World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

A proposed architecture for securing fintech applications using Hyperledger fabric in a hybrid cloud

Md Jafrin Hossain [1] , Umme Nusrat Jahan [1,*] and Rejuan Haque Rifat [2]

[1] *Knight Foundation of Computing and Information Sciences, Florida International University Miami, USA.*
[2] *Department of Computer Science and Engineering BRAC University, Dhaka, Bangladesh.*

World Journal of Advanced Research and Reviews, 2024, 23(02), 543–550

Publication history: Received on 16 June 2024; revised on 05 August 2024; accepted on 07 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2376

Abstract

The possibility of making secure transactions and keeping funds securely in fintech services highly depends on the security measures at the application layer. The growth of cutting-edge technologies opens many options for adopting a secure architecture for fintech organizations. However, most financial organizations, such as banks and MFS (mobile financial systems), still use conventional architecture to develop and host applications in any public or private cloud. The study considers this and proposes a comprehensive architecture based on the consortium blockchain, Hyperledger fabric in a hybrid cloud environment to make a more secure fintech application. The proposed architecture is a theoretical approach which is not yet been tested at the industry level. Nevertheless, consortium blockchain and hybrid cloud performance to secure any application have already proved individually in different fields. The research team also compared existing architecture and proposed one for evaluation. Hence, adopting this architecture will be one step ahead for making safe transactions and securing funds and data in this cyber world.

Keywords: Fintech; Blockchain; Hyperledger Fabric; Hybrid Cloud; Cybersecurity

1. Introduction

In this era of technology, it is tough to think of even a single day without making any online transactions. Hence, a good number of companies are founded based on financial services. Some offer regular banking services, and some offer more than those. Some financial companies are not typical banks but provide core services like cash in, cash out, and real-time funds transfer. These centralized-based financial services make life easier to live.

Cashless practice became more popular when COVID-19 hit the sudden world pandemic worldwide. However, the fact is that the risk factors of using online or mobile-based financial services are also higher in any number. Even though all the service providers are committed to entirely secure financial services. However, the possibility of a safe transaction depends on so many factors. Some of them are absolutely in the hands of the service providers, whereas some rely on the end users.

End users' risk factors can be mitigated by educating them

about the latest cyberattacks and a minimum surface-level idea of not falling into the trap of social engineering or other phishing attacks. However, the possibility of a safe transaction highly depends on the security measure of applying the financial platform. Different offerings and use cases are available because of the many options for developing a fintech application. However, even though there are a lot of tools and technologies out here, the number of architectures for developing a fintech application is a few. Moreover, to host the application, there are mainly only three options – public, private, or hybrid cloud.

* Corresponding author: Md Jafrin Hossain, Umme Nusrat Jahan

The research studies different architectures and proposes a new cutting-edge technology, blockchain-based architecture in the hybrid cloud, to adopt for fintech applications.

2. Literature review

2.1. Fintech

Fintech refers to incorporating technology into financial services provided by financial institutions such as traditional banks, mobile financial services, and e-money providers. The term was likely first used by Citicorp's chairman, John Reed, in the 1990s within the context of the Smart Card Forum [1]. The concept of fintech encompasses innovative financial services and business models that enhance the delivery, usage, and process of financial services [2]. The development of fintech has shifted the focus from internal solutions to customer-centric B2C and B2B solutions and inter-organizational provider-focused B2B solutions [3].

2.2. Consortium Blockchain

A consortium blockchain is a decentralized ledger system in which multiple organizations collaborate to verify transactions and maintain consensus on the network's transactions. Regarding blockchain technology, the system combines the efficiency and privacy of private blockchains with the decentralization and transparency of public blockchains [4]. Using consortium blockchains in the financial sector has improved cross-border payments' speed and efficiency and reduced fraud risk. Several financial institutions, including the R3 consortium, are currently working on developing a blockchain-based platform for cross-border payments [5].

2.3. Hyperledger Fabric

The Hyperledger Fabric platform is a permissioned blockchain technology designed to facilitate the developing and deploying secure, scalable, and highly customizable blockchain applications. In addition to being part of the open-source Hyperledger project family, Fabric provides a robust framework for developing and deploying enterprise-grade blockchain systems [6]. This technology supports the execution of distributed applications written in standard programming languages, which is one of the key innovations of Fabric. This allows multiple nodes to execute these applications consistently, giving the impression that they are being executed on a single globally distributed blockchain computer. This unique feature differentiates Fabric from other blockchain platforms and makes it a highly attractive option for organizations seeking to implement blockchain solutions [7].

2.4. Hybrid Cloud

This technology architecture combines the advantages of both public and private cloud computing. A hybrid cloud computing system incorporates public, private and on-premises infrastructure. This architecture provides a coordinated, managed, and portable experience across all components. This configuration allows organizations to benefit from the strengths of both on-premises and public cloud environments, creating a flexible and secure infrastructure [8]. The hybrid cloud combines the strengths of public and private cloud environments, taking advantage of the resource scalability of public clouds and the control of private clouds to create a more cost-effective and flexible solution [9]. In a typical hybrid cloud setup, critical data are hosted on a private cloud. In contrast, other data are hosted on a public cloud, which offers an effective solution for privacy protection.

2.5. Related Works

According to X. Huang and X. Du, 2013, the commonly used approach for data privacy protection is using cryptographic algorithms, which come with the drawback of intensive computation. As an alternative, this study suggested implementing a hybrid cloud consisting of public and private clouds, where sensitive data is separated and only non-sensitive data is outsourced to the public cloud [10]. The research team introduced a novel scheme to ensure data privacy. The scheme's effectiveness is tested in real-world network environments like Amazon EC2.

In their study, Y.-T. Lee et al. (2020) presented a blockchain-based time bank system built using the Hyperledger Fabric framework. The system utilizes blockchain technology to execute and record services and focuses on using autonomous smart contracts and a Hyperledger Fabric-based banking system comprising three distinct channels [11].

In another study, McSeth Antwi et al., 2021, evaluated the suitability of private blockchain technologies for healthcare applications. The team conducted experiments using Hyperledger Fabric to test various criteria and use cases for healthcare applications. The evaluation results indicated the potential advantages of private blockchain technologies, including compatibility, scalability, and security [12].

In the study conducted by Elghaish et al. (2022), a new financial management system utilizing Hyperledger fabric and chain code technology was proposed to tackle challenges in financial management practices within construction projects [13].

In another research, Shanmugapriya and Kavitha (2019) investigated the application of big data analytics in the healthcare industry. The study strongly emphasized the importance of implementing hybrid cloud computing for the secure storage of private healthcare data [14]. The proposed model mainly focuses on a tri-party authenticated key-agreement protocol based on bilinear pairing cryptography for secure communication and a decoy technique for data protection. In their model, the decoy technique features the display of decoy files to potential attackers while the original data remains hidden and encrypted, providing complete security for patient information. The proposed method is efficient and offers double security by granting access to the original data only to authorized users. The study by Son et al., (2019) showed a novel access control system named "Access Control Model in Hybrid Cloud for Healthcare Systems," which is proposed to tackle the threat of cyber-crimes and security vulnerabilities in the system [15]. The proposed system comprises two levels of access control:

i) Safeguarding shared patient data among hospitals and ii) Securing private patient information that the treating physician can only access. The model was tested in a real-case application and shown to manage security and privacy concerns at both levels effectively.

The study conducted by Darwish et al., (2020) introduced a blockchain-based hybrid algorithm to improve privacy in the existing system. The proposed algorithm mainly focuses on a hybrid encryption technique and generates a unique digital signature for data before it is outsourced to data centers [16].

3. Existing architecture

The existing software development ecosystem is so vast. The availability of many frameworks, libraries, and other tools makes it tougher to pick the suitable one. There is no clear winner of which language, framework, or library is the best for creating software, whether it is a fintech application or anything else. However, among all of them, Node.js, Django, Spring, and ASP.NET Core are the topmost frameworks that are widely used in fintech applications.

3.1. Blockchain Based Applications

There are a good number of blockchain-based applications in the industry. Even though blockchain was mainly implemented to develop crypto offerings like Bitcoin and Ethereum, nowadays, the usability of blockchain is accepted in almost every niche sector in the fintech ecosystem.

3.2. Different Categories of Blockchain

There are mainly four types of blockchains currently available. Some use cases in fintech and cryptocurrency of blockchains are given below

- Public Blockchain: Bitcoin, Ethereum
- Private Blockchain: Ethereum Private Network
- Hybrid Blockchain: Swisscoin
- Consortium Blockchain: Hyperledger Fabric

3.3. Cloud Based Applications

Nowadays, it is almost impossible to think of any global or well-recognized app-based fintech service provider without hosting its backend in any cloud platform. So, it can be said that almost every fintech application has some of its existence in cloud-based platforms.

4. Architecture

4.1. Architecture Breakdown

In the context of Hyperledger fabric architecture [17], there are mainly - Peers, Orderers, Channels, Leger and Smart Contracts, which consist of this consortium blockchain. This blockchain offers something very crucial in terms of financial organization. This consortium blockchain is modular because it provides a Membership Service Provider (MSP) enabling managing different financial organization departments in terms of peers. Every user can be treated as a

single peer for creating the network. Then again, orderers will verify transactions using the consensus method; all the transactions can be stored in the ledger. In addition, if needed, some extra functions can be adopted using smart contracts.

The following [Figure: 1] shows a sample network architecture of Hyperledger fabric [18].

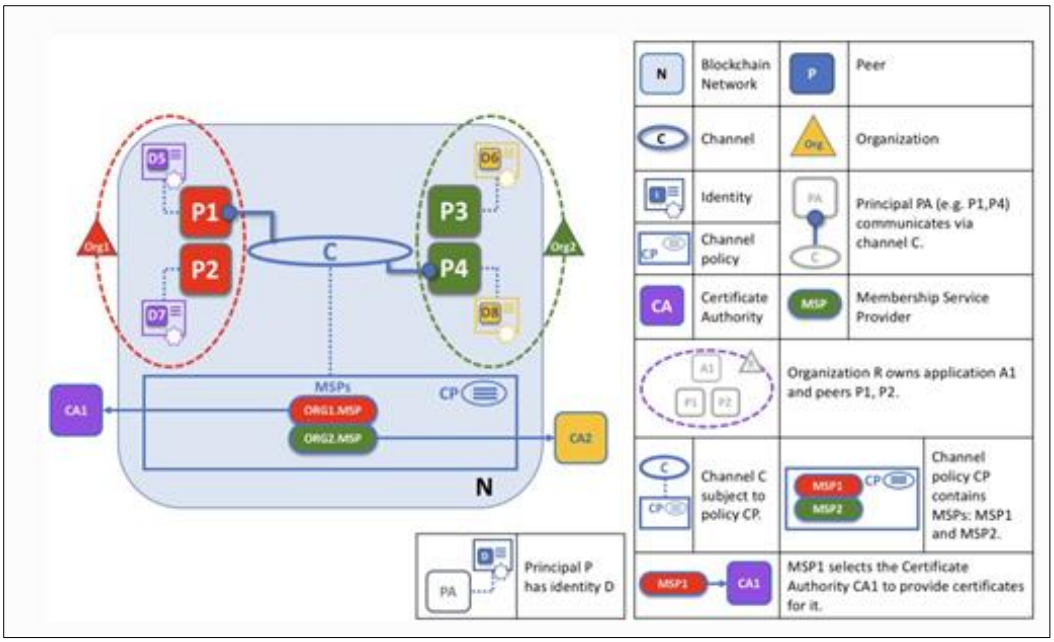

Figure 1 Architecture of Hyperledger Fabric; Ref: Linux Foundation

4.2. Proposed Architecture

The sole purpose of the study is to propose a new architecture based on Consortium Blockchain, Hyperledger Fabric in Hybrid Cloud. The Core part of the architecture is the implementation of Hyperledger Fabric in the Fintech Platforms or Applications. As discussed in the previous section, a permission-based blockchain is one of the best features of Hyperledger Fabric. Again, due to its modularity, it is possible for the typical financial organization, including fintech organizations and even regular banks, to adapt it for the departments inside the organization. For instance, the following [Figure: 2] shows multiple departments of a fintech organization managed by Hyperledger Fabric.

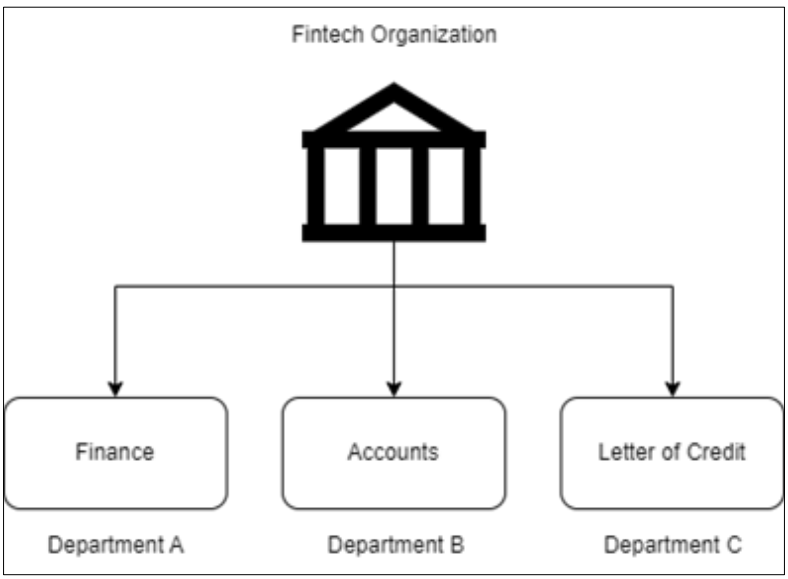

Figure 2 Single Organization

In addition, most of the fintech organizations and all the banks are somehow regulated by a country's central bank. To expand, Hyperledger Fabric is also implementable with a country's existing banking ecosystem. Because of its permission-based secure architecture, it is elementary for the ecosystem to implement governance regulation, which is important to a country's traditional banking system. The following [Figure: 3] shows how the central bank can regulate regular banks and financial organizations using the consortium blockchain, Hyperledger Fabric.

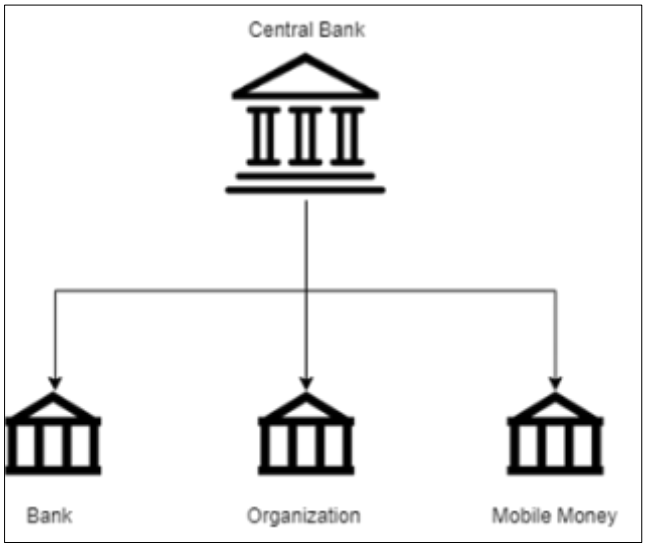

Figure 3 Central Bank

Hence, the research team shows how Hyperledger Fabric can be implemented in terms of a single organization and the total banking ecosystem. The following [Figure: 4] shows the combination of previously given two use cases and finally combining those into one.

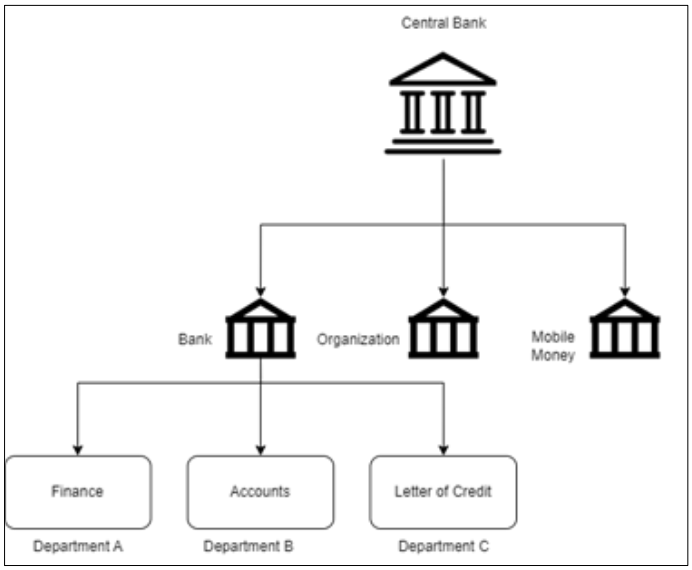

Figure 4 Central Bank Network

However, one of the biggest challenges of any organization, including Fintech, is to secure the data storage volume no matter which architecture it follows. In order to tackle this, some of them use an on-premises data center, and others rely on public cloud offerings. However, the fact is, in both cases, there are some pros and cons. The biggest problem with using an on-premises data center is the initial cost, capital cost, or CAPEX. On the other hand, managing this kind of server or data center is also a challenging task. Lastly, high availability is nearly impossible for on-premises solutions, even after ensuring everything. In terms of the public cloud, it solves a good number of obstacles. Among them, high availability, elasticity, and easily accessible new services are the main concerns that attract the organization for picking

public cloud over alternative ones. Nevertheless, the biggest issue with the public cloud is that the data's primary or physical location is outside or mostly far from the organization. Furthermore, sometimes, it is outside of the organization's primary country. The research team considers the issue in the topmost position and finally proposes a new proposal where Hyperledger Fabric can be implemented in Hybrid Cloud architecture. The team thinks picking one of the existing offerings for hosting the fintech applications is not optimal. Instead, if the benefits of both on-premises and public cloud can be achieved by ensuring the safety concern of the storage location, then it would be a great combination. To achieve the goal, the research team proposes some parts of the platform to keep on-premises, and some parts should be in the public cloud. Regarding any Fintech application, when any request comes to clients like mobile, browser, or desktop apps, it will first go through the Node.js-based API. The API will handle the router or any other operations and business logic. To host the API, any company may use any preferable hosting service, whether on the public cloud or on-premises. Then, the research team proposes implementing a Hyperledger Fabric network for the end users to make successful transactions. This permission-based blockchain will ensure security while making any transaction. To host Hyperledger Fabric with the help of Kubernetes Cluster, the research team proposes to use public cloud providers like IBM to implement this. It is because the computing power needed for this consortium blockchain is costly enough to set up on-premises. The research considers one of the most significant issues of the public cloud, which is a storage location, and proposes to keep persistent volumes in the on-premises private cloud attached to the Kubernetes Cluster. By adopting this architecture, any fintech Organization can ensure its security with the help of Hyperledger Fabric and mitigate the risk of the public cloud. The following [Figure: 5] shows a high-level overview of the blockchain network of the proposed architecture.

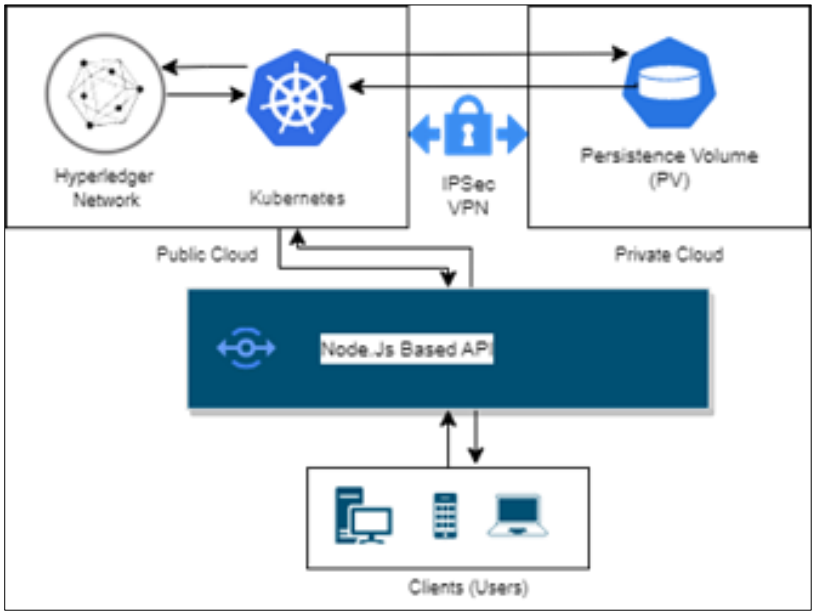

Figure 5 Blockchain Network

In addition, any fintech company may pick microservices over monolithic architecture to implement the proposed architecture. While implementing the architecture in microservices, not all the services may need a Hyperledger Network.

5. Comparison

The proposed theoretical architecture uses cutting-edge technologies to gain benefits from them and make the FinTech applications more secure for end-users.

- Framework: The proposed architecture uses the Node.js framework, which is famous for its performance. PayPal, a vastly used financial service provider, migrated to Node.js from Java for better performance [19].
- Consortium Blockchain: The architecture proposes implementing the application in consortium blockchain, Hyperledger Fabric, a permission-based blockchain with modularity and pluggable architecture [20].
- Hybrid Cloud: The research team also proposes a hybrid cloud architecture to host the fintech organization to gain the benefits of both public and private clouds.

So, the proposed architecture accepts all the benefits of cutting-edge technologies and implements comprehensively, hence, it is suggested to adopt the architecture for securing fintech applications.

5.1. Comparison with Regular Architecture

In a typical inter-banking system, a central server and database system form the backbone. Here, a backend API handles requests from various client applications on mobile or desktop. The following [Figure: 6] from the AWS reference illustrates the architecture of this regular banking application.

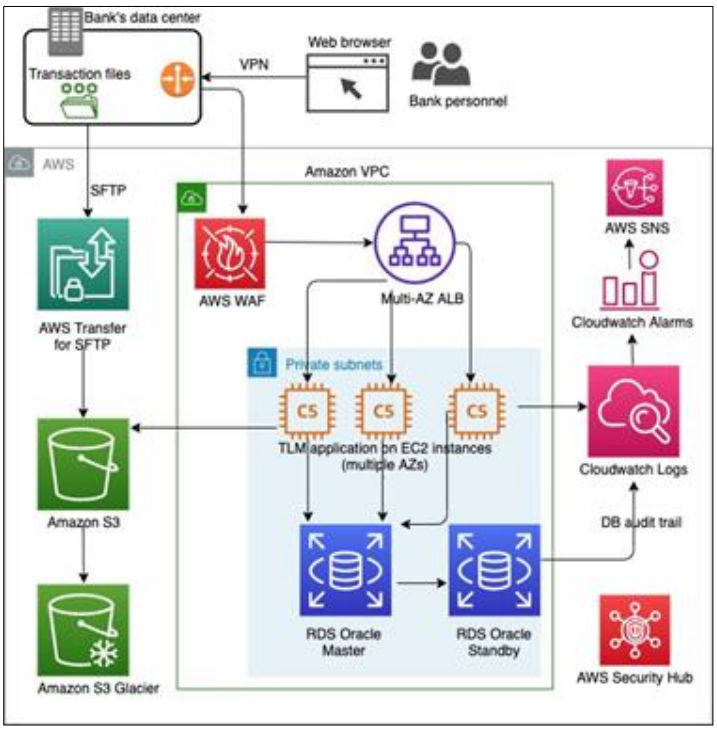

Figure 6 Regular Banking Architecture; Ref: AWS

This architecture mainly uses a backend system (API) serving responses from different client requests using multiple user interfaces like the web, android and iOS. In this regular architecture, some huge lacking can lead to massive losses in financial and data cases. In different cases, attackers can conduct various types of cyberattacks. Many options can be followed in terms of databases if attackers target them, e.g., SQL injection and phishing attacks. However, a simple mistake for any admin-level person managing the database can open the gate for access. However, due to its distributed architecture, Hyperledger is a better option considering that. On the other hand, facing fraudulent transactions is one of the worst experiences in the banking industry. However, if the typical banking system adopts a backend based on Hyperledger fabric, it is impossible to make instant fraud transactions because of the consensus mechanism.

5.2. Future work

The given architecture is a theoretical one, so the main future work that the research team focuses on is an industry-ready implementation of the proposed architecture. However, due to many cutting-edge technologies, one of the biggest challenges is to lower the cost.

6. Conclusion

The security of any fintech application is one of the biggest concerns for making a safe transaction nowadays. Even though there are a lot of frameworks and architectures for developing and hosting fintech applications, there are still some obstacles for all the existing architecture.

The research team proposes a theoretical architecture that combines one of the fastest frameworks, consortium blockchain and hybrid cloud. Combining all these in a single architecture, the research team proposes a comprehensive architecture for making FinTech applications more secure.

References

[1] T. Puschmann, "Fintech," Business &; Information Systems Engineering, vol. 59, no. 1, pp. 69–76, 2 2017. [Online]. Available: http://dx.doi.org/10.1007/s12599-017-0464-6

[2] I. Goldstein, W. Jiang, and G. A. Karolyi, "To FinTech and Beyond," The Review of Financial Studies, vol. 32, no. 5, pp. 1647–1661, 04 2019. [Online]. Available: https://doi.org/10.1093/rfs/hhz025

[3] A.-L. Mention, "The future of fintech," Research-Technology Management, vol. 62, no. 4, pp. 59–63, 2019. [Online]. Available: https://doi.org/10.1080/08956308.2019.1613123

[4] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," Int. J. Adv. Telecommun, vol. 11, no. 1, pp. 51–64, 2018.

[5] R. Bo¨hme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–38, May 2015. [Online]. Available: https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213

[6] H. Foundation, "About –," 9 2022. [Online]. Available: https://www.hyperledger.org/about

[7] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis,A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in Proceedings of the thirteenth EuroSys conference, 2018,pp. 1–15.

[8] "What is Hybrid Cloud? — IBM." [Online]. Available: https://www.ibm.com/topics/hybrid-cloud

[9] J. Lei, Q. Wu, and J. Xu, "Privacy and security-aware workflow scheduling in a hybrid cloud," Future Generation Computer Systems, vol. 131, pp. 269–278, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X22000279

[10] X. Huang and X. Du, "Efficiently secure data privacy on hybrid cloud," in 2013 IEEE International Conference on Communications (ICC), 2013, pp. 1936–1940.

[11] Y.-T. Lee, J.-J. Lin, J. Y.-J. Hsu, and J.-L. Wu, "A time bank system design on the basis of hyperledger fabric framework," in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1–3.

[12] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, "The case of hyperledger fabric as a blockchain solution for healthcare applications," Blockchain: Research and Applications, vol. 2, no. 1, p. 100012, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720921000075

[13] F. Elghaish, F. Pour Rahimian, M. R. Hosseini, D. Edwards, and M. Shelbourn, "Financial management of construction projects: Hyperledger fabric and chaincode solutions," Automation in Construction, vol. 137, p. 104185, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0926580522000589

[14] E. Shanmugapriya and R. Kavitha, "Medical big data analysis: preserving security and privacy with hybrid cloud technology," Soft Computing, vol. 23, no. 8, pp. 2585–2596, 2 2019. [Online]. Available: http://dx.doi.org/10.1007/s00500-019-03857-z

[15] H. X. Son, M. H. Nguyen, H. K. Vo, and T. P. Nguyen, "Toward an privacy protection based on access control model in hybrid cloud for healthcare systems," in International Joint Conference: 12th Interna- tional Conference on Computational Intelligence in Security for Infor- mation Systems (CISIS 2019) and 10th International Conference on EU- ropean Transnational Education (ICEUTE 2019), F. Mart´ınez A´ lvarez, A. Troncoso Lora, J. A. Sa´ez Mun˜oz, H. Quintia´n, and E. Corchado, Eds. Cham: Springer International Publishing, 2020, pp. 77–86.

[16] M. A. Darwish, E. Yafi, M. A. Al Ghamdi, and A. Almasri, "Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 3369–3378, 2 2020. [Online].Available: http://dx.doi.org/10.1007/s13369-020-04394-w

[17] "Architecture explained - hyperledger fabric documentation," 2018. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release- 1.3/arch-deep-dive.html

[18] "Peers - hyperledger fabric documentation," 2020. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/peers/peers.html

[19] B. Schwartz, "Analysis of PayPal's Node-vs-Java benchmarks," 5 2020. [Online]. Available: https://orangematter.solarwinds.com/2013/ 12/09/analysis-of-paypals-node-vs-java-benchmarks/

[20] "What is hyperledger fabric? — IBM." [Online]. Available: https://www.ibm.com/topics/hyperledger