

A Systematic Review of Cloud Computing Security Risks in E-Commerce

An Exploratory Analysis of Indian Cyber-Incident Datasets and Framework-Driven Risk Mapping

Shruti Dimote^{#1}, Pradnya Dongare^{#2}, Dr. Rupali Kalekar^{#3}

[#] student(1), student (2) and Guide(3), ZIBACAR, Affiliated to
Savitribai Phule Pune University (SPPU), Pune, Maharashtra, India

ORCID ID -0009-0007-6623-9275 (Shruti Dimote); ORCID ID- 0009-0004-8963-4268 (Pradnya Dongare);

ORCID ID- 0000-0001-9567-3344 (Dr. Rupali Kalekar)

shrutidimote234@gmail.com, dongarepradnya2301@gmail.com, rupali.kalekar@zealeducation.com

Abstract—

Cloud computing facilitates scalable infrastructure, distributed applications and the management of large volumes of customer and transaction data in e-commerce, but poses risks to customer information, payment data, credentials, application programming interfaces (APIs), and cloud storage. This paper presents an exploratory analysis of cloud security risks in e-commerce based solely on secondary data; no primary data were collected. Three public Indian government data sources were examined: NCRB cyber-crime statistics by crime head and State/UT for 2014–2023, National Cyber Crime Reporting Portal (NCRP) cyber-fraud totals to 28 Feb 2025, and CERT-In incident counts for 2018–2023, together with CSA, OWASP, PCI DSS, and peer-reviewed literature. Registered cyber-crime cases rose from 9,622 in 2014 to 86,420 in 2023; computer 11 related, fraud, cheating, data-theft, and forgery heads made up 83.7% of 2023 cases; and three States accounted for 58.9%. None of the datasets identify cloud or e-commerce contexts, so they serve as contextual indicators, and risk themes (misconfiguration, IAM, APIs, data exposure, monitoring) are compared qualitatively with stated evidence levels rather than likelihood–impact scores. Security controls and practical recommendations are discussed.

Index Terms—Cloud Computing Security, E-Commerce Security, Cloud Misconfiguration, API Security, Exploratory Research, Secondary Data, Identity and Access Management, Customer Data Protection.

I. INTRODUCTION

Cloud computing has become an important infrastructure model for modern e-commerce platforms. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) enable organizations to support high-volume transaction processing, distributed product catalogs, web applications, and automated checkout services. The scalability and flexibility of cloud infrastructure allow e-commerce organizations to respond to changes in customer demand without maintaining extensive physical infrastructure.

However, the migration of e-commerce applications and data to cloud environments introduces additional security considerations. The shared responsibility model distributes security duties between cloud service providers and cloud customers, so incorrect configurations, excessive privileges, weak authentication, and insecure interfaces may create security exposure.

E-commerce platforms process personally identifiable information (PII), authentication credentials, transaction information, and payment-related data. Protecting such information is important for confidentiality, integrity, and availability, and incidents involving cloud infrastructure can affect business continuity, customer confidence, and regulatory compliance.

This study therefore explores existing evidence on cloud security risks in e-commerce. It does not collect new data from respondents. Instead, it examines publicly available Indian government datasets on cyber crime and cyber security incidents, and interprets them alongside authoritative literature and frameworks. The analysis is exploratory: it looks for

patterns and recurring risks rather than testing causal hypotheses.

II. RELATED WORK AND RESEARCH GAP

Previous research has examined cloud computing security from the perspectives of threats, vulnerabilities, privacy, access control, and mitigation. Alouffi et al. presented a systematic literature review of cloud security threats and mitigation solutions [1]. Sun discussed security and privacy protection challenges in cloud environments [2], and Tabrizchi and Kuchaki Rafsanjani surveyed security challenges, threats, and solutions [3].

Industry bodies provide complementary views. The Cloud Security Alliance (CSA) Top Threats to Cloud Computing 2024 report ranks misconfiguration and inadequate change control first, followed by identity and access management (IAM), insecure interfaces and APIs, and inadequate cloud security strategy; the report was compiled from surveys of cybersecurity professionals [5], [16]. The OWASP API Security Top 10 (2023) catalogues recurring API weaknesses [4], and the PCI DSS defines requirements for protecting payment account data [6].

Existing literature is broad, but it rarely connects cloud security risks to the operating characteristics of online transaction platforms, and it seldom combines threat catalogues with publicly available national incident statistics. The research gap addressed here is an e-commerce focused, evidence-based exploration that (i) organizes cloud security risks by theme, (ii) examines what public Indian datasets can and cannot reveal about those themes, and (iii) states clearly where only literature-based discussion is possible.

III. PROBLEM STATEMENT

E-commerce organizations depend on cloud platforms for hosting applications, storing customer information, and processing transactions. Cloud-based e-commerce systems may be exposed to threats arising from configuration errors, insecure APIs, insufficient access controls, weak authentication, and inadequate monitoring. Because these risks span application interfaces, identity management, storage, databases, and monitoring systems, a structured, evidence-based approach is required to organize them. This research addresses the problem of identifying and organizing major cloud security risks affecting e-commerce systems, and of determining how far publicly available secondary data can support their comparison.

IV. RESEARCH OBJECTIVES

- 1) To identify major cloud security vulnerabilities and threat vectors affecting cloud-hosted e-commerce architectures.
- 2) To analyze the security implications of cloud storage misconfiguration, insecure APIs, and identity management weaknesses.
- 3) To examine risks associated with the protection of personally identifiable information and payment related data.
- 4) To explore publicly available datasets on cyber crime and cyber security incidents for patterns, trends, and category-wise distributions relevant to these risks.
- 5) To compare the identified risks qualitatively using documented secondary evidence, and to state where evidence is insufficient.
- 6) To examine security controls including IAM, encryption, multi-factor authentication, API security, and configuration auditing, and to derive practical recommendations for e-commerce developers and cloud administrators.

V. RESEARCH METHODOLOGY

A. Research Approach

The study adopts an exploratory research approach based entirely on secondary data and publicly available datasets. The purpose is to explore existing data and literature to identify patterns, trends, recurring security risks, and relationships relevant to cloud-based e-commerce environments, rather than to collect new data. No primary data were collected: no questionnaire, interview, survey, or sampling procedure was used. The study does not claim to establish causality.

B. Secondary Data Sources

Three public dataset groups were used (Table I). Quantitative findings in Section X come only from these datasets. Literature sources (peer-reviewed papers [1]–[3], CSA [5], OWASP [4], PCI DSS [6], and industry reporting [16]) support the qualitative discussion and are never used to generate numerical results in this paper.

TABLE I
SECONDARY DATASET REGISTER

ID	Dataset and source	Period	Variables used
D1	NCRB “Crime in India”: cyber-crime cases registered, by crime head (Annexure-I) and by State/UT (Annexure-II); Ministry of Home Affairs, Lok Sabha USQ 438, 2 Dec. 2025 [7]. Cross-checked with [8].	2014–2023	Cases registered per crime head; per State/UT; IT Act / IPC / SLL subtotals
D2	NCRP cyber-fraud statistics, State/UT-wise, cumulative to 28 Feb. 2025; Rajya Sabha reply of 12 Mar. 2025 [9]; OGD record [10].	Since inception to 28.02.2025	National total: incidents, amount reported, lien amount
D3	CERT-In cyber security incidents, data-breach and data-leak counts; Rajya Sabha replies [12]–[14].	2018–2023 (breach/leak 2023: to June)	Annual incident, breach, and leak counts

D1–D3 are official government statistics; the OGD portal (Data.gov.in) hosts parliamentary-reply datasets of this type [10], [11].

C. Dataset Selection Criteria

Candidate datasets were retained if they (a) were published by a government body or tabled in Parliament, (b) covered cyber crime, fraud, data breaches, or cyber incidents, (c) reported counts by year, crime head, or State/UT, and (d) could be checked for internal consistency. Datasets not meeting these conditions were excluded, and no dataset was used for a variable it does not contain.

D. Data Collection

The Data.gov.in listings for the NCRP cyber-fraud dataset [10] and the 2019–2021 State/UT cyber-crime dataset [11] were located and their metadata inspected. For D1–D3, the numerical values were transcribed from the original government documents cited in Table I. This means the values are exactly those published by the government, but D1 was not downloaded in machine-readable form from Data.gov.in; readers can verify it against [7] and the OGD records.

E. Data Preparation and Cleaning

- Variables were identified and mapped to the risk themes of Section VII (Table II).
- Internal consistency was verified: IT Act, IPC, and SLL subtotals sum to the published total in every year 2014–2023; the 28 State rows sum to the published “Total States” in every year; the 2018–2022 national totals match an independent earlier reply [8].
- Blank cells in the source (heads not reported separately before 2017) were treated as “not reported,” not as zero. Analyses of those heads cover 2017–2023 only.
- 2023 CERT-In breach and leak counts cover January–June only and are not compared with full years.

F. Exploratory Analysis

The analysis uses frequency counts, percentage distribution, year-on-year change, compound annual growth rate (CAGR), category-wise and State-wise comparison, and cross-tabulation of State by year. Inferential tests were not applied, for the reasons given in Section X-F. Analyses requiring variables absent from the datasets (for example, cloud deployment model, platform type, or attack vector) are stated as not possible.

G. Ethical and Data Integrity Considerations

All data are aggregate, public, and anonymous; no personal data were processed and no ethical clearance for human participants was required. No value was estimated, interpolated, or imputed. Dataset-derived findings (Section X) are kept separate from literature-based discussion (Sections VII–IX and XI). One metadata inconsistency was noted: the OGD record for D2 cites Rajya Sabha question no. 1517 [10], whereas the Rajya Sabha document retrieved for the figures is numbered 1513 and was answered on the same date [9]. The figures used are those in [9].

VI. EVIDENCE-BASED RISK ANALYSIS FRAMEWORK

The original framework scored each risk as $R = L \times I$, with likelihood (L) and impact (I) each rated 1–5. That scoring is not retained as a computed result. The public datasets used here do not record likelihood or impact for cloud misconfiguration, API weakness, or IAM failure in e-commerce, and assigning scores without such evidence would be arbitrary. The formula remains a valid method for a future study that obtains documented L and I evidence (for example, organization-level incident logs).

Instead, risks are compared qualitatively using the documented evidence available for each. The evidence level (Table III) describes the kind of support behind a risk, not its severity.

TABLE III
EVIDENCE LEVELS USED FOR QUALITATIVE COMPARISON

Level	Criterion
A	Ranked as a leading threat in an authoritative framework or survey, and an indirect indicator exists in a public dataset (D1–D3).
B	Ranked or catalogued in an authoritative framework or survey, but no dataset variable measures it.
C	Described in guidance or literature only; no ranking and no dataset variable.

VII. MAJOR CLOUD SECURITY RISKS IN E-COMMERCE

The following risk themes are discussed on the basis of the literature [1]–[6]. Table II shows which dataset heads, if any, relate to each theme.

A. Cloud Storage Misconfiguration

Incorrect permissions and publicly exposed storage resources can allow unauthorized access to sensitive information. CSA ranks misconfiguration and inadequate change control as the leading cloud threat in 2024 and notes that several top contributors trace back to human error [5], [16]. OWASP lists security misconfiguration as API8 [4].

B. Insecure APIs

APIs connect clients, applications, and backend services. Weak authentication, insufficient authorization (for example, broken object-level authorization, API1), missing rate limiting (API4), and incomplete API inventories (API9) can increase the exposure of transaction APIs [4]. CSA ranks insecure interfaces and APIs third in 2024 [5].

C. Identity and Access Management

Excessive privileges, poorly configured roles, and weak authentication can allow compromised credentials to reach sensitive resources. CSA ranks IAM second in 2024, down from first in 2022 [5], [16]. OWASP lists broken authentication as API2 [4].

D. Data Exposure

E-commerce platforms hold PII, credentials, and transaction data, so unauthorized disclosure has direct customer and regulatory consequences. Accidental cloud data exposure appears among the human-factor threats in the CSA 2024 top ten [16]. PCI DSS requires protection of stored and transmitted account data [6].

E. Monitoring and Logging

Security monitoring and audit logging provide visibility into suspicious activity and support incident investigation. PCI DSS requires logging and monitoring of access to system components and cardholder data [6]. This theme is discussed from guidance only; no public dataset used here measures it.

TABLE II
MAPPING OF RISK THEMES TO DATASET VARIABLES

Risk theme	Related dataset variable (source)	Limitation
Misconfiguration	None	No variable records cause or configuration state
Insecure APIs	None	No variable records API-related incidents
IAM weaknesses	NCRB “Unauthorised access to protected computer system” (D1)	Applies to protected systems; not cloud/e-commerce-specific
Data exposure	NCRB “Data theft” (D1); CERT-In breach and leak counts (D3)	All sectors; no cloud flag
Payment / transaction fraud	NCRB Fraud, Cheating, Forgery, Counterfeiting, Computer-related offences (D1); NCRP totals (D2)	Not limited to e-commerce
Monitoring / logging	None	Literature-based only

VIII. SECURITY CONTROLS AND MITIGATION MEASURES

The controls considered are mapped to the risk themes and to PCI DSS v4.0.1 requirement areas [6] and OWASP API items [4]. The mapping is conceptual and is not derived from the datasets.

TABLE IV
SECURITY CONTROLS CONSIDERED IN THE STUDY

Control	Security purpose	Related risk / reference
IAM	Controlled access and least privilege	IAM weakness; PCI DSS Req. 7–8
MFA	Additional authentication factor	IAM; API2; PCI DSS Req. 8
Encryption	Protects data in transit and at rest	Data exposure; PCI DSS Req. 3–4
API security	Authentication, authorization, rate limiting, API inventory	Insecure APIs; API1, API2, API4, API9
Configuration auditing	Detects insecure cloud configurations	Misconfiguration; API8
Monitoring	Detection and investigation of events	Monitoring; PCI DSS Req. 10

IX. E-COMMERCE CLOUD THREAT SURFACE

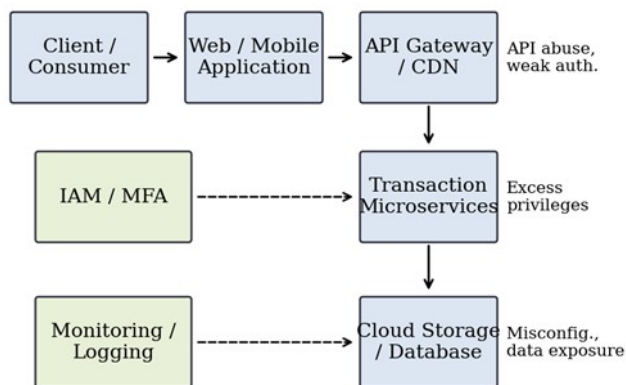


Fig. 1. Conceptual cloud-based e-commerce threat surface. Labels indicate illustrative risk themes from the literature, not measured values.

Fig. 1 shows the relationship between consumer applications, API gateways, transaction services, cloud storage, and security controls. Risks may arise at each layer and affect the confidentiality, integrity, or availability of e-commerce resources.

X. EXPLORATORY DATA ANALYSIS AND FINDINGS

All numbers in this section are dataset-derived (D1–D3) or computed directly from them. None of the datasets identify cloud deployments or e-commerce platforms; they are used as contextual indicators of the cyber-threat environment in which cloud-based e-commerce operates.

A. Overall Trend in Registered Cyber Crime (D1)

Registered cyber-crime cases in India rose from 9,622 in 2014 to 86,420 in 2023, about 9.0 times, a CAGR of 27.6% (Table V, Fig. 2). Year-on-year change varied widely: +77.0% in 2017 and +64.2% in 2019, but +5.9% in 2021. Several crime heads are first reported separately from 2017, so part of the 2017 rise may reflect expanded classification; the data cannot separate this from real growth.

TABLE V
CYBER-CRIME CASES REGISTERED IN INDIA BY LEGAL CATEGORY (D1)

Year	Total	IT Act	IPC	SLL	YoY %
2014	9,622	7,201	2,272	149	–
2015	11,592	8,045	3,422	125	20.5
2016	12,317	8,613	3,518	186	6.3
2017	21,796	13,635	7,976	185	77.0
2018	27,248	18,495	8,647	106	25.0
2019	44,735	30,846	13,800	89	64.2
2020	50,035	29,643	20,201	191	11.8
2021	52,974	27,427	25,384	163	5.9
2022	65,893	31,908	33,798	187	24.4
2023	86,420	44,237	41,849	334	31.2

Source: NCRB, via [7]. YoY computed by the authors.

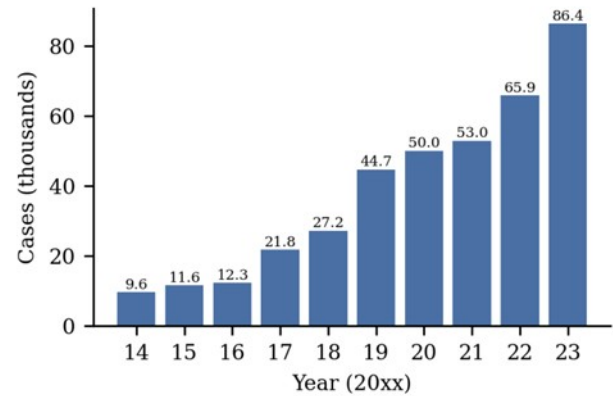


Fig. 2. Cyber-crime cases registered in India, 2014–2023 (D1, [7]).

The composition shifted. The IT Act share fell from 74.8% (2014) to 51.2% (2023), while the IPC share rose from 23.6% to 48.4%. Cases under IPC heads grew at a CAGR of 38.2%, against 22.3% for IT Act heads.

B. Category-Wise Comparison (D1)

Table VI compares heads mapped in Table II. Computer-related offences were the largest head in every year (40.9% of 2023 cases). Cheating grew from 1,115 to 16,943 cases (CAGR 57.4%), and Fraud, reported separately from 2017, grew from 3,466 to 19,466 (CAGR 33.3%). Together, computer-related offences, fraud, cheating, data theft, and forgery account for 72,295 of 86,420 cases in 2023 (83.7%), up from 15,876 of 21,796 in 2017 (72.8%). This grouping is the authors' analytical choice, not an NCRB category.

TABLE VI
SELECTED CRIME HEADS RELATED TO THE RISK THEMES (D1)

Crime head	2014	2017	2020	2023	2023 share %
Computer-related offences	5,548	10,108	21,926	35,329	40.9
Cheating	1,115	1,896	4,480	16,943	19.6
Fraud	n.r.	3,466	10,395	19,466	22.5
Forgery	63	99	582	444	0.5
Data theft	55	307	98	113	0.1
Unauthorised access (protected systems)	0	2	2	1	<0.01

n.r. = not reported separately. Source: NCRB, via [7]; shares computed by the authors.

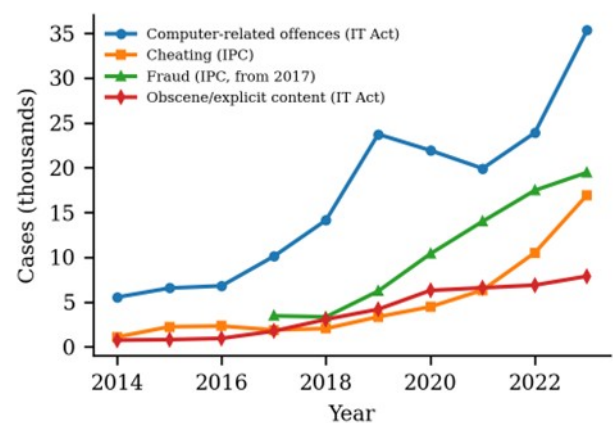


Fig. 3. Selected crime heads, 2014–2023 (D1). Fraud is plotted from 2017.

Two heads most directly tied to data confidentiality show little growth. Data theft fluctuated between 55 and 307 cases a year with no sustained trend, and unauthorised access to protected systems totaled 19 cases over ten years. The data cannot show whether this reflects low incidence, under-reporting, or recording under other heads.

C. State-Wise Distribution and Cross-Tabulation (D1)

Registered cases are concentrated. Karnataka, Telangana, and Uttar Pradesh together accounted for 58.9% of 2023 cases, up from 36.0% in 2014 (51.5% in 2021). The 11 States in Table VII account for 92.6% of the 2023 total. Karnataka rose from 12,556 (2022) to 21,889 (2023), and Telangana from 5,024 (2020) to 10,303 (2021).

TABLE VII
CASES REGISTERED IN SELECTED STATES (D1)

State	2014	2019	2023	2023 share %	Growth (× 2014)
Karnataka	1,020	12,020	21,889	25.3	21.5
Telangana	703	2,691	18,236	21.1	25.9
Uttar Pradesh	1,737	11,416	10,794	12.5	6.2
Maharashtra	1,879	4,967	8,103	9.4	4.3
Bihar	114	1,050	4,450	5.1	39.0
Tamil Nadu	172	385	4,121	4.8	24.0
Kerala	450	307	3,295	3.8	7.3
Rajasthan	697	1,762	2,435	2.8	3.5
Odisha	124	1,485	2,348	2.7	18.9
Andhra Pradesh	282	1,886	2,341	2.7	8.3
Gujarat	227	784	1,995	2.3	8.8

Source: NCRB, via [7]. Shares and growth multiples computed by the authors; no population or internet-user normalization.

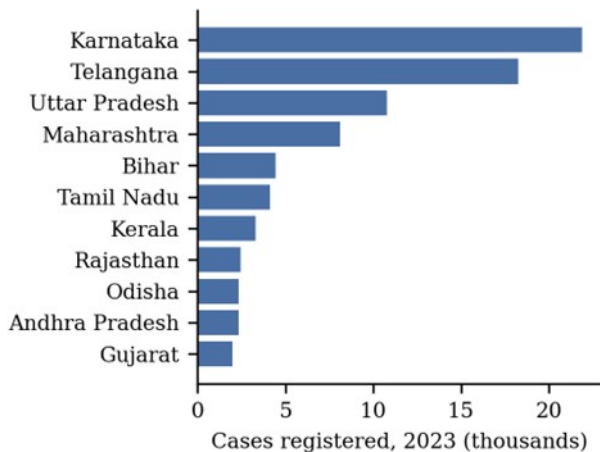


Fig. 4. Cases registered in selected States, 2023 (D1).

No normalization is performed based on population, internet usage or e-commerce volume as those variables are not included in the datasets. The numbers should not be interpreted as a risk ranking.

D. Cyber Fraud Reporting (D2)

There have been 3,822,550 cyber-fraud incidents reported to NCRP since inception till 28 February 2025 with a reported amount of 3,644,819.85 and a lien amount of 438,080.57 (₹ lakh, as per the OGD field description [10]). The ratio between lien amount and reported amount is 12.0%, and the average amount per incident is approximately ₹0.95 lakh. The

obtain information give as cumulative total, and there is no possibility to analyze any year-wise or category-wise trends, and any e-commerce payment channel breakdown in D2.

E. CERT-In Incidents, Breaches, and Leaks (D3)

The number of CERT-In incidents increased from 208,456 in 2018 to 1,592,917 in 2023 (+ 7.6 times), and the year-on-year growth rate was +89.2% (2019), +193.6% (2020), +21.1% (2021), -0.8% (2022), and +14.5% (2023). Number of tracked data-breach incidents increased from 5 in 2018 to 51 in 2022, while 49 data breach incidents have been recorded in Jan–Jun 2023 (Table VIII, Fig. 5). Numbers are low and applicable to all sectors, and there is no cloud flag.

TABLE VIII
CERT-IN INCIDENT, DATA-BREACH, AND DATA-LEAK COUNTS (D3)

Year	Cyber security incidents	Data breach incidents	Data leak incidents
2018	208,456	5	0
2019	394,499	11	0
2020	1,158,208	36	14
2021	1,402,809	39	6
2022	1,391,457	51	27
2023	1,592,917	49*	15*

*Jan–Jun 2023 only. Sources: [12]–[14].

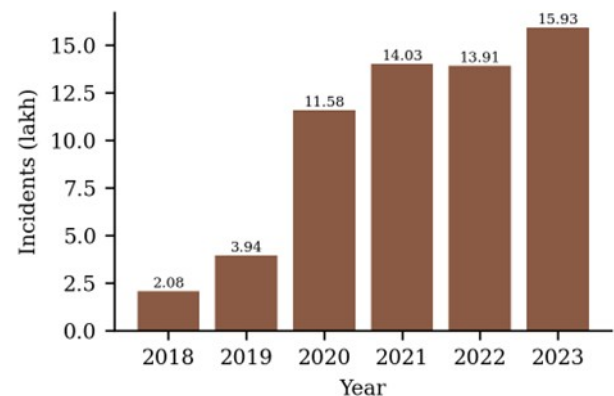


Fig. 5. CERT-In Cyber security incidents count, 2018–2023 (D3).

F. Analyses Not Performed

- Correlation or regression between D1 and D3 (n = 6 annual points): both series demonstrate a positive upward time trend and apply to concepts with distinct reporting rules. In addition CERT-In has introduced a new requirement for mandatory report submission within six hours[15].
- Association between security-control adoption and incidents: no dataset contains information on the adoption. The available secondary data do not provide enough evidence for this task.
- Cloud-specific or e-commerce-specific incident counts, and likelihood–impact scoring: there is no such variable among in D1–D3 (see Section VI).

XI. DISCUSSION

A. Qualitative Risk Comparison

The following table show how the literature rankings compare to dataset indicators (if any) with evidence levels (see Section VII)

TABLE IX

EVIDENCE-BASED COMPARISON OF CLOUD SECURITY RISK THEMES

Risk theme	Literature position	Dataset indicator (D1–D3)	Evidence level
Misconfiguration	CSA 2024: rank 1 [5]; OWASP API8 [4]	None	B
IAM weaknesses	CSA 2024: rank 2 [5]; OWASP API2 [4]	Unauthorised access head: 19 cases in 2014–2023 (D1); not cloud-specific	B
Insecure APIs	CSA 2024: rank 3 [5]; OWASP API1, API4, API9 [4]	None	B
Data exposure	In CSA 2024 top ten [16]; PCI DSS [6]	Data theft 55–307 cases/yr (D1); CERT-In breach and leak counts (D3)	A
Payment / transaction fraud	PCI DSS [6]	Fraud, cheating, computer-related offences: large and growing (D1); NCRP totals (D2)	A
Monitoring / logging	PCI DSS Req. 10 [6]	None	C

Evidence levels as defined in Table III. “A” does not imply higher severity.

B. Interpretation

The data indicate a rapid increase in registered cyber crimes, fraud-and computer-related offences accounting for the majority of such crimes. While this is consistent with the idea of transaction and payment data being highly attractive to e-commerce platforms, the facts that datasets do not capture the geographical location of such crimes prevents one from drawing a definitive conclusion on whether cloud-hosted e-commerce is affected and whether cloud misconfiguration, IAM and API weaknesses have any part in it. The top three threats, identified by CSA and OWASP (cloud misconfiguration, IAM, and APIs) cannot be quantified via D1–D3 and are backed up exclusively by the literature.

C. Practical Recommendations

These recommendations follow from the literature [4]–[6] and the controls in Table IV; they are not derived statistically from the datasets.

- Apply least-privilege IAM and MFA, and review access regularly.
- Audit cloud storage and infrastructure configuration continuously, with change control.
- Enforce authentication, object-level authorization, and rate limiting on transaction APIs, and maintain an API inventory.
- Protect PII and payment data with encryption according to PCI DSS requirements.
- Maintain Centralized logs, monitor for fraud-related anomalies, maintain tested backups and an incident response plan according to CERT-In reporting requirements.

XII. RESEARCH CONTRIBUTION

- 7) A structured classification of cloud security risks affecting e-commerce platforms, mapped to authoritative frameworks.
- 8) A transparent mapping of public Indian cyber-crime and incident datasets to those risk themes, showing which themes the data can and cannot inform.
- 9) Exploratory analysis of secondary verified data on trends, category distribution, and State-wise distribution.
- 10) An evidence-level approach for comparison of risks in the absence of data on likelihood and impact, and practical recommendations on IAM, API security, data protection, monitoring, and configuration management.

XIII. LIMITATIONS

- None of the datasets D1–D3 identifies cloud environments or e-commerce platforms; the findings are contextual, but not cloud-specific.
- The NCRB numbers represents the number of registered cases, not true incidence; underreporting, the registration procedure and changing classifications (multiple themes first appearing in 2017) influence them.
- Counts per State is not normalized; D2 dataset only provides the national cumulative number of cases in the retrieved material, with units obtained from OGD metadata [10].
- CERT-In counts are influenced by definition and reporting rules; the 2023 breach and leak count are incomplete.
- D1 was transcribed from a parliamentary reply rather than downloaded from Data.gov.in; the OGD record for D2 shows a question-number discrepancy (Section V-G).
- CSA rankings reflect professional opinion surveys, not measured incident frequencies.
- No causal conclusions are drawn. A future study could add other public incident datasets or organization-level incident data to support likelihood–impact scoring.

XIV. CONCLUSION

This paper explored cloud computing security risks in e-commerce using only secondary data. Public Indian statistics show a steep rise in registered cyber crime, from 9,622 cases in 2014 to 86,420 in 2023, with computer-related, fraud, and cheating offences making up most cases, a geographic concentration in a few States, and growing CERT-In incident counts. These patterns are consistent with a threat environment in which transaction and customer data are valuable targets, but the datasets do not allow conclusions about cloud misconfiguration, API weaknesses, or IAM failures in e-commerce specifically. Those themes were therefore compared qualitatively using CSA, OWASP, and PCI DSS sources, with explicit evidence levels instead of invented likelihood–impact scores.

Security controls such as IAM, MFA, encryption, API security, configuration auditing, monitoring, and backup remain the main mitigation measures. Stronger, cloud-specific quantitative conclusions will require datasets that record cloud context, attack vector, and impact.

REFERENCES

- [1] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: Threats and mitigation solutions," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.
- [2] P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *J. Netw. Comput. Appl.*, vol. 160, p. 102642, 2020, doi: 10.1016/j.jnca.2020.102642.
- [3] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020, doi: 10.1007/s11227-020-03213-1.
- [4] OWASP Foundation, "OWASP API Security Top 10 – 2023," Open Web Application Security Project, 2023.
- [5] Cloud Security Alliance, "Top Threats to Cloud Computing 2024," CSA Top Threats Working Group, Aug. 2024.
- [6] PCI Security Standards Council, "Payment Card Industry Data Security Standard, v4.0.1," Jun. 2024.
- [7] Ministry of Home Affairs, Govt. of India, "Rise in cybercrime cases," Lok Sabha Unstarred Question No. 438, Dec. 2, 2025 (data: NCRB, Crime in India). [Online]. Available: <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/438.pdf>
- [8] Ministry of Home Affairs, Govt. of India, "Cybercrime complaints," Rajya Sabha Unstarred Question No. 239, Jul. 24, 2024. [Online]. Available: https://rsdebate.nic.in/bitstream/123456789/749335/1/PQ_265_24072024_U239_p323_p326.pdf
- [9] Ministry of Home Affairs, Govt. of India, "Cyber crime cases," Rajya Sabha Unstarred Question No. 1513, Mar. 12, 2025. [Online]. Available: https://rsdebate.nic.in/bitstream/123456789/757298/1/PQ_267_12032025_U1513_p304_p308.pdf
- [10] Open Government Data (OGD) Platform India, "State/UT-wise details of statistics on National Cyber Crime Reporting Portal (NCRP) related to cyber fraud cases as on 28-02-2025." [Online]. Available: <https://www.data.gov.in/resource/stateut-wise-details-statistics-national-cyber-crime-reporting-portal-ncrp-related-cyber>
- [11] Open Government Data (OGD) Platform India, "State/UT-wise details of cases registered, chargesheeted, convicted ... under total cyber crimes from 2019 to 2021." [Online]. Available: <https://www.data.gov.in/resource/stateut-wise-details-cases-registered-cr-cases-chargesheeted-ccs-cases-convicted-con>
- [12] Ministry of Electronics and Information Technology, Govt. of India, Rajya Sabha Unstarred Question No. 528, Feb. 7, 2025. [Online]. Available: https://rsdebate.nic.in/bitstream/123456789/758307/1/PQ_267_07022025_U528_p201_p202.pdf
- [13] Ministry of Electronics and Information Technology, Govt. of India, "Data breaches and cyber incidents," Rajya Sabha Unstarred Question No. 3430, Mar. 25, 2021. [Online]. Available: https://rsdebate.nic.in/bitstream/123456789/717803/1/PQ_253_25032021_U3430_p162_p163.pdf
- [14] Ministry of Electronics and Information Technology, Govt. of India, "Data breaches and hacking of CoWIN and government websites," Rajya Sabha Unstarred Question No. 1039, Jul. 28, 2023. [Online]. Available: https://rsdebate.nic.in/bitstream/123456789/743482/1/PQ_260_28072023_U1039_p223_p223.pdf
- [15] Ministry of Electronics and Information Technology, Govt. of India, "Cyber attacks," Rajya Sabha Starred Question reply (statement), Feb. 3, 2023. [Online]. Available: https://rsdebate.nic.in/bitstream/123456789/739975/1/PQ_259_03022023_S18_p9_p11.pdf
- [16] "Humans are top factor in cloud security: CSA study," Security Boulevard, Aug. 2024 (reporting CSA Top Threats 2024 and the Thales 2024 Cloud Security Study). [Online]. Available: <https://securityboulevard.com/2024/08/humans-are-top-factor-in-cloud-security-csa-study>