessed 15 03 2023].

[13] M. Fagan, J. Marron, K. G. Brandy, B. B. Cuthill, K. N. Megas, R. Herold, D. Lemire and B. Hoehn, "NIST Special Publication 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements," National Institute of Standards and Technology (NIST), 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf. [Accessed 20 03 2023].

[14] P. A. Grassi, M. E. Garcia and J. L. Fenton, "NIST Special Publication 800-63, Revision 3, Digital Identity Guidelines," National Institute of Standards and Technology (NIST), [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed 15 03 2023].