Advances in Artificial Intelligence of Things, highlighting Semantic Interoperability and Cyber-Security with AI-Powered Embedded Finance Example

*Martin Serrano, Wahhed Ashraf,
Subhasis Thakur and John Breslin
Insight SFI Research Centre, Ireland
(University of Galway)
name.surname@[insight-centre.org]
(*Corresponding Author)

Bardia Khorsand and Richard
Walsh Banking and Payment
Federation of Ireland - BPFI
bardiakhorsand.consultant@bpfi.ie
richard.walsh@bpfi.ie

Ihsan Ullah and Umair
Hassan University of Galway
Galway City, Ireland Ireland
umair.ulhassan; ihsan.ullah
name.surname
@{universityofgalway.ie}

Abstract—**The rapid advances in Artificial Intelligence (AI) technology and the race for developing the best AI-powered application is generating that data interoperability, data protection and data privacy became priorities that must be addressed in each AI-powered design. Cyber-security techniques from IoT and AI must converge to ensure data sharing and data exchange following best practices and ensure privacy preservation and regulatory compliance. Data coming from smart sources (IoT devices) and used in AI applications, shall be provided with full cyber-security capabilities. Conceptually, AI-powered solutions include both high levels of interoperability, transparency and capabilities to securely interpret and analyse data close to the source (edge-IoT) and thus through the use of semantic models advanced data processing capabilities are possible. This paper uses best cybersecurity practices and explore the integration between AI-Technologies and the IoT systems, enabling more smart interactions and more sophisticated intelligent and complex services. This paper also introduce an implementation example with focus on AI-powered complex analytics and smart wallets as novel example on how securing Know-Your-Customer (KYC) and Embedded Finance (EmFi) operations. Finally this paper underlines concerns about the role of semantics supporting levels of interoperability at large and transparency by means of AI explainability aspects in AIoT applications.**

Keywords—Artificial Intelligence, Internet of Things, Cyber-Security, Authentication and Authorization, Distributed Identities, Embedded Finance, Semantic Interoperability, AIoT Solutions.

I. INTRODUCTION

The current Artificial Intelligence (AI) landscape is changing drastically as a result of the rapid advances developing AI technology. The most novel AI-powered solutions must provide better AI and IoT systems convergence and likewise seamless integration with the regulations in relation to data protection. The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) and its fast evolving convergence by means of data production in one hand and data consumption on the other is consolidating the novel area of Artificial intelligence of Things (AIoT) where data management operations are ensured together with the conditions for data interoperability [1] and systems reliability. The race for developing the best IoT-powered applications motivates that AI-powered systems must include the latest advances on cyber-security and data protection technology. AI-Powered systems bring new challenges in relation to data protection and systems control. The integration of AI-powered solutions with IoT-generated knowledge is not merely a technological upgrade; it is an enabled catalyst for autonomous services and sustainable digital transformation**,** laying the groundwork for resilient, adaptive, and human-centric AIoT environments**.** AIoT solutions also demand that user identity and other sensitive information shall be non-interoperable across multiple databases allowing to various organizations benefit from the use of full or pieces of these information. A secure way to enable this is by fragmenting the information and decentralize the permission to access it. It is well-known exposing personal data imposes elevated risk to cyberattacks and security breaches. A highly sensitive and vulnerable infrastructure necessitates the frequent creation of new accounts for different data services, such as online cybersecurity services, leading to a proliferation of potentially decentralized data repositories.

This paper addresses novel advances in Artificial Intelligence of Things, an emerging area bringing the smartness from Internet of Things devices and Artificial Intelligence capabilities in using data from the data sources including physical devices to enrich the so-called multi-modal data processing and the advantages in using machine learning and deep learning capabilities for capturing and processing data through a transformation process for finding the most near-by word defined by the probability and taking the multiplicity of option from the generated multimodal outputs. Highlights on semantic data interoperability and explaining the advances in cybersecurity [2] following regulation and technology advances are also described as part of the cybersecurity demands necessary in any AI-powered solution.

The remainder of this paper is as follows: **Section II** introduces the necessary cybersecurity capabilities and the possible impact of AI over the emerging area of embedded finance and explains the role of semantics in enabling interoperability across AI-powered solutions. **Section III** introduces the various relevant functionalities to ensure cybersecurity, in terms of systems authentication and authorisation, data accessibility and data protection, including the use of decentralized ledger technologies (DLT). **Section IV** introduces the architectural design of the proposed AI-powered cybersecurity framework with an open source implemented wallet enabling edge-intelligence together with cybersecurity. Component descriptions are included and details in how them are integrated with AI application in Embedded Finance explained. **Section V** describes the experimental setup used to validate this AI-powered secure architecture, focusing on Embedded Finance use cases in the context of a large initiative for improving financial services at large scale. The reference experiments are to demonstrate the scalability of the cybersecurity framework. Finally, **Section VI** concludes the paper by summarizing key findings and identifying future research directions, particularly in line with growing regulatory demands in Privacy and Data Protections.

II. AI-POWERED CYBERSECURITY CAPABILITIES

AI-powered solutions concerns both high levels of interoperability by means of using digital data sources and reduce cybersecurity risk [3]. In one hand an alternative for high levels of data interoperability can be achieved with advanced text-based prediction engines (LLMs). LLM's takes an input (prompt) and predicts the most contextually appropriate output (response), based in the multi-modal inputs enabling natural human-AI interactions. Technically, an LLM is a deep machine learning model**,** often based on data transformer architectures**,** trained on massive datasets of text to identify/learn patterns, context, and using semantics in language**.** Once trained, an LLM can predict and/or identify the closes coherent word/text, answer questions, translate languages, summarize information, or even run reasoning.

In the other hand AI-powered cybersecurity is more complex to achieve and requires high-level capabilities, cybersecurity must evolve alongside intelligence. Figure 1 summarises the overall capabilities to secure an AI-powered systems. Core capabilities include threat detection and prediction, where machine learning and deep learning models analyse network traffic, user behaviour, and system logs to identify anomalies, zero-day attacks, and advanced persistent threats (APTs). Cybersecurity capabilities must operate in real-time and at scale, leveraging techniques like behavioural analytics, anomaly detection, and predictive threat modelling to anticipate breaches before they materialize.

A) AI-powered Cybersecurity

Cybersecurity capabilities must represent real time protection and adaptive defence and automated response using intelligent mechanisms named AI-driven approach. AI-driven cybersecurity systems must be resilient to recover from potential attacks, provide dynamic access control, and enable automated incident response, reducing the time between detection and mitigation. Data integrity and privacy protection require secure AI model training through federated learning, homomorphic encryption, and adversarial robustness to prevent data poisoning or model inversion attacks. Finally, effective governance and explainability are critical—AI-powered cybersecurity capabilities that should provide transparent decision-making, continuous risk assessment, and regulatory compliance to ensure that intelligent systems remain resilient and human-trustworthy.

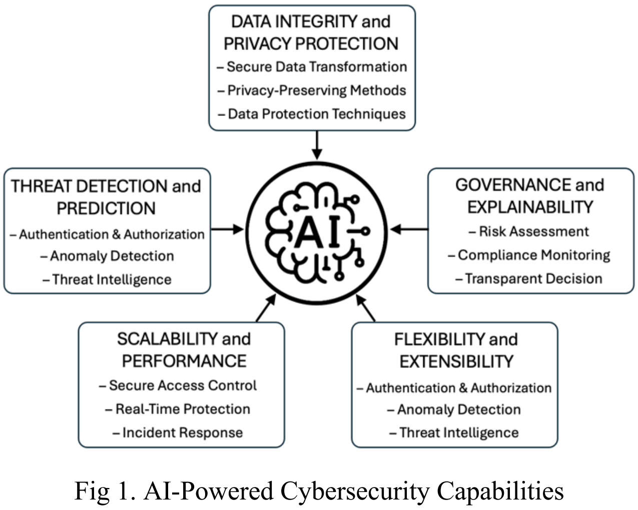

DATA INTEGRITY and PRIVACY PROTECTION
– Secure Data Transformation
– Privacy-Preserving Methods
– Data Protection Techniques
THREAT DETECTION and PREDICTION
– Authentication & Authorization
– Anomaly Detection
– Threat Intelligence
AI
GOVERNANCE and EXPLAINABILITY
– Risk Assessment
– Compliance Monitoring
– Transparent Decision
SCALABILITY and PERFORMANCE
– Secure Access Control
– Real-Time Protection
– Incident Response
FLEXIBILITY and EXTENSIBILITY
– Authentication & Authorization
– Anomaly Detection
– Threat Intelligence

Fig 1. AI-Powered Cybersecurity Capabilities

The following are the high-level capabilities provided by the Federated AAI and APM subsystems.

- **Secure Access Control**: This capability ensures that only authenticated and authorized users can access the system or application resources alike the protection of assets.
- **User Authentication**: This capability verifies the identity of users through reliable and secure methods i.e., SIOPv2.
- **User Authorization**: This capability determines and enforce what authenticated users are permitted to do within the system or application based on their roles, permissions, or policies.
- **User Experience:** This capability ensures that the authentication process is possible without compromising security, thereby improving user satisfaction.
- **Scalability and Performance:** This capability builds upon authentication and authorization mechanisms that can scale with the growth of users and system demands without degrading the operation and system performance.
- **Flexibility and Extensibility:** This capability designs the system in a way that supports future expansion, such as adding new security methods or services integration.

B) Embedded Finance

Embedded Finance (EmFi) is a result of integration financial services with customer offerings in non-financial institution platforms [4]. EmFi is a modern method of finance, and they have a significant role in easing up the process and events of financial activities. Therefore, there isa high demand for correlation between knowledge and usage of EmFi services. Interest in Internet information about EmFi hiked up in recent years that shows its favourability among internet users.

The usage of EmFi relies on the optimization of the Internet services and the financial data applications. Two separate domain activities but that converge to facilitate a new generation of secured services and applications. There are incidents that set an increasing risk for EmFi, first search for internet information about Financial data which increases cybersecurity threats [5]. Second, the use of global web Internet information about EmFi activities increases the vulnerability of a system to protect its integrity [6].

The EmFi facilitates rendering of financial services through websites, mobile applications and business processes of non-financial organizations in a direct way. EmFi is a process in which payments or any other type of EmFi application is possible through usage of application programming interface (API) and/or other offline methods. Different organizations with different financial services and products can use EmFi to improve upon user journeys through delivering subject services and products. EmFi providers are not necessarily banks. They are mostly software companies that partner with banks to develop technologies for EmFi products to facilitate users' experience with banking services. In this paper we strive to address EmFi is a valuable financial innovation and has its own application and market share in the financial industry and it benefits with AI and IoT convergence known AIoT, therefore, there is a huge opportunity for AIoT and EmFi. AIoT can improve EmFi customer experience and unlock a huge market opportunity [7]. Therefore, AIoT is a new concept where technology and applications benefits, the use in EmFi defines scenarios where banking provide solutions for customers subscribing to those EmFi services.

The EmFi has a set of problems arising from the payment process itself induced from the diversity of EmFi products and particularly in the payment industry. Flexibility, reliability, and speed were among the facilities that EmFi industry provide to customers. Other examples of EmFi applications include, real-estate loaning apps, shopping-cart platform, customer loyalty APIs, digital wallets platforms, accounting software apps, shopping online, scheduling employees to work shifts, or managing inventory, and etc. [8]. This is essential to note that customer experience with EmFi is a combination of satisfying their needs through a non-financial platform that provides financial services.

EmFi was enabled by changes in technology and commerce, 50 percent of card spending in the US and 33 percent of global card spending now takes place online [9]. Vast majority of small and midsize companies in the US use software solutions provided by EmFi platforms to manage their everyday business [6]. This wave of revolution in customer and users experience eased by EmFi platforms is boosted by open banking innovation and new laws and regulation in Europe and the US. Market share of EmFi industry, according to McKinsey's market sizing model [7], reached $20 billion in revenues in the United States alone in 2021. According to expert estimates, the market could double within the next three to five years. However, the EmFi field remains vague and unexplored. The players are many and not well known by all parties. The aspect of competition in this market, more particularly, is fierce and has not been explored.

III. Requirements in Cybersecurity & EmFi

Cybersecurity in AI-powered systems is a major concern attracting both academic and industrial focus due to its significant impact on technology adoption. Authentication and authorization are prioritized areas where existing methods often fall short. Typically, deployment systems implement separate methods for authentication and authorization, with few integrated solutions available. The study in [10] introduces an adaptive, blockchain-based approach for both authentication and authorization in IoT, implemented in Java and its extensive evaluations demonstrate the approach effectiveness in meeting various requirements while maintaining low operational costs. Adaptive authentication is a flexible, risk-oriented method of verifying identities that uses up-to-date data to assess the risk associated with a user's actions, dynamically allocates authentication measures based on various factors, and adjusts security measures in response to current events to enhance system security and prevent unauthorized access. Adaptive authentication enhances identity verification by dynamically assessing risks in real-time and adjusting security measures accordingly. It employs risk profiles, which categorize access requests into varying risk levels and determine the necessary authentication methods, such as biometrics or PINs [11] utilizes AI and machine learning to continually refine these assessments and automate decision-making, thereby bolstering security and trust. Adaptive authentication offers a complex solution that surpasses the capabilities of traditional and multi-factor authentication systems. Adaptive authentication leverages various techniques to assess and mitigate risks within an authentication system, enabling decisions on user access based on factors such as location, behaviour, and user attributes. This method integrates dynamic and static elements to tailor authentication requirements according to the sensitivity of the accessed resource. Benefits of this approach include frictionless authentication for trusted entities, enhanced risk management through intelligent assessments, continuously updated security protocols accommodating Bring Your Own Device environments [12].

Singh et al. [13] introduced the Resilient Risk-based Adaptive Authentication and Authorization (RAD-AA) framework, engineered to dynamically adjust based on risk scores and trust profiles, thereby enhancing system security. It is underscored that credential theft has become a predominant attack vector in recent cyber incidents, facilitating unauthorized system access via techniques such as token manipulation. This highlights the critical need for robust authentication and token-based authorization systems. RAD-AA offers mayor resilience using threat models including STRIDE and PASTA against established standards like OAuth 2.0, OpenID Connect [14], and SAML 2.0, and assessed. Furthermore the application of ML methods within RAD-AA to precisely evaluate transaction risks, significantly complicating the efforts of adversaries to initiate and sustain attacks on critical infrastructure.

A detailed analysis and overview of research on Context Modelling for Adaptive Authentication systems using Systematic Mapping Study (SMS) and Systematic Literature Review (SLR) methods to identify key properties for these models in adaptive systems is provided in [15]. A thorough revision and evaluation of cybersecurity technologies like Microsoft .NET Passport, Liberty Alliance Project, Kerberos-based solutions, and digital certificates along with PKIs for developing AAIs are provide in [5], and concluded that no single technology is superior; each has its pros and cons, and an effective AAI should integrate multiple technologies and strategies. IoT security practices, technologies, and standards used in recent research, offering a practical guide and overview of recent research efforts in these areas are analysed in [16]. Analysis of the Authentication and Authorization Advancements for the Internet of Things, categorizing security solutions are studied in [17] which reviews current Access Control techniques and trends, examining the evolving cyber-attack landscape and zero-trust networking challenges, and discuss the application of Access Control across key domains such as Cloud Computing, Blockchain, IoT, and Software-Defined Networking, and explores business adoption strategies and integration into cybersecurity and network architectures. A scalable identity management scheme using blockchain technology to enhance identity protection and traceability, which integrates blockchain with Reed-Solomon encoding and Certificateless Aggregate Signature to protect user information, with nodes storing parts of the encoded data block are introduced in Ma and Qian [18]. The authors argue that unlike traditional solutions, their approach prevents single points of failure, secures identities, and tracks malicious users, allowing single-upload access across multiple applications without multiple passwords. A survey on Adaptive Authentication, which dynamically selects the most suitable user authentication methods based on contextual factors such as location and device proximity are included in [19]. Despite its potential to revolutionize the prevalent password-based authentication system, practical applications in everyday life are still limited. To improve the design of adaptive authentication, they conducted a comprehensive review of the existing research, identifying current challenges and proposing future directions. A Multi-Factor Authentication for cloud Infrastructure systematic survey, highlighting the urgent need for robust protective measures against unauthorized service used in cloud computing is conducted in [20]. Advancements in computing and techniques, has generated to move from single-factor Authentication relied on methods like usernames and passwords to multi-factor authentications.

The process from understanding and using obfuscation models to sophisticated cryptographic algorithms, have exposed vulnerabilities in systems. As a result, multi-factor authentication, which employs multiple simultaneous authentication factors, has become essential for bolstering cloud security. The regulations continue towards providing an extensive number of factors to review that influence the adoption and effectiveness of multi-factor authentication systems, ultimately advocating for a unique, biometric-based authentication factor that does not require specialized equipment, thereby enhancing security and mitigate risks.

To ensure secure, standardized credential exchange, AAI integrates OID4VCI [21], facilitating a reliable protocol for identity information exchange. This protocol supports secure, consent-based sharing of credentials, which reinforces user autonomy over personal data while streamlining the verification. In addition, AAI is designed with rigorous adherence to the latest security protocols and privacy standards, establishing a resilient defence against common vulnerabilities and emerging threats in the digital identity landscape [22]. The platform is built to accommodate current digital verification needs while maintaining flexibility for future advancements in decentralized identity, ensuring that it remains adaptable to the evolving requirements of secure, privacy-preserving access management, EmFi providers are non-financial institutions that provide financial products, the nature of EmFi organisations is different than banks. Non-financial organisations acting as EmFi providers have various opportunities to enhance customer experience by offering new services and applications. This is of vital importance to also understand that EmFi providers do not incur hefty overhead associated with operating as a bank. The field of operation for EmFi organisations extends from retailers, business software, online marketplaces, platforms, telecom companies, and equipment manufacturers [8]. All these fields experienced innovation and lively activities in EmFi industry and for the past years there is a demand saturation and maturity for the banking sector because there are mature banks with historical track records of attracting new customers.

EmFi industry is a young industry with significant entry rate for new businesses and organisations. In the other side the banking sector is mature industry with lowers arrival rates compared to EmFi industry. This framework dictates the role of new entry for EmFi new arrivals compared to incumbent banks. Banks have two options. First, to acquire EmFi organisations and assimilate them into their already running business or to compete with stand-alone EmFi organisations.

EmFi providers target gaps in the financial market which are the areas where bank coverage is reduced or not active. However, for EmFi non-financials a significant increase in demand, and they are at the beginning of the road in different fields of EmFi applications ranging from deposit and payment to issuing, and lending products. Customer satisfaction and flexibility of the product by APIs on the run are examples of these gaps. An unanswered gap remains by given available funds of large banks, why do they not penetrate EmFi market and acquire all EmFi related firms. EmFi industry is a unique industry that requires significant know-how in Internet technology, data, AI and ICT infrastructure and many other unique skills. Banks do not pose those skills, thus those gaps presents a significant barrier to entry for banks. EmFi operates dynamically adjusting activities according to the evolution of services, it is rather difficult for banks to keep up with the pace since banks present traditional slow responses to services changes.

IV. AI-POWERED CYBER-SECURITY FRAMEWORK

The design and development of AI-powered cybersecurity architectures are evolving based on the emerging demands from AI and IoT convergence, they must address the security gaps and go beyond traditional infrastructures defences and include data protection, resilience and consider the AI-Powered capabilities to address the unique complex risks of AI-driven and systems. In general terms secured AI-powered EmFi implementation refers to deploying federated Authentication and Authorisation Infrastructures where Deployed components are responsible for managing secured processes called FAAID. In this regard, Federated components act as the mechanism for serving as a reference authority ensuring secure and seamless access control across all architecture modules. FAAID is a prototype implementation withing a European project with the aim to demonstrate and include AI-Powered cybersecurity capabilities. FAAID secured infrastructure aims to provide a comprehensive solution for managing digital identities, verifiable credentials, and access control policies, promoting streamlined and consistent security practices throughout the system. FAAID addresses secured AI-powered capabilities:

Identity Management:

- Creating, storing, and verifying digital identities and associated credentials.
- Issuing, managing, and revoking verifiable credentials

Authentication:

- Authentication relied on Verifying the identity of users and entities attempting to access the system.
- Leveraging verifiable credentials for secure authentication.

Authorization:

- Controlling access to resources based on verified credentials and defined policies.
- Enforcing fine-grained access controls and permissions

Interoperability:

- Utilizing open standards like OpenID for Verifiable Credential Issuance (OID4VCI) [21] and OpenID for

Verifiable Presentations (OID4VP) [23] for cross-system integration.
- Enabling federated identity and access management across different domains.

FAAID approach acts as a robust, standards-based solution for identity and access management, serving as the backbone of secure access control across the entire system. FAAID provides a cryptographically secure mechanism for the issuance and management of Verifiable Credentials, empowering users with enhanced control over their digital identities and permissions. Utilizing Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), the system enables users to manage identities independently, reducing reliance on a central authority strengthening both privacy and trust.

Cybersecurity in AIoT systems must go beyond traditional perimeter defences to address the unique risks of AI-driven and IoT-enabled ecosystems. Effective security involves a multi-layered approach, combining data protection, secure communication, model integrity, and regulatory compliance. AIoT key frameworks and strategies should include:

A) Zero-Trust Architecture (ZTA)
- AIoT systems should adopt a zero-trust model, where no device, user, or application is inherently trusted.
- AIoT provides continuous identity verification, dynamic access controls, and micro-segmentation prevent lateral movement in case of a breach.

B) Secure Data Management and Encryption
- All data in transit and at rest must be protected using end-to-end encryption (TLS/SSL, AES-256) at AIoT.
- Tokenization and data anonymization reduce the exposure of sensitive user information in AIoT.
- Fragmented and decentralized storage (similar to data sharing) can reduce single points of failure for AIoT.

C) Federated Learning and Privacy-Preserving AI
- Instead of centralizing sensitive data for model training, federated learning enables local AIoT training on edge devices.
- Combined with homomorphic encryption or secure multi-party computation, this approach prevents raw data exposure while improving AIoT model performance.

D) AI-Driven Threat Detection and Response
- Real-time anomaly detection and behavioural analytics powered by AIoT can identify zero-day attacks and Advanced Persistent Threats (APTs).
- Integration of automated incident response (e.g., isolating compromised AIoT nodes or revoking credentials) minimizes reaction time and potential damage.

E) Adversarial AI and Model Integrity Protection
- AIoT models themselves can be targets for attacks, such as data poisoning, model inversion, or adversarial inputs.
- Techniques like robust training, model watermarking, and continuous integrity checks are required to ensure trustworthy AIoT operations.

F) Regulatory Compliance and Auditability
- AIoT cybersecurity strategies must align with data protection regulations (GDPR, CCPA, ISO/IEC 27001).
- Implementing continuous auditing, explainable AIoT (XAI) frameworks, and secure logging mechanisms helps maintain regulatory trustworthiness and forensic readiness.

The extensive use and regular use of these strategies transform AIoT from a vulnerable data ecosystem into a resilient and adaptive environment capable of safeguarding sensitive information, maintaining system integrity, and supporting sustainable digital transformation.

The main feature of AIoT and its applicability for EmFi revolves around the provisioning of financial services provided by third parties without losing the control and operational efficiency, but it is the cybersecurity the mayor concern and what makes EmFi having not the 100% of acceptance however gradually Artificial Intelligence and the advanced technologies in decentralized cybersecurity are being incorporated in payments and financial operations. At large extent, EmFi solutions enable non-financial platforms to offer services like payments, lending, or insurance directly within their ecosystems, but doing so and beyond technological security requires adherence to financial regulations such as Know Your Customer (KYC), Anti-Money Laundering (AML), and data protection laws like GDPR or CCPA. EmFi AI-driven architectures are essential, allowing edge-enabled decisions and secure and reliable data operations alike communication between financial institutions and digital platforms.

Additionally, high availability and low-latency performance are critical to ensure frictionless user experiences. Scalability is also a key requirement, as EmFi services must handle large volumes of transactions while supporting dynamic onboarding and cross-border operations.

Cybersecurity for EmFi is paramount because financial transactions are inherently sensitive and attractive to attackers. Security regulations demands multi-factor authentication (MFA), measures must include end-to-end encryption, tokenization, and secure API gateways to prevent data breaches and unauthorized access. Moreover, EmFi providers must implement robust incident response and compliance auditing mechanisms, ensuring that any cyber event is detected and addressed swiftly. An AI-powered cybersecurity approach not only protects users and financial partners but also builds the trust and regulatory alignment necessary for the optimal protection of EmFi.

V. Reference Implementation & Experiments

FAAID reference implementation extends the AIoT ecosystem into an emerging Embedded Finance domain as a demonstration that smart and intelligence can be done with Zero Trust & Security Levels following data, cybersecurity and AI regulations(s) [24]. Embedded Finance refers to the seamless integration of financial services—like payments, lending, insurance, or investments—directly into third party digital platforms. Thus, instead of going to a traditional bank or financial app, financial tools can be exactly accessed where they are needed, such as paying for a ride inside a mobility app, getting instant financing at an e-commerce checkout, or receiving micro-insurance within a travel booking platform. These scenarios are made possible and widely used through

APIs, commonly described Banking-as-a-Service (BaaS) platforms, which allow non-financial businesses to embed financial capabilities without becoming full-fledged banks themselves. e.g., zero-trust architecture, AI-driven secure data, etc.

In reference to the FAAID reference implementation, this paper highlights the security and protection services as they are the most relevant ones to ensure that AIoT follows Zero trust design principles. Figure 2 shows the workflow for creating and managing verifiable claims, (implemented in the context of the FAME project [25]) where an Issuer service process as shown. These claims are subsequently embedded in the ID token and can be utilized during authentication flows for verification purposes.

Purpose: To provide secure issuance of VOC credentials through standardized APIs.

Key Functions:

- Credential Generation: Creates credentials in compliance with W3C standards, allowing for proof of identity or attribute claims.
- Credential Formatting: Structures credentials to be portable and readable by various verifiers across ecosystems.
- Credential Issuance: Issues digitally signed credentials to users, ensuring data integrity and authenticity.

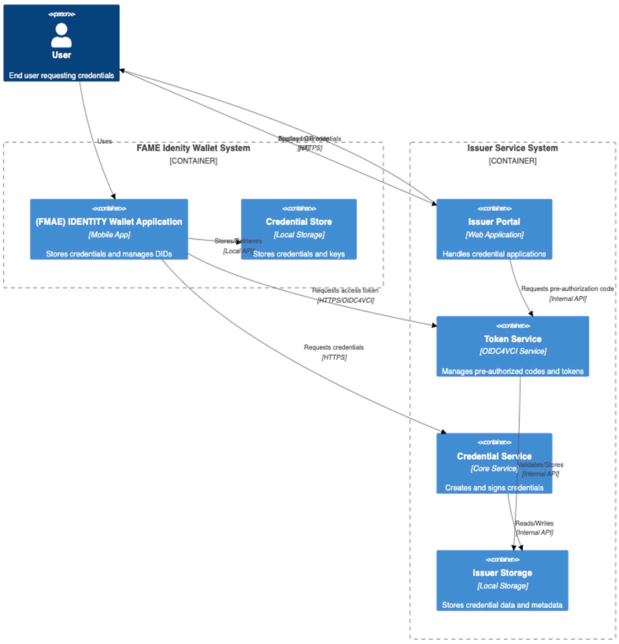


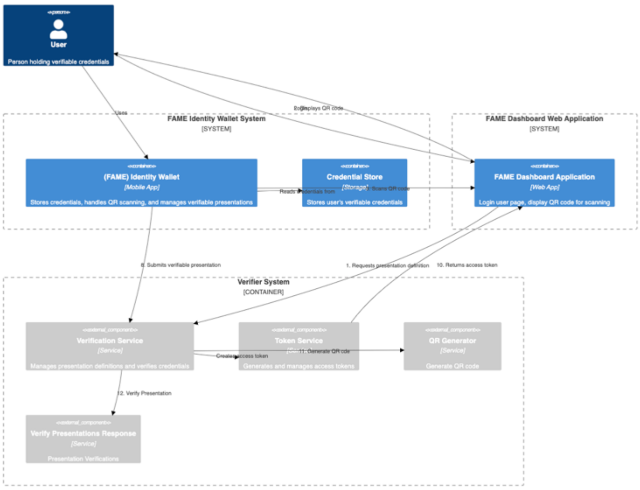
Fig 2. Verifiable Credential Issuer Service: Issuance Process

The Verifications service process, as depicted in Figure 3, outlines the steps involved in confirming the validity and authenticity of a user-provided Verifiable Credentials (VOC). This process ensures that the credential originates from a trusted Organization Authority (OA) issuer, thereby establishing its reliability. Additionally, the service authenticates the user during the verification process, ensuring that the individual presenting the credential is its rightful owner. This dual-layer verification enhances the security and trustworthiness of the system.

Purpose: To validate user-presented VOC credentials, ensuring authenticity and integrity before granting access or permissions.

Key Functions:

- Credential Verification: Verifies that the user-provided VOC credential originates from a trusted OA issuer, is still valid and has not been tampered with.
- vp_token Generation: Issues to the user a Verifiable Presentation Token (vp_token) as proof of successful verification, enabling access to resources.



«person»
User
Person holding verifiable credentials
Uses
2. Displays QR code
Login
FAME Identity Wallet System
[SYSTEM]
«container»
(FAME) Identity Wallet
[Mobile App]
Stores credentials, handles QR scanning, and manages verifiable presentations
Reads credentials from
«container»
Credential Store
[Storage]
Stores user's verifiable credentials
3. Scans QR code
FAME Dashboard Web Application
[SYSTEM]
«container»
FAME Dashboard Application
[Web App]
Login user page, display QR code for scanning
8. Submits verifiable presentation
1. Requests presentation definition
10. Returns access token
Verifier System
[CONTAINER]
«external_component»
Verification Service
[Service]
Manages presentation definitions and verifies credentials
Creates access token
«external_component»
Token Service
[Service]
Generates and manages access tokens
11. Generate QR code
«external_component»
QR Generator
[Service]
Generate QR code
12. Verify Presentation
«external_component»
Verify Presentations Response
[Service]
Presentation Verifications

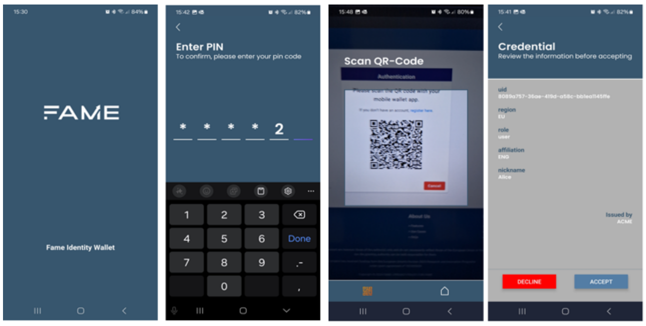
Fig. 3 AAI Verifier Service: DID Self-Sovereign Process

The user-side client enables seamless participation in the VOC issuance and verification processes. It retrieves VOC from the Verifiable Credential Issuer Service, securely stores them in an encrypted database on the user's device (FAAID Identity wallet) which is implemented using Open Source Spherion VOCs wallet and facilitates their presentation to a Verifier Service for Authentication & Authorisation and IDs.

Purpose: Act as the user-side client, enabling the user to participate the VOC issuance and verification processes.

Key Functions:

- **Credential Retrieval**: Retrieves an issued VOC from a Verifiable Credential Issuer Service.
- **Credential Secure Storage**: Maintains retrieved VOCs in an encrypted database on the user's personal device.
- **Credential Presentation**: Presents a VOC stored on the user's personal device to a Verifier Service.



Enter PIN

To confirm, please enter your pin code

Scan QR-Code

Please scan the QR code with your mobile wallet app.

Credential

Review the information before accepting

uid
8089a757-36ae-419d-a58c-bbleal145ffe

region
EU

role
user

affiliation
ENG

nickname
Alice

Issued by
ACME

Fig. 4 DID Identity Wallet, 2-FA, QR Code and Credential

VI. Conclusions and Next Steps

In This article we reviewed the definition for EmFi organisations. We provide an overview of the industry, and we offer insight into the competition arising between EmFi providers and established traditional banks.

The emerging Artificial Intelligence of Things (AIoT) ecosystem defines a transformative convergence where Internet of Things (IoT) devices evolve from connected data collectors into more autonomous and at certain level intelligent actors. IoT systems focused on sensing and transmitting environmental or operational data to cloud-based platforms for analysis. However, the exponential growth of IoT connected devices has led to unprecedented data volumes, velocity, and variety, challenging conventional cloud-only processing bridging Edge-Intelligence as part of the IoT extensions. AIoT addresses this by embedding machine learning and cognitive capabilities directly into IoT ecosystems, enabling real-time decision-making, edge intelligence, and context-aware automation.

The AIoT paradigm from IoT sensing infrastructure into a core element in self-adaptive, predictive, and value-generating AI-powered system.

We conclude that the knowledge gap poses a significant hurdle on the entry of the banking sector to penetrate EmFi industry. The speed of changes in industry framework is another barrier to entry for banks.

Acknowledgments

Acknowledgements: This work has been partially supported by the FAME project EU-Horizon Europe 101092639, The SENSE project EU-Digital Europe 01167948 and The Insight SFI research Centre for Data Analytics supported by Science Foundation Ireland Grant Number SFI/12/RC/2289_P2.

Disclosure of Interest: Certain commercial products or company names are identified here to describe our study adequately. Such identification is not intended to imply recommendation or endorsement by any of the authors or co-authors, nor is it intended to imply that the products or names identified are necessarily the best available for such purpose.

References

[1] Gutt, Federico, Martin Huschka, and Alexander Stolz. "Cascading Effects Analysis Enabled by Semantic Interoperability in the Resilience Data Space.", Position Paper, 2024

[2] Fernandez-Gago, Carmen, et al. "Trust interoperability in the Internet of Things." Internet of Things 26 (2024): 101226.

[3] More, Stefan. "Trust Scheme Interoperability: Connecting Heterogeneous Trust Schemes." Proceedings of the 18th International Conference on Availability, Reliability and Security. 2023.

[4] Fusion, Kore. "Embedded finance: this decade's largest creator of value." A Kore Fusion Report, New York, available at: https://korefusion. com/embedded-finance-this-decades-largest-creatorof-valu (2021).

[5] Lopez, Javier; Oppliger, Rolf and Pernul, Günther. 2004. Authentication and authorization infrastructures (AAIs): a comparative survey. Comput. Secur. 23, 7 (October 2004), 578–590. https://doi.org/10.1016/j.cose.2004.06.013

[6] Ozili, Peterson K. "Assessing global interest in decentralized finance, embedded finance, open finance, ocean finance and sustainable finance." Asian Journal of Economics and Banking 7, no. 2 (2023): 197-216.

[7] Badirova, Aytaj et al. "Towards Robust Trust Frameworks for Data Exchange: A Multidisciplinary Inquiry." Open Identity Summit 2024. Gesellschaft für Informatik eV, 2024.

[8] Dresner, Andy, Albion Murati, Brian Pike, and Jonathan Zell. "Embedded finance: Who will lead the next payments revolution." McKinsey & Company 18 (2022).

[9] McKinsey's Global Banking Revenue Pools, 2022; McKinsey's Global Payments Map, 2022.

[10] Achraf Fayad, Badis Hammi, Rida Khatoun. An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach. 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Oct 2018, Shanghai, China. pp.1-7, 10.1109/SSIC.2018.8556668

[11] Javed Shah, "what is Adaptive Authentication and Authorization?" January 3, 2023, https://www.1kosmos.com/authentication/adaptive-authentication/

[12] Cuñat, Salvador et al. "Secure, Trusted, Privacy-Protected Data Exchange in an-Edge-Cloud Continuum Environment." IoT Edge Intelligence. Cham: Springer Nature Switzerland, 2024. 201-231.

[13] Singh, J., Patel, C., & Chaudhary, N. K. (2022, December). Resilient Risk-Based Adaptive Authentication and Authorization (RAD-AA) Framework. In International Conference on Information Security, Privacy and Digital Forensics (pp. 371-385). Singapore: Springer Nature Singapore.

[14] OpenID Connect Core 1.0 Specification https://openid.net/specs/openid-connect-core-1_0.html

[15] Anne Bumiller, Stéphanie Challita, Benoit Combemale, Olivier Barais, Nicolas Aillery, et al. "On Understanding Context Modelling for Adaptive Authentication Systems". ACM Transactions on Autonomous and Adaptive Systems, 2023, 18 (1), pp.1-35. doi: 10.1145/3582696

[16] Trnka M, Abdelfattah AS, Shrestha A, Coffey M, Cerny T. Systematic Review of Authentication and Authorization Advancements for the Internet of Things. Sensors (Basel). 2022 Feb 10;22(4):1361. doi: 10.3390/s22041361. PMID: 35214259; PMCID: PMC8963074.

[17] Lewis Golightly, Paolo Modesti, Rémi Garcia, Victor Chang, Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN, Cyber Security and Applications, Volume 1, 2023, 100015, ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100015.

[18] Ma, B., Qian, H. A scalable identity management scheme via blockchain: Identity protection and traceability. Peer-to-Peer Netw. Appl. 18, 1–12 (2025). https://doi.org/10.1007/s12083-024-01866-w

[19] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. 2019]. A Survey on Adaptive Authentication. ACM Comput. Surv. 52, 4, Article 80 (July 2020), 30 pages. https://doi.org/10.1145/3336117

[20] Otta SP, Panda S, Gupta M, Hota C. a Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. Future Internet. 2023; 15(4):146. https://doi.org/10.3390/fi15040146

[21] "OpenID for Verifiable Credential Issuance (OID4VCI)," [Online]. Available [Online]. Available: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[22] Ghirmai, Siem et al. "Self-sovereign identity for trust and interoperability in the metaverse." 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta). IEEE, 2022.

[23] Foundation (n.d.), "OpenID for Verifiable Presentations," [Online]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html/.

[24] Abie, Habtamu, Trenton Schulz, and Reijo Savola. "Adaptive Security and Trust Management for Autonomous Messaging Systems." arXiv preprint arXiv:2203.03559 (2022).

[25] A. Mavrogiorgou, et al., "FAME: Federated Decentralized Trusted Data Marketplace for Embedded Finance", [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10215814.