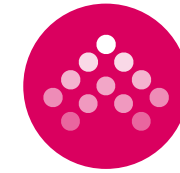


Toward Secure M3M Authentication for S3 Object Storage

Michael Geiger, Andreas U. Schmidt

22nd International Conference on Applied Computing 2025
Porto, 2nd November, 2025



wbh
WILHELM BÜCHNER
HOCHSCHULE

Eine Hochschule der Klett Gruppe

wb-fernstudium.de

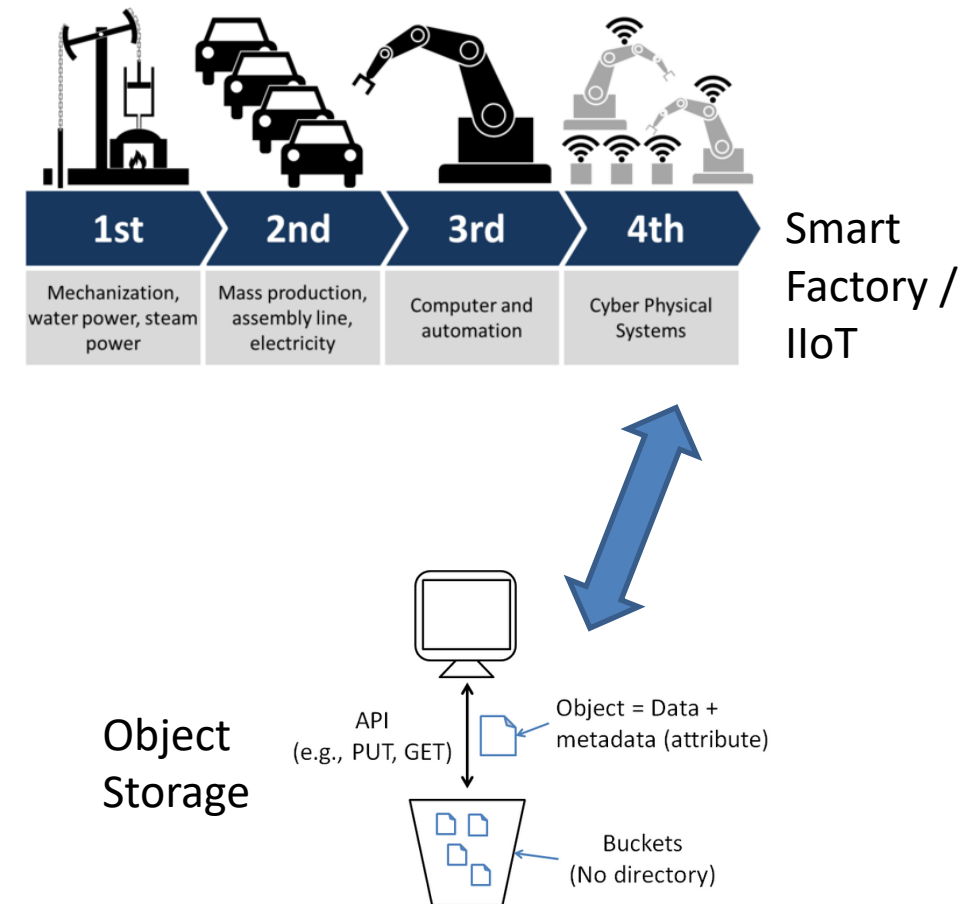
Object Storage in Smart Factories and IIoT

IIoT likes Object Storage

- Scalable, cost-effective data storage
- Handles massive sensor/machine data
- Enables real-time analytics & automation
- Supports digital twins & predictive maintenance
- Integrates with automated workflows
- Powers unified data lakes for data science

Amazon S3 is one of the most important services

- Security, scalability, HA, long-term archiving, ... data sharing via cloud
- Added benefits
 - AWS IoT Core, Greengrass, edge solutions
 - AWS analytics / AI tools

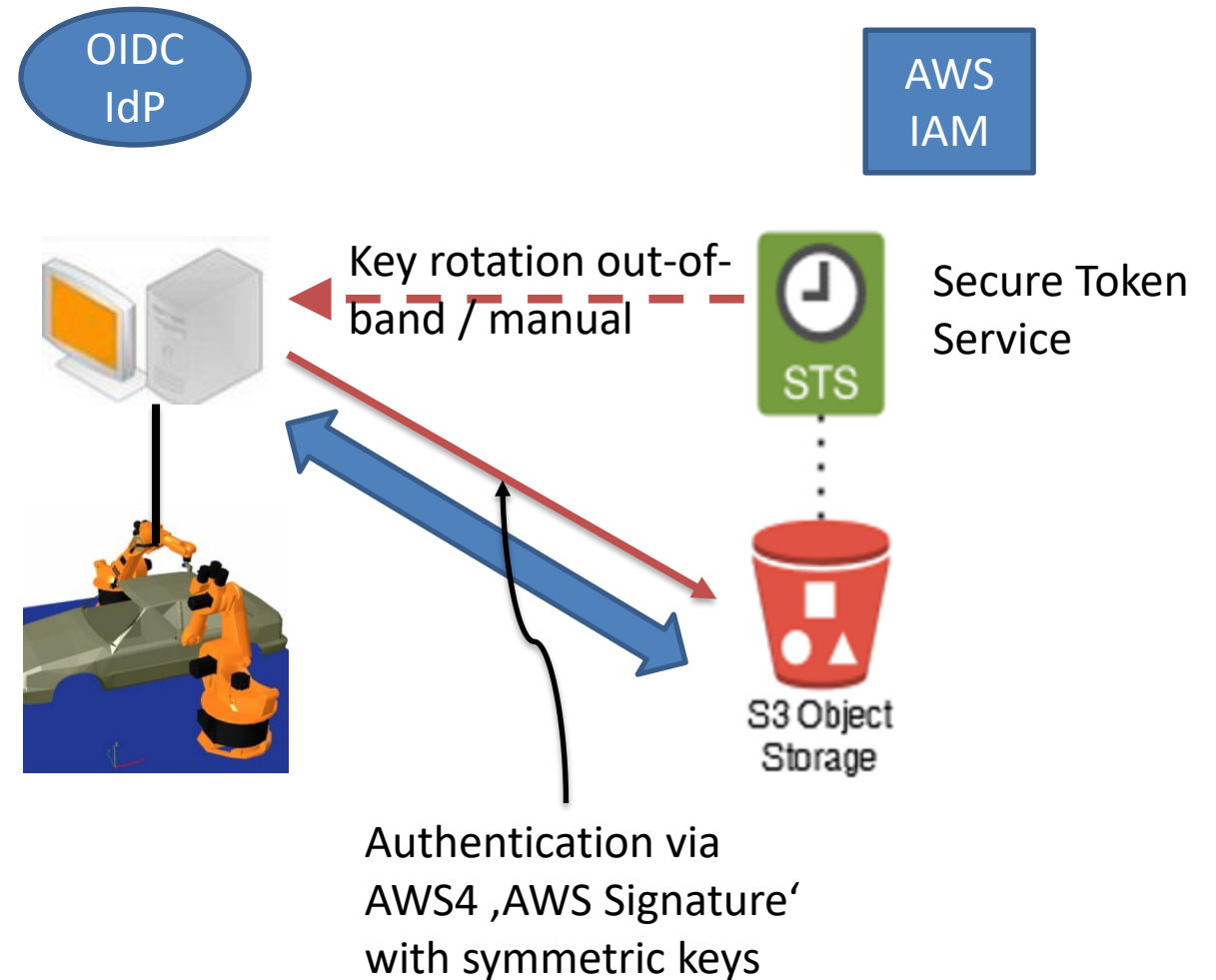


Images: Wikimedia Commons

S3 has Some Practical Problems

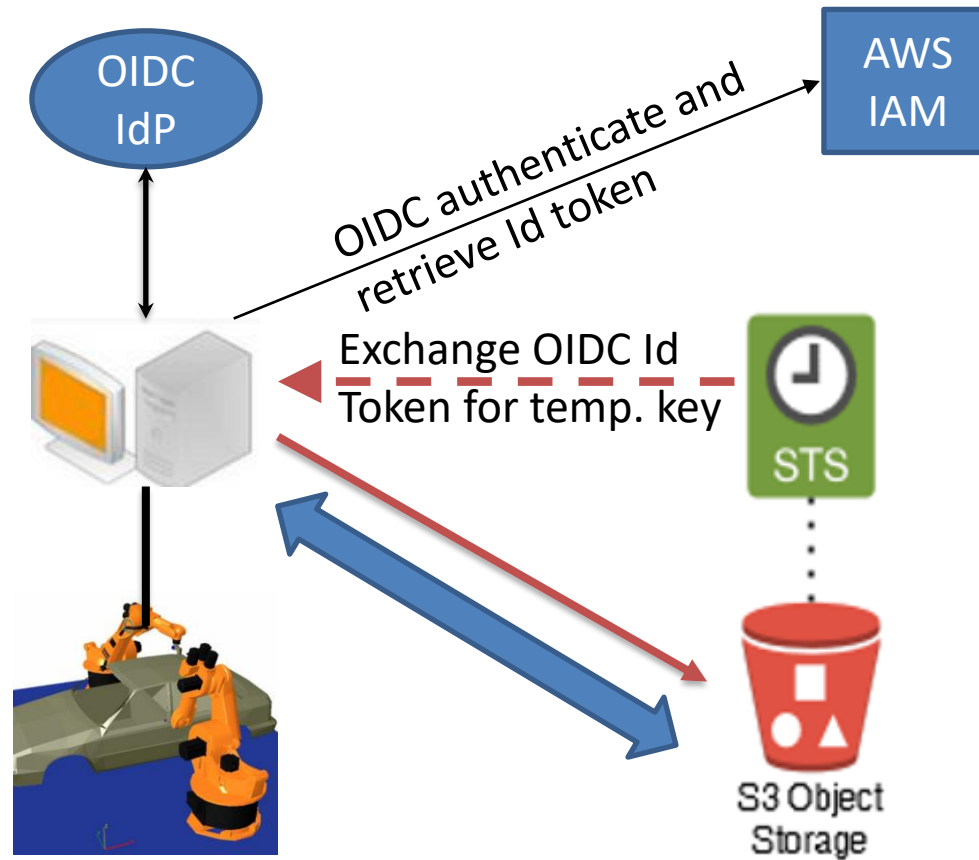
- AWS4 protocol uses simple, symmetric key authentication
- S3 buckets common, but often insecure in devel. cycles, causing risks in production.
- AWS4 keys stored insecurely, key rotation manual and disrupts automated production.
- Credentials leaked in source code, no strict abstraction leads to exposure.
- *AWS STS with OIDC offers temporary keys but support is limited.*
- Public/unprotected buckets sometimes undetected, enabling data breaches.
- Reused or abandoned buckets increase supply chain attack risk.
- Automated, secure key management lacking, threatening production continuity.

S3 with simple AWS4 method has security issues and risks production disruption



Indirection Solution via AWS IAM with OIDC

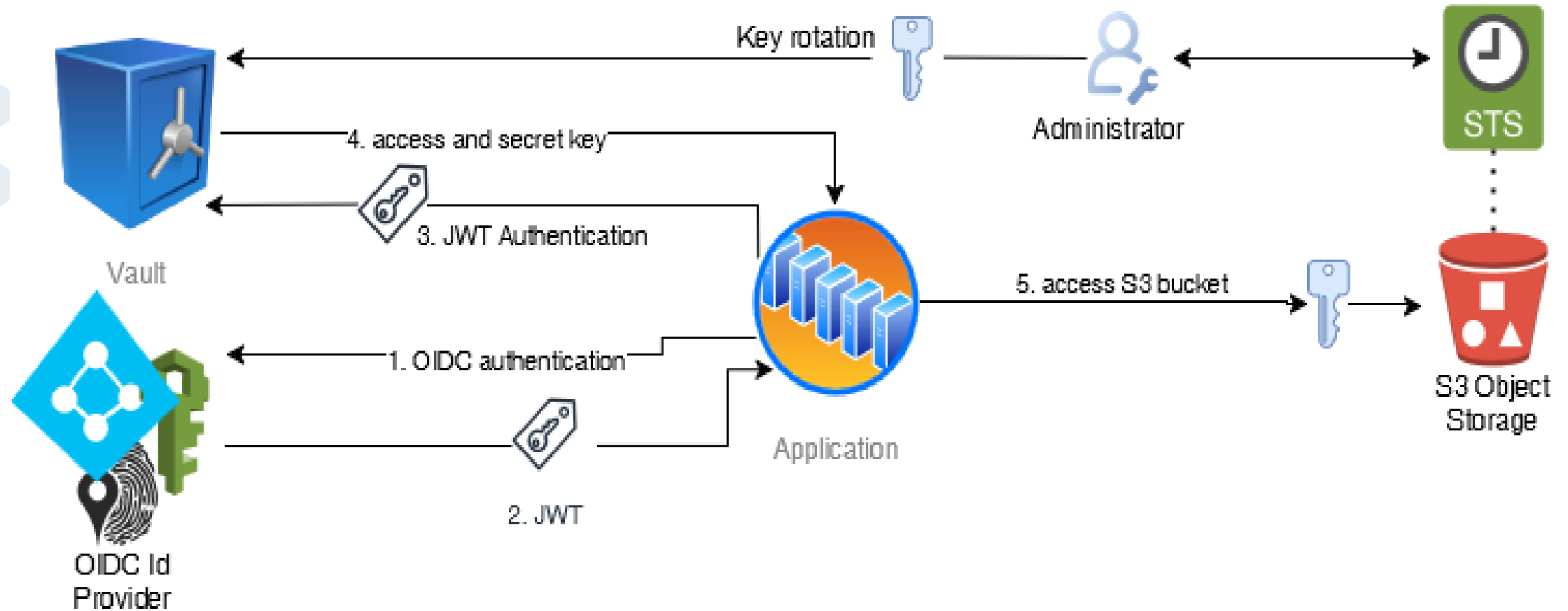
- One key at a time
- Dependency on connectivity to IdP and IAM
- Limited vendor support



S3 Object storage and support for STS with OIDC

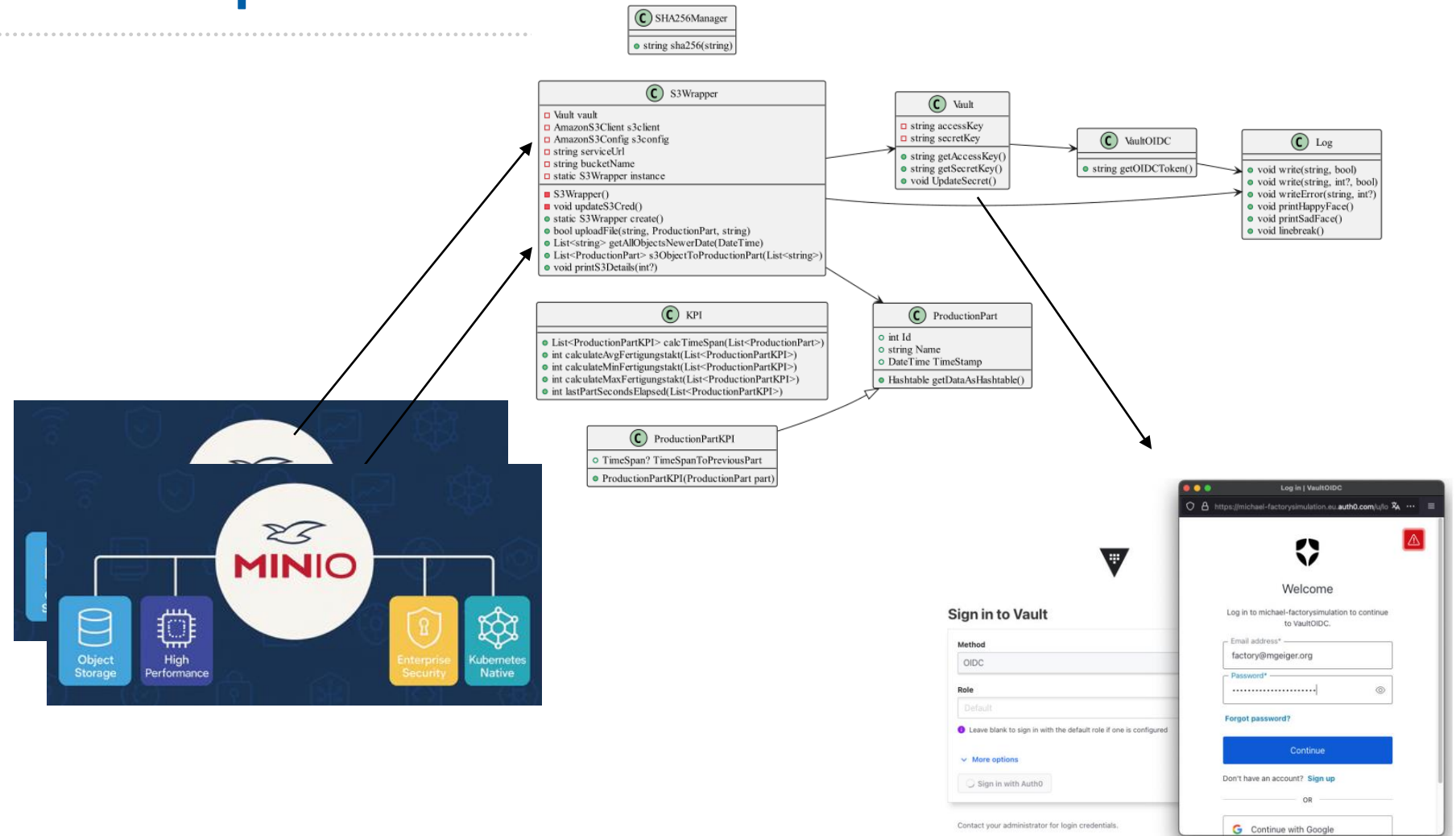
Product	STS	OAuth/OIDC
Amazon S3	✓	✓
<u>Ceph</u> Object Gateway	✓	✓
Dell/EMC ECS	✓	✗ (but SAML)
Dell/EMC Isilon	✗	✗
<u>MinIO</u>	✓	✓
NetApp ONTAP	✗	✗
NetApp <u>StorageGrid</u>	✗	✗
Nutanix Objects	✗	✗
<u>PureStorage</u> <u>FlashBlade</u>	✓	✓
<u>Qumolo</u>	✗	✗

Security Architecture with OIDC/PAM Authentication



Implementation Components

- OIDC IdP: Auth0
- STS Endpoint: MinIO
- S3 Endpoint: MinIO
- PAM: Hashicorp Vault
- FactorySimulation (C#)



- [illegible]

Solution?

- This is a workaround with some specific benefits
 - Full S3 authentication with OAuth/OIDC is not coming anytime soon
 - Key control – that may be good for compliance
 - Options for Risk Mgmt. / Disaster Recovery Scenarios ...
 - Less dependency on external entities
 - Works with all S3 implementations like Azure's or Google's

References

- Bhatt, S. (2024). Security and Compliance Considerations for Running SAP Systems on AWS. *Journal of Sustainable Solutions*, 15(4), pp. 72–86.
- Continella, A., Polino, M., Pogliani, M. and Zanero, S., 2018. There's a Hole in that Bucket!: A Large-scale Analysis of Misconfigured S3 Buckets. *Asia-Pacific Computer Systems Architecture Conference*, pp. 1-6.
- Geiger, M., 2025. FactorySimulation, <https://github.com/tux1337/FactorySimulation>**
- K, U., Sai Keerthan, N. K., Kumar Musunuru, N. and Beena, B. M., 2024. Cloud-Infused AWS Services: Automobile Database Management System. *2024 2nd International Conference on Networking, Embedded and Wireless Systems (ICNEWS)*, Bangalore, India, 2024, pp. 1-7, doi: 10.1109/ICNEWS60873.2024.10731084.
- Mishra, S., Kumar, M., Singh N. and Dwivedi, S., 2022. A Survey on AWS Cloud Computing Security Challenges & Solutions. *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2022, pp. 614-617, doi: 10.1109/ICICCS53718.2022.9788254.
- Siemens (2024). The True Cost of Downtime 2024. Available at:
https://assets.new.siemens.com/siemens/assets/api/uuid:1b43afb5-2d07-47f7-9eb7-893fe7d0bc59/TCOD-2024_original.pdf [Accessed 07 September 2025].



Thank You for Your Attention!

Q & (A)

Wilhelm Büchner Hochschule
Hilpertstraße 31
D-64295 Darmstadt
<http://www.wb-fernstudium.de>