



UNIVERSITÀ DEGLI STUDI DI MILANO  
Facoltà di Scienze e Tecnologie  
*Corso di Laurea in Sicurezza dei Sistemi e delle Reti  
Informatiche*

SICUREZZA DELL'INFRASTRUTTURA  
AWS IN UNA STARTUP FINTECH:  
SFIDE, BEST PRACTICES E  
IMPLEMENTAZIONE DI UN  
MODELLO DI SICUREZZA  
RESILIENTE LOW COST

**Relatore:** Prof. Claudio Agostino Ardagna

**Correlatore:** Lorenzo Perotta, Andrea Pasini, Simone Cortese

Tesi di:  
Andrea Ferraboli  
Matricola: 09985A

Anno Accademico 2024-2025

*dedicato a ...*

# Prefazione

# Indice

	iii
<b>Prefazione</b>	<b>iv</b>
0.1 Contesto: Crescita delle startup fintech e importanza della sicurezza .	viii
0.2 Obiettivi della tesi e domande di ricerca . . . . .	viii
0.2.1 Quali sono le principali sfide di cybersecurity per una startup fintech che utilizza AWS? . . . . .	viii
0.2.2 Quali sono le best practice di sicurezza di AWS più rilevanti per una startup fintech? . . . . .	viii
0.2.3 Come si può implementare un'infrastruttura AWS sicura e resiliente per una startup fintech? . . . . .	viii
0.3 Struttura della tesi . . . . .	viii
<b>1 Principi</b>	<b>ix</b>
1.1 Il concetto di "Security by Design" . . . . .	ix
1.2 Best practice e principi di sicurezza . . . . .	ix
<b>2 Fondamenti di Sicurezza su AWS</b>	<b>x</b>
2.1 Modello di responsabilità condivisa di AWS . . . . .	x
2.2 Best practice di sicurezza specifiche per startup fintech . . . . .	x
2.3 Panoramica dei principali servizi di sicurezza di AWS . . . . .	x
2.3.1 AWS Identity and Access Management (IAM) . . . . .	x
2.3.2 AWS Key Management Service (KMS) . . . . .	x
2.3.3 AWS CloudTrail e Amazon CloudWatch (servizi concorrenti) .	x
2.3.4 AWS GuardDuty, Amazon Inspector e Amazon Macie (alternativa valida) . . . . .	x
2.3.5 Altri servizi rilevanti (es. AWS WAF, VPC) . . . . .	x
<b>3 Gestione delle Identità e degli Accessi (IAM)</b>	<b>xi</b>
3.1 Implementazione del principio del minimo privilegio . . . . .	xi
3.2 Creazione e gestione di utenti, gruppi e ruoli IAM . . . . .	xi

3.3	Utilizzo di policy IAM per concedere permessi granulari . . . . .	xi
3.4	Configurazione dell'autenticazione a più fattori (MFA) . . . . .	xi
3.5	Gestione delle credenziali (es. utilizzo di IAM Roles per EC2) . . . .	xi
3.6	Audit e monitoraggio degli accessi IAM . . . . .	xi
<b>4</b>	<b>Monitoraggio e Logging della Sicurezza</b>	<b>xii</b>
4.1	Configurazione di AWS CloudTrail per tracciare le attività degli utenti	xii
4.2	Implementazione di Amazon CloudWatch per monitorare le metriche di sistema . . . . .	xii
4.3	Creazione di allarmi per eventi specifici e attività sospette . . . . .	xii
4.4	Utilizzo di AWS GuardDuty per il rilevamento automatico di minacce	xii
4.5	Integrazione con sistemi SIEM (Security Information and Event Ma- nagement) . . . . .	xii
4.6	Gestione e analisi dei log . . . . .	xii
<b>5</b>	<b>Protezione dei Dati Sensibili e Conformità Normativa</b>	<b>xiii</b>
5.1	Crittografia dei dati a riposo e in transito . . . . .	xiii
5.2	Gestione delle chiavi di crittografia con AWS KMS o CloudHSM . . .	xiii
5.3	Implementazione di meccanismi per la protezione dei dati in S3 . . .	xiii
5.4	Misure per la conformità a PCI DSS (se rilevante) . . . . .	xiii
5.5	Misure per la conformità al GDPR e protezione dei dati personali . .	xiii
5.6	Valutazione e gestione del rischio di perdita di dati . . . . .	xiii
<b>6</b>	<b>Casi Studio e Implementazione Pratica</b>	<b>xiv</b>
6.1	Esempio di architettura di sicurezza AWS per una startup fintech (proposta) . . . . .	xv
6.2	Implementazione delle best practice descritte nei capitoli precedenti .	xv
6.3	Test di penetrazione e valutazione della sicurezza dell'ambiente . . . .	xv
6.4	Analisi dei risultati e confronto con le best practice . . . . .	xv
6.5	Integrazione di strumenti di sicurezza terzi (es. SentinelOne) . . . . .	xv
6.6	Infrastruttura di base AWS, integrazione codice e infrastruttura di un sistema honeypot . . . . .	xv
6.7	Deadcode per confondere malware (Capitolo 7) . . . . .	xv
6.8	Autenticazione con chiavi pubbliche (Capitolo 8) . . . . .	xv
6.9	Progettazione e implementazione di una Virtual Private Cloud (VPC) isolata . . . . .	xv
6.9.1	Creazione di subnet pubbliche e private . . . . .	xv
6.9.2	Utilizzo di gruppi di sicurezza e ACL per controllare il traffico di rete . . . . .	xv
6.9.3	Implementazione di Network Address Translation (NAT) e VPN/Direct Connect . . . . .	xv

6.9.4	Configurazione di load balancer per alta disponibilità e scalabilità	xv
6.9.5	Utilizzo di container (es. ECS o EKS) per una maggiore sicurezza e scalabilità . . . . .	xv
<b>7</b>	<b>Discussione e Conclusioni</b>	<b>xvi</b>
7.1	Rielaborazione delle domande di ricerca iniziali e discussione dei risultati	xvi
7.2	Riflessioni sulle sfide e opportunità per la sicurezza di AWS nelle startup fintech . . . . .	xvi
7.3	Prospettive future per la ricerca e l'innovazione . . . . .	xvi
7.4	Raccomandazioni per la creazione di un modello di cybersecurity resiliente per startup fintech . . . . .	xvi
	<b>Bibliografia</b>	<b>xvii</b>
	<b>Ringraziamenti</b>	<b>xviii</b>
<b>8</b>	<b>Introduzione</b>	<b>1</b>

# Introduzione

- 0.1 Contesto: Crescita delle startup fintech e importanza della sicurezza
- 0.2 Obiettivi della tesi e domande di ricerca
  - 0.2.1 Quali sono le principali sfide di cybersecurity per una startup fintech che utilizza AWS?
  - 0.2.2 Quali sono le best practice di sicurezza di AWS più rilevanti per una startup fintech?
  - 0.2.3 Come si può implementare un'infrastruttura AWS sicura e resiliente per una startup fintech?
- 0.3 Struttura della tesi



# Capitolo 1

## Principi

1.1 Il concetto di "Security by Design"

1.2 Best practice e principi di sicurezza

## Capitolo 2

# Fondamenti di Sicurezza su AWS

- 2.1 Modello di responsabilità condivisa di AWS
- 2.2 Best practice di sicurezza specifiche per startup fintech
- 2.3 Panoramica dei principali servizi di sicurezza di AWS
  - 2.3.1 AWS Identity and Access Management (IAM)
  - 2.3.2 AWS Key Management Service (KMS)
  - 2.3.3 AWS CloudTrail e Amazon CloudWatch (servizi concorrenti)
  - 2.3.4 AWS GuardDuty, Amazon Inspector e Amazon Macie (alternativa valida)
  - 2.3.5 Altri servizi rilevanti (es. AWS WAF, VPC)

## Capitolo 3

# Gestione delle Identità e degli Accessi (IAM)

- 3.1 Implementazione del principio del minimo privilegio
- 3.2 Creazione e gestione di utenti, gruppi e ruoli IAM
- 3.3 Utilizzo di policy IAM per concedere permessi granulari
- 3.4 Configurazione dell'autenticazione a più fattori (MFA)
- 3.5 Gestione delle credenziali (es. utilizzo di IAM Roles per EC2)
- 3.6 Audit e monitoraggio degli accessi IAM

## Capitolo 4

# Monitoraggio e Logging della Sicurezza

- 4.1 Configurazione di AWS CloudTrail per tracciare le attività degli utenti
- 4.2 Implementazione di Amazon CloudWatch per monitorare le metriche di sistema
- 4.3 Creazione di allarmi per eventi specifici e attività sospette
- 4.4 Utilizzo di AWS GuardDuty per il rilevamento automatico di minacce
- 4.5 Integrazione con sistemi SIEM (Security Information and Event Management)
- 4.6 Gestione e analisi dei log

## Capitolo 5

# Protezione dei Dati Sensibili e Conformità Normativa

- 5.1 Crittografia dei dati a riposo e in transito
- 5.2 Gestione delle chiavi di crittografia con AWS KMS o CloudHSM
- 5.3 Implementazione di meccanismi per la protezione dei dati in S3
- 5.4 Misure per la conformità a PCI DSS (se rilevante)
- 5.5 Misure per la conformità al GDPR e protezione dei dati personali
- 5.6 Valutazione e gestione del rischio di perdita di dati



## Capitolo 6

# Casi Studio e Implementazione Pratica

- 6.1 Esempio di architettura di sicurezza AWS per una startup fintech (proposta)
- 6.2 Implementazione delle best practice descritte nei capitoli precedenti
- 6.3 Test di penetrazione e valutazione della sicurezza dell'ambiente
- 6.4 Analisi dei risultati e confronto con le best practice
- 6.5 Integrazione di strumenti di sicurezza terzi (es. SentinelOne)
- 6.6 Infrastruttura di base AWS, integrazione codice e infrastruttura di un sistema honeypot
- 6.7 Deadcode per confondere malware (Capitolo 7)
- 6.8 Autenticazione con <sup>xv</sup>chiavi pubbliche (Capitolo 8)
- 6.9 Progettazione e implementazione di una Virtual Private Cloud (VPC) isolata

## Capitolo 7

### Discussione e Conclusioni

- 7.1 Rielaborazione delle domande di ricerca iniziali e discussione dei risultati
- 7.2 Riflessioni sulle sfide e opportunità per la sicurezza di AWS nelle startup fintech
- 7.3 Prospettive future per la ricerca e l'innovazione
- 7.4 Raccomandazioni per la creazione di un modello di cybersecurity resiliente per startup fintech



# Bibliografia

Elenco di tutti i materiali consultati durante la stesura della tesi.

# Ringraziamenti

asdjhgtry.

# Indice

# Capitolo 8

## Introduzione

# Bibliografia

- [1] M. Gotti, I linguaggi specialistici, Firenze, La Nuova Italia, 1991.
- [2] R. Wellek, A. Warren, Theory of Literature , 3rd edition, New York, Harcourt, 1962.
- [3] A. Canziani et al., Come comunica il teatro: dal testo alla scena. Milano, Il Formichiere, 1978.
- [4] Ministry of Defence, Great Britain, Author and Subject Catalogues of the Naval Library, London, Ministry of Defence, HMSO, 1967.
- [5] H. Heine, Pensieri e ghiribizzi. A cura di A. Meozzi. Lanciano, Carabba, 1923.
- [6] L. Basso, "Capitalismo monopolistico e strategia operaia", Problemi del socialismo, vol. 8, n. 5, pp. 585-612, 1962.
- [7] L. Avirovic, J. Dodds (a cura di), Atti del Convegno internazionale "Umberto Eco, Claudio Magris. Autori e traduttori a confronto" ( Trieste, 27-28 novembre 1989), Udine, Campanotto, 1993.
- [8] E.L. Gans, "The Discovery of Illusion: Flaubert's Early Works, 1835-1837", unpublished Ph.D. Dissertation, Johns Hopkins University, 1967.
- [9] R. Harrison, Bibliography of planned languages (excluding Esperanto). <http://www.vor.nu/langlab/bibliog.html>, 1992, agg. 1997.