A Review of Cybersecurity and Biometric Authentication in Cloud Network

Manjunath Reddy[1*], Nur Mohammad Ali Chisty[2], Anusha Bodepudi[3]

[1]Customer Engineering Lead, Qualcomm, San Diego, CA, **USA**
[2]Additional Superintendent of Police (Cyber Crime Wing), Anti-Terrorism Unit, Bangladesh Police, Dhaka, **BANGLADESH**
[3]Staff Engineer, Intuit, Plano, TX, **USA**

[*]Corresponding Contact:
Email: reddymanjushari@gmail.com

ABSTRACT

Cloud computing uses few resources to give customers complete distant services via the internet. Data privacy, security, and reliability are major issues with cloud computing. Security is the biggest issue. This study discusses the biometrics framework and safe cloud computing identity management method. This paper discusses cloud computing security challenges and reviews cloud access framework approaches. It describes a novel fingerprint access-based authentication system to protect cloud services from DOS and DDoS attacks. This biometrics-based system can secure cloud services from illegal access. This study addresses cloud security and privacy via biometric face recognition. Cloud users' security and privacy are protected via biometrics recognition. This article discusses CPS and its applications, technologies, and standards. SIGNIFICANT DIFFICULTIES AND CHALLENGES ARE FOUND IN reviewing CPS security weaknesses, threats, and attacks. Presenting and analyzing current security measures and their key drawbacks. Finally, this extensive examination yields various recommendations.

Key words:
Cloud Network, Cyber Security, Privacy Preservation, Biometrics Identification, Encrypted Biometrics

5/30/2022 **Source of Support:** None, **No Conflict of Interest:** Declared

INTRODUCTION

Recent years have seen a rise in the prevalence of biometrics-based recognition systems and increased attention given to these systems. It does so effectively, preserving the users' privacy while also guaranteeing the safety of the more sensitive data stored on cloud servers. Therefore, the recent research trend emphasizes the need to solve the concerns of preserving the privacy of cloud users, maintaining the integrity of cloud data, and managing the

expansion of cloud data (Mandapuram et al., 2018). In addition to preserving the users' privacy, processing, and maintaining the integrity of the data, the biometrics-based recognition system retrieval has played an essential role in maintaining the data in cloud computing (Bodepudi et al., 2019). Over the last few decades, research has been conducted on the applications made of various biometrics-based recognition systems. These systems use sophisticated and practical algorithms to protect the privacy and security of biometric information. These recognition systems take care of user authentication, which checks each individual's identity. During the verification process, the unique biometric characteristics of each user are compared to those stored in a biometric template database, employing techniques analogous to those used for similarity matching (Yaacoub et al., 2020). Physiological and behavioral biometrics characteristics are the two primary subgroups comprising the whole biometric characteristic classification system. Face, fingerprints, hand geometry, DNA, and iris are some traits based on physiological biometrics. Behavioral biometric traits include a person's signature, stride, and voice, among other things. These aspects of an individual's biometrics cannot be changed, are easily distinguishable from other people, and may be quantified for use in verifying and identifying persons. Traditional authentication methods, such as passwords and token-based systems, do not compare favorably to biometrics, which offers a significantly greater level of data security, users' privacy is preserved, the likelihood of forgery is significantly reduced, cost-effective solutions are utilized, and biometrics is very user-friendly (Tahir & Tahir, 2008). When it comes to user authentication, the biometric data that has been recorded is first pre-processed and then compared to a biometric template database that has been kept on the cloud servers. Because data stored can be stolen and exploited during user enrollment, cloud computing comes with some inherent dangers, including but not limited to the hazards of identity theft, forgery, and duplication of sensitive data, as well as the risk of breaching the integrity and authentication of users (Bodepudi et al., 2021). As a result, users cannot replicate or counterfeit the biometric data of other enrolled users, which is the primary benefit of using biometric data.

This article explores a unique privacy-preserving biometrics-based recognition system for cloud computing. The system makes use of biometrics. In the recognition system that has been developed, the collected biometric data from cloud users will first be encrypted before being sent to a third party. The biometric information of cloud users is decrypted and then used for authentication during the identification and verification processes before gaining access to cloud services and system resources (Vinoth et al., 2021). In this step, the database administrators or managers of the cloud produce a credential for the candidate based on their biometric characteristics and then present it to the cloud to identify it.

CLOUD AUTHENTICATION ISSUES

Innovative technologies such as smart mobile devices, mobile applications with sensors, Internet spread and usage, and data availability in social media have all contributed to data sharing and processing in the cloud (Gunzel, 2017). These technological advancements have wide-ranging effects on the extensive data that we generate in our day-to-day activities. Several companies, like Amazon, Flipkart, and Netflix, are among the many that engage in data collecting, mining, and analysis from various sources. Cloud storage has made it possible to easily and quickly make enormous amounts of data available to others across a network. In addition, security concerns have arisen as a result of an increase in the demand for storage disks over the network searches for authentication of data that has been saved. These concerns relate to both the cloud and distributed storage.

Redundant copies of data records take up a significant portion of the storage capacity in cloud infrastructure. Researchers have been concentrating on methods for data de-duplication employing biometric de-duplication in conjunction with user authentication to address the technical issues raised (Sabri et al., 2014; Reddy et al., 2020). The link between an individual's inc characteristics and their behavior, physical, and physiological characteristics are utilized to authenticate an individual by recognizing biometric data. Compared to authentication based on knowledge, biometric authentication can provide higher guarantees of security. The development of a cloud-based system that is biometrics-enabled is crucial not only for the improvement of security but also for safety. Forensics, surveillance, defense, finance, and personal authentication are some of the fields that compared the protection that is given (Masala et al., 2018). Compared to more conventional authentication methods for sensitive applications, using other biometric-based authentication processes has been shown to give stronger security guarantees and greater robustness.

BIOMETRIC AUTHENTICATION METHODS

"Biometric Authentication" is a security procedure that verifies an individual's identity using their distinct biological traits. This helps to ensure that the person is who they claim to be. In biometric authentication, a person's physical or behavioral characteristics are compared to data in a database that has been verified and authenticated. In order for authentication to be successful, both sets of biometric data must be identical. The management of access to physical and digital resources, such as buildings, rooms, and computing devices, is typically handled through biometric authentication (Patel, 2020). The process of identifying a person by biometrics, such as fingerprints or retina scans, is called biometric identification. On the other hand, biometric authentication refers to using biometrics to verify that a person is who they say they are.

People can be digitally identified and given permission to enter a system through the use of the following technologies:

- Devices based on chemical biometrics
    - DNA (deoxyribonucleic acid) matching refers to the process of identifying a person by comparing their genetic material.
- Visual biometric devices
    - Subjects are identified by conducting a scan of the retina, which examines the pattern of blood vessels located in the back of their eyes.
    - Iris recognition compares an image of an individual's iris to a database of known individuals.
    - Individuals can be identified using only their fingerprints by using fingerprint scanning.
    - Hand geometry recognition uses a mathematical representation of hand features to verify the identity or authorize transactions. This is done by measuring finger length, breadth, and knuckle valleys.
    - Facial recognition uses distinctive features and patterns to verify identity. Face prints are numeric codes based on 80 nodal points on a human face.
    - Ear authentication is a form of identity verification that uses a user's distinctive ear shape.

  - Signature recognition is a form of pattern recognition that may determine an individual's identity based solely on their handwritten signature.

- Vein or vascular scanners
  - Finger vein ID is a method for identifying people by analyzing the patterns of veins in their fingers.

- Behavioral identifiers
  - Gait analysis examines the manner in which individuals walk.
  - A person's identification can be determined through typing recognition by analyzing their typing features, such as their typing speed.

- Biometric instruments that rely on hearing
  - A person's identity can be deduced from their voice using a system called voice identification based on the unique features provided by the mouth and throat.

Various Forms of Authentication Based on Biometrics-

COMPONENTS OF BIOMETRIC AUTHENTICATION DEVICES

A biometric device comprises three parts: a reader or scanning device, technology that can transform and compare the biometric data that was acquired, and a database that can store the information. A device that can measure and record biometric data is referred to as a sensor (Gutlapalli, 2017). It could be a voice analyzer, a retina scanner, or a fingerprint reader. These devices are collecting data in order to compare it with the information that has been saved and look for a match. The program processes the biometric information, and the results are compared to the stored data in search of match points. The vast majority of biometric information is kept in a database connected to a central server where all the data is kept. The data can also be hashed cryptographically, which is another way to store biometric information and makes it possible to authenticate a user without having direct access to the data.

ADVANTAGES AND DISADVANTAGES OF BIOMETRIC AUTHENTICATION

The use of biometric authentication is not only reliable but also quite convenient. Because of the use of one-of-a-kind traits in the verification process, biometric forms of authentication are relatively easy to fake. The traditional methods, such as using passwords or ID cards, are less safe than their modern counterparts because they are easier to steal or decipher.

Despite its many opportunities for specific business sectors, there are debates over the appropriate applications of biometrics. For instance, corporations might need to give adequate consideration to the safety of these data-driven security systems (Obergrusberger et al., 2012). For example, malicious actors can intercept biometric data as it is being transmitted to a centralized database. In that case, they will be able to fraudulently recreate that data in order to carry out another transaction. For instance, malicious actors might acquire sensitive data, such as private messages or financial information, by collecting an individual's fingerprint and utilizing it to gain access to a fingerprint-secured device. This would allow them to gain access to the device.

Another possible drawback of using biometric authentication is that once a system has been implemented, an organization may be enticed to utilize the system for functions not initially intended to be performed by the system. This phenomenon is referred to as function creep. For instance, a corporation may find the technology helpful for employee monitoring and management. However, once a biometric system has been installed, the firm may discover that it can trace precisely where an employee has gone and when they were there.

USE CASES OF BIOMETRIC AUTHENTICATION

Law Prosecution

For identification, law enforcement and state and federal entities utilize many types of biometric data. Fingerprints, facial traits, iris patterns, voice samples, and DNA are all examples of this type of evidence. For instance, the Automated Fingerprint Identification System, often known as AFIS, is a database that can recognize fingerprints. The FBI developed this system. It was in the early 1970s that it was applied for the first time as a method for police agencies to automate their previously manual fingerprint identification process in order to make it more efficient and accurate. In the past, a human examiner with

the appropriate training was required to compare a fingerprint image to the actual prints stored. If there were a match, the examiner would review both prints again to confirm a match. Finally, AFIS can compare a fingerprint to a database containing millions of other prints and find a match in only a few minutes.

Tourism

Electronic passports, also known as e-passports, are the same size as traditional passports, and they contain a microchip that holds the same kinds of biometric information as traditional passports, including a digital photograph of the person holding the passport. A digital photograph of the person holding the passport is stored on a chip, and this photo is connected to the owner's name as well as other identifying information. Before issuing the passport, the authority responsible for issuing passports in a country verifies the applicant's identification using fingerprints or other biometric information. Then it compares the data stored in the chip to the information the applicant provided. The e-passport is then issued electronically.

Healthcare

In hospitals, using biometrics allows for more accurate patient tracking and helps eliminate the possibility of mix-ups. In clinics and doctors' offices, biometric authentication is utilized to protect patient information's confidentiality. For example, a patient's medical history can be stored in a hospital and accessed there using the patient's biometric data. This information can be used to ensure that the appropriate patient receives the appropriate care, whether that entails expedited patient identification in the event of an emergency or the prevention of medical errors.

A NEW APPROACH TO DEFENSE CONTRACTOR CYBER SECURITY

On August 26, 2015, the DoD issued an interim regulation, "Network Penetration Reporting and Contracting for Cloud Services," to strengthen defense contractor cybersecurity and streamline incident reporting. This interim rule required "contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support (Mandapuram, 2016)." This interim rule required contractors to notify the DoD of cyber-attacks within 72 hours, like the November 2013 final rule. However, the regulation also had a few goals: to expand the type of information covered under the previous DFARS clause, to change the NIST safeguards for protecting protected information, to clarify the applicable procedures for reporting a cyber incident to the DoD and limit the use of "third-party cyber incident information," to require "flow down" of the rule to all subcontractors and to regulate contracting services for cloud computing systems.

The DoD released a second interim rule on December 30, 2015, to address industry concerns about prime and subcontractors meeting the August interim rule's criteria.94 This second interim rule delayed the deadline for contractors to comply with NIST SP 800-171 to December 31, 2017, providing them more time to modernize their systems or hire security experts. "Any NIST SP 800-171 security requirements that are not implemented at the time of contract award, within [thirty] days of contract award" must be reported to the DoD CIO. The interim regulation limited subcontractor flow-down requirements to "where their efforts will involve covered defense information or where they will provide operationally critical support."

The DoD finalized the rule on October 21, 2016. In response to military industry concerns, the DoD made several modest adjustments to the final rule. Most importantly, the rule clarifies that "covered defense information" (CDI) includes controlled technical information or other information that requires safeguarding that is (1) "marked or otherwise identified" and "provided to the contractor by or on behalf of [the] DoD in connection with the performance of the contract" or (2) "collected, developed, received, transmitted, used, or stored by... the contractor in support of the performance of the contract." "All covered contractor information systems must implement information protection requirements," the final regulation states.

REGULATORY ISSUES THAT THREATEN CONTRACTOR COMPLIANCE

The final rule improves DoD contractors' cybersecurity but raises many challenges that must be addressed before the DoD has a fully enforceable and effective law. This section discusses major issues that can directly affect prime and subcontractor compliance. The final rule's new requirements could cost small businesses too much to comply. Small firms may need more resources to comply with the regulation (Malathi & Raj, 2016). According to the DoD, contractors may need "information technology experts" to report cyber issues, which smaller businesses may not be able to afford. High compliance costs could hurt small firms and the DoD. Smaller contractors are less likely to have a cybersecurity system that can be easily modified to fulfill the final rule and NIST SP B00-I71 security standards than more giant contractors. As a result, small contractors may need to hire professionals and install a new cybersecurity system, which may be too expensive (Gutlapalli et al., 2019).

This new law could "potentially cripple" the DoD's purchasing system. Small defense firms have traditionally completed DoD contracts. In FY2014, the DoD "obligated approximately $55.5 billion to small business prime contractors at over 51,000 locations." The DoD expects the new regulations will affect 10,000 contractors, with less than half being small enterprises. Compliance difficulties could lead small businesses to leave DoD contracts, reducing the DoD's contractor pool. The DoD acknowledges that these requirements may have "a significant economic impact on a substantial number of small entities" but claims that the NIST SP 800-171 standards are streamlined to include only "security requirements necessary to provide adequate protections for the impact level of CUI" and that by defining one set of standards, small businesses can "avoid a situation in which [they] must adopt multiple standards and rule sets as [they] navigate am The DoD has no plans to help small firms comply with these new criteria or lower implementation costs. As a result, small firms may only meet new criteria with support.

Another concern is the final rule's NIST SP 800-171 security provisions. The DoD claims that NIST SP 800-171 standards were "carefully crafted" to incorporate only "those security requirements necessary to provide adequate protections for the impact level of CUT and should simplify the compliance process."125 NIST SP 800-171 defines "fourteen families of controls," each with numerous "Basic Security Requirements" and many with extra "Derived Security Requirements." Sixty-four percent of NIST SP 800-171 requirements are new or partially new, according to CODSIA. As mentioned above, these new regulations might put a tremendous financial strain on already-strapped small enterprises, making compliance impossible. Even large contractors may struggle to comply because "[m]any businesses subject to this Rule will not have systems already in place that cover all the fourteen control families, much less all of the [thirty] Basic Security and [seventy-nine] Derived Security Requirements[,] [n]or will they have resources in-house to conduct this analysis." The

compliance extension to December 2017 may assist contractors in updating their cybersecurity systems. Even with the delay, other contractors may need help to comply. The GAO found that thirteen years after FISMA was enacted, most of the twenty-four federal agencies observed had weaknesses and compliance issues in five major categories of information system controls. Contractors and agencies can take time to adapt to new cybersecurity standards. Since federal agencies took thirteen years (and counting) to comply with FISMA, it is improbable that all DoD contractors will comply with NIST SP 800-171 standards by December 2017.

The final regulation exempts contractors from NIST SP 800-171 compliance if they submit an "alternative, but equally effective, a security measure that may be implemented in its place." This phrase does not define "equally effective" security measures, leaving contractors to experiment and risk losing contracts that require compliance with the new DFARS norm. The final rule also gives prime and subcontractors 30 days to notify the DoD CIO if they cannot achieve NIST SP 800-171 security criteria. While prime contractors may be able to assess whether they will meet NIST SP 800-171 requirements within that time frame, small subcontractors may find it harder, especially if they were not subject to heightened security standards before this final rule. These issues may cause prime and subcontractors to decline contracts with these security standards, or worse, let non-NIST SP 800-171 compliant contractors win contracts and leave vulnerable CDI open to attack.

The final rule does not address whether contractors' reputations will suffer from disclosing cyber events. According to DFARS 204.7302(d) (October 2016), a reported cyber incident will not "by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of the clause at 252.204-7012." The final rule does not promise contractors that reporting a cyber event will not result in sanctions. Yet, it may be reassuring. The DoD said the final rule would "gain awareness of the full scope of cyber incidents being committed against defense contractors." However, without a "safe harbor" clause to protect contractors from penalties, contractors may be unwilling to complain, mainly if they rely significantly on the DoD for contract wins. The final rule enhances incident reporting requirements from the 2013 rule. However, by expanding the number of persons responsible for reporting while retaining the strict seventy-two-hour limit, the new rule will likely lead to incomplete or delayed reporting and additional uncertainty regarding the occurrence (Kumar et al., 2018). The 2013 rule required only prime contractors to disclose cyber events to the DoD within 72 hours of detection. Prime and subcontractors must report cyber intrusions to the DoD within 72 hours under the new rule. This reporting system has various flaws that could slow the reporting process and confuse the incident observed.

The 72-hour period is too short for contractors to investigate and report the incident. This new rule requires contractors to (1) review computers, servers, specific data, user accounts, contractor information systems, and other systems on the contractor's network that may have been compromised; (2) obtain a "DoD-approved medium assurance certificate" to report the incident; (3) report the incident to the DoD; and (4) "isolate malicious software" related to the incident. DFARS 252.204-7012's rigorous reporting requirements may not allow contractors enough time to comply. Subcontractors without the resources to identify, isolate, and report cyber events face this difficulty. A seventy-two-hour deadline is too short for these subcontractors to hire experts and report on the suspected infiltration. The seventy-two-hour limit will likely result in incomplete or delayed reports. Therefore, the DoD will fail to expedite cyber incident reporting.

CONCLUSION

In this article, we discuss a biometrics-based recognition system to protect individuals' privacy and maintain the safety of critical biometric databases and information. The system recognizes the users of the cloud based on the encrypted face template database that they have stored in the encryption domain. The user's privacy is protected by the biometric-based recognition system utilizing the extraction of facial features. In addition, it protects the privacy of cloud users by storing sensitive biometric data in an encrypted form within the cloud database and by providing Eigenfaces facial features for usage with the cloud. Implementing a biometric-based recognition system to determine a system's effectiveness and identify an individual without any loss of information in cloud computing is possible. The recognition system needs to be fixed because it cannot do better individual recognition within a limited database, and it takes too much time to match facial encryption and image data. This is the system's main drawback. Authenticating cloud users in real-time identification with extensive biometric databases requires significantly more storage space, processing power, and extensive computational resources than is now available. A series of successful attacks were launched against OPM in June of 2015, which revealed that millions of people were made aware of a sobering truth: their personal and, possibly, most valuable information was now in the hands of an anonymous organization. Despite this, strikes such as this are rapidly becoming the norm in this digital age, which sees conflict being waged on physical and cyber battlefields. A stricter cybersecurity policy created by the Department of Defense (DoD) develops a monitoring system that spans more information and covers a more significant number of prime and subcontractors. The DoD has taken a significant first step to protect its contractors from future assaults. However, the multitude of problems that have arisen for contractors as a direct result of this law reveals that this policy will not be sustainable, and it may cause several contractors to be unable to compete for future contracts with the Department of Defense. This analysis is only the first stage in a lengthy process to achieve complete cybersecurity. Shortly, we intend to design and build an automatic biometrics-based authentication system, as well as more adaptive encryption and quantization methods, to help alleviate the loss of cloud data and improve the performance of the proposed biometrics-based recognition system.

REFERENCES

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2019). Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential? *Asian Journal of Applied Science and Engineering*, *8*(1), 51–60. https://doi.org/10.18034/ajase.v8i1.12

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2021). Algorithm Policy for the Authentication of Indirect Fingerprints Used in Cloud Computing. *American Journal of Trade and Policy*, *8*(3), 231–238. https://doi.org/10.18034/ajtp.v8i3.651

Gunzel, J. A. (2017). TACKLING THE CYBER THREAT: THE IMPACT OF THE DOD'S "NETWORK PENETRATION REPORTING AND CONTRACTING FOR CLOUD SERVICES" RULE ON DOD CONTRACTOR CYBERSECURITY, *Public Contract Law Journal*, *46*(3), 687-712.

Gutlapalli, S. S. (2017). The Role of Deep Learning in the Fourth Industrial Revolution: A Digital Transformation Approach. *Asian Accounting and Auditing Advancement*, *8*(1), 52–56. Retrieved from https://4ajournal.com/article/view/77

Gutlapalli, S. S., Mandapuram, M., Reddy, M., & Bodepudi, A. (2019). Evaluation of Hospital Information Systems (HIS) regarding their Suitability for Tasks. *Malaysian Journal of Medical and Biological Research*, *6*(2), 143–150. https://doi.org/10.18034/mjmbr.v6i2.661

Kumar, S., Singh, S. K., Singh, A. K., Tiwari, S., & Ravi, S. S. (2018). Privacy-preserving security using biometrics in cloud computing. *Multimedia Tools and Applications, 77*(9), 11017-11039. https://doi.org/10.1007/s11042-017-4966-5

Malathi, R., and Raj, R. JR. (2016). An integrated approach of physical biometric authentication system. *Procedia Computer Science, 85*, 820-826

Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement, 7*(1), 50–57. Retrieved from https://4ajournal.com/article/view/76

Mandapuram, M., Gutlapalli, S. S., Bodepudi, A., & Reddy, M. (2018). Investigating the Prospects of Generative Artificial Intelligence. *Asian Journal of Humanity, Art and Literature*, *5*(2), 167–174. https://doi.org/10.18034/ajhal.v5i2.659

Masala, G.L., Ruiu, P., Grosso, E. (2018). Biometric Authentication and Data Security in Cloud Computing. In: Daimi, K. (eds) Computer and Network Security Essentials. Springer, Cham. https://doi.org/10.1007/978-3-319-58424-9_19

Obergrusberger, F., Baloglu, B., Sänger, J., Senk, C. (2012). Biometric identity trust: toward secure biometric enrollment in web environments. In: International Conference on Cloud Computing. Springer. 124-133.

Patel, A. R. (2020). Biometrics-based access framework for secure cloud computing. 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 1318-1321, https://doi.org/10.1109/CSCI51800.2020.00246

Reddy, M., Bodepudi, A., Mandapuram, M., & Gutlapalli, S. S. (2020). Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study. *ABC Journal of Advanced Research*, *9*(2), 103–114. https://doi.org/10.18034/abcjar.v9i2.660

Sabri, H. M., Ghany, K. K. A., Hefny, H. A. and Elkhameesy, N. (2014). Biometrics template security on cloud computing. 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, 672-676. https://doi.org/10.1109/ICACCI.2014.6968607

Tahir, H., and Tahir, R. (2008). Biofim: Multifactor authentication for defeating vehicle theft. In: Proceedings of the world congress on Engineering, London, UK.

Vinoth, K. M., Venkatachalam, K., Prabu, P., Almutairi, A., & Abouhawwash, M. (2021). Secure biometric authentication with de-duplication on distributed cloud storage. *PeerJ Computer Science,* https://doi.org/10.7717/peerj-cs.569

Yaacoub, J. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues, and future trends. *Microprocessors and Microsystems, 77*, 103201. https://doi.org/10.1016/j.micpro.2020.103201

--0--