**Hybrid Cloud Security and Architecture: Personal Research Contribution**

*Exploring encryption practices, biometric vulnerabilities, and cybersecurity trends through an architectural lens*

Author: Jared Alwyn  
Program Solution Architect, Salesforce & MuleSoft | Manager  
Affiliation: Graduate coursework for Master of Science in Information Technology  
Publication Date: July 2025  
Contact: https://github.com/Jalwyn

*Disclaimer: This document represents my individual contribution to a team research paper submitted for academic credit as part of a graduate-level course. It is republished independently for external reference and professional visibility. All opinions and analysis are my own and do not represent those of my academic institution or employer.*

# Data Storage and Encryption Methods

Hybrid encryption methods can be used to combine the performance efficiency (speed) of symmetric algorithms such as AES-256 along with the robust security of asymmetric security to offer a much fuller solution to cloud storage vulnerabilities.  
Agarwal et al. (2018) describe a hybrid cryptographic framework that leverages the encryption symmetric standard AES-256 for data encryption and asymmetric RSA for secure key distribution. Continuing this paraphrase, this would not only protect cloud storage data at the transmission and storage layers.  
Breaking these technical details down, it’s first important to understand symmetric AES-256. Basically, this is a fast, but efficient way to handle and encrypt data that is at our storage layer (data that is being stored on cloud). Asymmetric RSA basically helps in authentication by ensuring the encryption key isn’t exposed. This helps protect the storage and transfer of the data. A well suited combination.  
From my experience as a Sr. Solution architect designing Mulesoft-based integrations from different cloud environments such as Salesforce, I rely a lot on this hybrid approach to maintain compliance and performance during data transfer that might be at higher risk. With that being said, a cloud environment such as salesforce already uses AES-256 to encrypt data at rest as the standard and it being the largest CRM shows the reliability Salesforce put on the security architecture for this. As far as RSA, I recently shared an updated Architecture using Oauth 2.0 with PKCE and Ping identifier to secure access to our portals. The underlying validation of JWTs used asymmetric cryptography (RSA), to verify authenticity before allowing access. This architecture was highly highly requested among the enterprise architecture group as a modern standard.  
Countering this argument to using this in my solution from my Sr. Tech arch was that adding an extra layer such as asymmetric cryptography in this case might be overkill since symmetric AES-256 is already sufficient on its own, especially when using TLS to handle data flow. From my perspective, honestly this is a good observation however it doesn’t mean that TLS is completely immune from being compromised. In this situation if TLS was compromised, RSA would be a sufficient layer on top to provide additional security. They agreed and RSA stayed on the final solution with really maybe the project management aspect and cost of implementing it is an argument. This wasn’t brought up from the enterprise architecture perspective on the presentation though.  
From my own personal experience and that of feedback from enterprise architects reviewing my work, I think this is a highly effective solution that is well recognized in the industry, and I strongly support hybrid encryption as a best practice standard for enterprise systems using cloud storage.

# Security Risks and Threats in Biometric Systems

When considering fingerprint biometric systems, they offer convenience and perceived security, however, vulnerabilities across their components and communication have been shown to expose both direct and indirect attacks.  
Joshi et al. (2020) propose a comprehensive 16-point threat model that outlines real world attacks such as spoofing, replay, brute force, trojan horse, side channel leaks, and administrative frauds. These can all target components from the sensor to template databases.  
A further explanation of the source basically breaks down threats into eight different classes. This is basically the risk level. So for example, something such as spoofing is considered a high risk because of how easy it is to pull off and how hard detection is. Something such as database tampering is considered higher at eight and nine as an insider can enable full impersonation in a database. One key aspect noted of when attacks primarily occur would be at the data transmission layer. I have an interesting note in the Data Encryption topic, but this is because it tends to be the weak point.  
From my personal experience, especially in the area of securing data via role based actions when sending data through Mulesoft, I’ve seen firsthand how critical it is to enforce encrypted transport, enforce session timeout, and protect stored credentials. Even how credentials are tied across access from my architectural experience should really be separated out by system to avoid an individual gaining superuser access. I can apply this to biometric data, as the data isn’t stored as an image, it is stored as data relevant to specific features and converted mathematically to be stored. This data needs to be secure and protected just as any other data and isn’t any more secured once stored or reused.  
Interesting enough, I have a lot of biometric security systems I’ve installed throughout my house. Just from the knowledge of how these systems work and how I’ve implemented them, I could easily make an argument that it would be inherently more difficult to steal because of its uniqueness and difficulty to replicate. All fingerprints would realistically be a unique primary key for each individual, so how can that be replicated easily?  
With that being said, I think we can actually make a very common statement that can easily counter this even to say that even though it’s unique, it doesn't mean it’s immune from being stolen. The detached biometric models I’m thinking of don’t even technically mention anything such as encrypted templates, so we can’t even assume that’s being used. If this were the situation and your bio data does get leaked, imagine you have leaked your unique primary key and can’t change it. I would highly recommend very detailed consideration of what devices store your biometric data. Once that is leaked, you now have a permanent security problem for any biometric solutions.

# Future Trends and Emerging Technologies in Cybersecurity

As we continue to move deeper into the future we can see our transformation and move into Industry 4.0 and 5.0 technologies. AI has helped propel this a lot. Cybersecurity has not only continued to be a primary concern, but has further been thrown more and more into the limelight as technology advances. This has a large impact across many industries and even with decision makers such as enterprise architecture.  
Kumar and Mallipeddi (2022) highlight emerging technologies such as AI, Internet of things, cloud computing and continue to further push us into efficiency, automation, and increased connectivity. As systems become more and more interconnected so does the increase of cyber security risks and threats. This has an impact across a wide range of industries and global industries.  
I think the premise of the message is very clean in that as systems become more interconnected, so does cyber security risk. Individuals not only need to think about the systems they primarily work on, but how that data stays secure as it moves through the flow into these other systems. Interestingly enough this has been a common theme among all my topics as moving data seems to be the most risky place for it to be compromised. Even with that, new technologies such as the Internet of Things, which I wouldn’t call as new anymore, has become more common in households and businesses and the autonomous methods of their sharing can actually produce significant security risk. This is a core of the point that security must be built into design and not an afterthought.  
As a Sr Solution Architect that works a lot with Mulesoft and Salesforce, I do see these risks daily and have even noticed much more vision from enterprise architects on these subjects as well. They want security to be built into solutions and not thought about later. I’ve really noticed this in the risky area of integrations as we really start to build out our API led architecture which heavily increases API endpoints across the enterprise. Each of these increase the risks of gaps in OAuth, session management, and security logging. I’ve also noticed that leaving it up to developers alone won’t work, it must be built into the solution architecture.  
Actually, an interesting counter argument I had with a developer when developing a new OIDC flow for enhanced authentication was that what is the point of overburdening their teams with these requirements and denying other development efforts we deem unsecure if the client is already doing this unsecure practice they would just be simply making their process easier. The thought really premised around emphasising so much on cyber risk when they didn’t think the risk was inherently high and this was just adding extra overhead slowing them down instead of allowing them to streamline quick development in agile form.  
From my perspective, while developing quickly and attempting to innovate for the client more quickly while looking at it from the perspective that the risks really are not that high are something I get, I still think that it would be reckless to not consider the actual impact if that risk does occur or even not take into the account of risk as technologies progress into the future. For example, maybe the load on this portal is low now, but we want to expand, bring more people in to streamline this portal, enhance connectivity with other systems for a better experience, now the risk might increase even more if we just didn’t build them in design to start off with. I agree that we should build with security in mind and not make it an afterthought. I think this is an absolute must type of thinking today, and I guarantee our Architectural designs would get rejected by enterprise Architects if we did not include this type of thinking.

# References

* Agarwal, V., Chand, S., Sah, J. P., & Shilpa, N. R. (2018). A framework: Encryption method on cloud storage for data security. International Journal of Advanced Research in Computer Science, 9(Special Issue 3), 276. https://doi.org/10.26483/ijarcs.v9i0.6249
* Joshi, M., Mazumdar, B., & Dey, S. (2020). A comprehensive security analysis of match-in-database fingerprint biometric system. Pattern Recognition Letters, 138, 247–266. https://doi.org/10.1016/j.patrec.2020.07.024
* Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and Operations Management, 31(12), 4488–4500. https://doi.org/10.1111/poms.13859