

Chapter VII

System Security



Chapter – VII

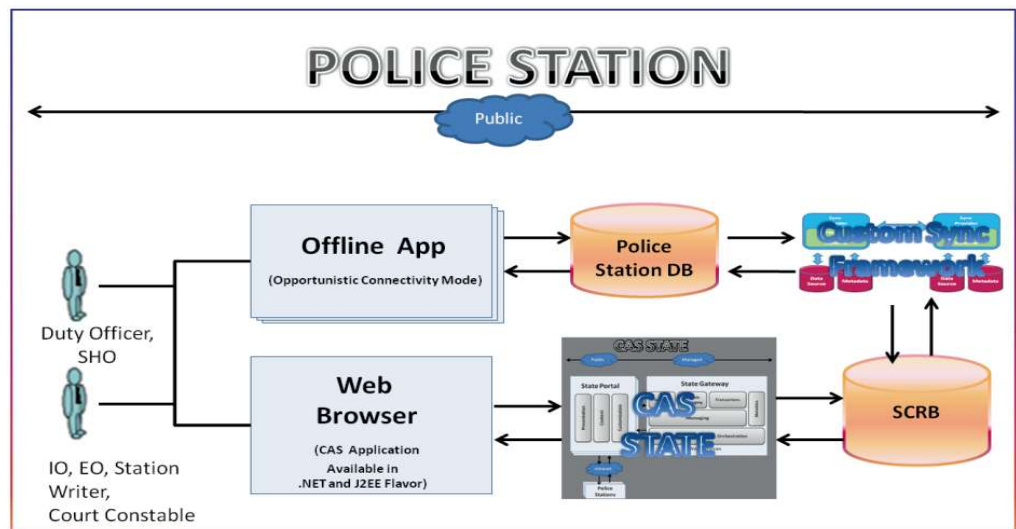
System Security

7.1 Deficiencies in system process for synchronisation of data and in manual process for backup of data

To address the challenges of network connectivity at Police Stations located in remote areas, CCTNS (CAS) was implemented (2014) with a combination of online-offline architecture, with one central online server located at the State Data Center (SDC) at Bhubaneswar accessed directly through the web-browser and local offline servers located at each Police Station. Simultaneously, the system was also designed to take regular backups in the hard disks and the PS users were required to take offline copies of the daily backups into an external media.

The transactions of the local offline servers and the central online server was designed to be synchronized when network connectivity between the State Data Centre and the remote Police Stations was available. Police stations could also choose to consciously work in offline mode despite available network connectivity for day to day work on CCTNS, since the system had higher responsiveness when working in offline mode. The details are described in the *Figure 7.1* below.

Figure 7.1 Chart Showing Data Synchronisation process



Source: CCTNS System Design Documents

The above diagram displays the overall process flow of using a custom sync framework through which the eligible data between SDC online database and Police Station local database were stated to be synced and *vice versa*. When the network status was online, reports of both the databases *i.e.*, online and offline would maintain consistency.

In order to protect against data loss at the Police Stations, in addition to the synchronisation activity between the local offline servers and the central online server, the system was also required to maintain a backup of the local database on a daily basis in the local offline server at the Police Station. The offline backup files were required to be moved periodically by the PS users to an external hard disk provided to each Police Station, to free up storage space on the local offline server.

Audit test checked the process of storing backups from the local offline server on external hard disks and noticed that in 56¹⁷ out of 68 Police Stations, these prescribed procedures had not been followed. Such non-compliance created the avoidable risk of loss of data and the associated impacts on police investigation and prosecution.

To derive assurance about the correct functioning of the synchronisation process, Audit analysed the transaction data pertaining to 40 out of 68 selected Police Stations as available in their local offline servers and as available in the central online server and noticed mismatches in data in the 40 PSs¹⁸ (*Appendix-XII*). These data mismatches are discussed below.

- i. There was disparity between the number of records pertaining to each Police Station, as stored in the local offline databases and the central online database, as detailed below:

Table 7.1: Statement showing disparity in number of records for Police Stations, between local offline databases and central online database as on March 2023

No. of Police Stations whose data was verified	Table Name	No. of records in central online database	No. of records in the local offline databases	Remarks
37	FIR registration	11,566	11,488	<ul style="list-style-type: none"> Two FIRs of offline database failed to sync with the online database. 80 FIRs of the online database failed to sync with offline records. During test check of Chudamani Marine PS, it was noticed that two FIRs of

¹⁷ Audit could not verify the procedure in the remaining 12 PS due to reasons like three Police stations were energy PSs and one police station was a traffic police station which were not functional. There were technical problems in the remaining eight offline servers which could not be checked.

¹⁸ Audit collected backups of offline databases from 40 police station during field audit. Some data tables could not be restored due to incompatibility of field types between MsSQL server data format and MySQL data format.

No. of Police Stations whose data was verified	Table Name	No. of records in central online database	No. of records in the local offline databases	Remarks
				Badagada PS, Ganjam were present in the offline database of Chudamani PS.
33	Arrest Memo	29,050	29,263	<ul style="list-style-type: none"> 221 arrest records of offline database failed to sync with the online database. Eight arrest records of online database failed to sync with offline records.
37	Charge Sheet/ Final Report	24,969	24,947	<ul style="list-style-type: none"> Two chargesheet/ final report records failed to sync with the online database. 24 chargesheet/ final report records failed to sync with offline records.
37	Missing person	1,916	1,944	<ul style="list-style-type: none"> 28 missing person records failed to sync with the online database
35	Dead body Registration	2,435	2,444	<ul style="list-style-type: none"> 51 dead body records of offline database failed to sync with the online database. 40 dead body records of the online database failed to sync with offline records.
38	Accused information	2,77,924	2,80,012	<ul style="list-style-type: none"> 2095 records of offline table were not available in the online table. 8 records of the online table were not in offline table.
40	Accused charge sheeted	1,25,674	1,25,655	<ul style="list-style-type: none"> 74 records of offline database were not available in the online database. 93 records of the online database were not in offline database indicating deletion from offline server.

Source: CCTNS database

Due to above highlighted disparities there is a serious risk associated with the deletion of records in local offline servers and its relevance cannot be overstated. If backend access is provided to Police Station users without stringent controls, it opens up significant vulnerabilities. Also, the absence of DBA logs for backend activities while operating in offline mode (as discussed in **Paragraph 7.3**) aggravates this risk, as it eliminates the ability to trace and audit critical actions taken on the server. Additionally, the lack of application user logs to track deletion activities during offline operations is a security lapse. These deficiencies created an environment ripe for data manipulation and loss, potentially leading to legal consequences, including destruction of crucial evidence, disruption of investigations, and loss of public trust.

- ii. There were mismatches in the contents/ values of data fields pertaining to seven test checked tables of the Police Stations, in the local offline

databases as compared to the central online database, which indicated synchronisation deficiencies in the system.

Table 7.2: Statement showing mismatches in contents/ values of data fields, between offline local databases and central online database

No. of Police Stations whose data was verified	Database Table Name	No. of data fields with mismatches	Count of total data mismatches
37	FIR registration	33	76,828
33	Arrest Memo	54	12,743
37	Charge Sheet/ Final Report	25	12,480
37	Missing person	12	2,633
35	Dead body Registration	33	1,891
38	Accused Information	50	41,508
40	Accused Charge sheeted	8	12,659

Source: CCTNS database

Thus, Audit concluded that there were deficiencies in the system process related to synchronisation of data between the local offline servers and the central online server of CCTNS. Further, the system lacked the functionality to generate alerts/ MIS/ Exception Reports when the synchronisation process led to mismatches between the number of records as well as the actual contents/ values of data fields in the tables of the database. The resulting inconsistent state of the central database rendered it incomplete, and hence the MIS Reports generated on the basis of the central database were not reliable.

During test check of local offline servers in the 68 selected Police Stations, Audit observed that in five Police Stations¹⁹, the backups had not been moved from the server to the external hard disk periodically. Due to this lapse, the storage space on the local offline server was full, and the automatic daily back up had failed. This resulted in the risk that in case of system crash or database damage, it would not be possible to restore the system without data loss.

Audit noticed an instance of loss of critical data due to system crash in Sector-7 PS, Rourkela, as described in the case study below.

¹⁹ Sheragada, Ganjam; Sadar PS, Jajpur; Mangalpur, Jajpur; Town PS, Jajpur; and Dhama, Sambalpur;

Case Study**Loss of FIR data in Sector-7 PS, Rourkela**

Due to absence of periodic transfer of backup of offline CCTNS data to the external hard disk, the local server storage space was full and daily backup process could not take place.

Chargesheet in case of FIR No. 28/2020 of Sector-7 PS of Rourkela district had been prepared through offline mode in CCTNS (in March 2020) but, the chargesheet had not been synchronized with the online CCTNS. Subsequently, in May 2022, the hard drive of the offline sever of Sector-7 PS, Rourkela crashed. The CCTNS helpdesk eventually restored the offline server data from the central online database, since the offline server backup data had been lost. However, the restored data did not include this Chargesheet, since it had not been synchronized.

As a result, although the chargesheet in case of FIR No. 28/2020 of Sector-7 PS, Rourkela had been generated through CCTNS and was available as a hard copy in the PS's case records, the same is now missing from both the offline and online databases and the FIR status of this case is incorrectly reported as 'Pending Investigation' in CCTNS.

- **Deficiency in handing over of charge by officers**

Audit also noticed that even after the transfer of IIC from a Police Station, the cases related to that Police Station could still be accessed by using the same credentials. Reports such as CDF and FIR generated by the transferred officer in the new Police Station continued to exhibit the place of posting as the old Police Station, as depicted in the examples below in *Figure-7.2*.

Figure 7.2: Figure Showing discrepancy in CDFs generated from Offline and Online Servers

<i>CDF (IIF-II) in the new station in online application</i>	<i>CDF (IIF-II) in the new station in offline application</i>

Source: CCTNS Reports

Government did not furnish any specific reply to the synchronisation and backup issues, and stated (September 2024) that the SsP had been instructed to direct all SHOs to take backup from server to external hard disk periodically. However, the synchronisation issues still remained unresolved.

7.2 Manual data entry at the back end of the central online server by the DBA, due to lack of synchronisation caused by missing static IP addresses for 16 Police Stations

As per system design, each Police Station's offline server was to be allocated unique static IP address. This was a vital requirement to enable the correct synchronisation of data between both the local offline servers and the central online server.

Audit analysed the master table for Police Stations in the CCTNS database and noticed that 662 Police Stations out of 678 had been assigned static IP addresses, and the remaining 16 PSs had not been assigned the same, as shown in *Table 7.3*:

Table 7.3: Table showing list of Police Stations with static IP addresses not assigned (for the period from January 2018 to March 2023)

Police Station Code	Name of the Police Station	Date of creation of record	IP Address	Number of FIRs registered	Starting date of registration of FIR	End date of registration of FIR
24482074	Anantpur	2023-01-09				
24484066	Agalpur	2023-01-09		48	2023-01-10 17:30:00.000	2023-03-30 20:45:00.000
24484067	Laxmijore	2023-01-09				
24495048	Karlapat	2023-01-09				
24496059	KOTIA			3	2022-06-10 09:30:00.000	2022-09-28 16:30:00.000
24496061	SPECIAL PS, ENERGY					
24497057	Manoharpur	2023-01-09				
24499044	Cyber Crime & Economic Offences, Mayurbhanj	2021-12-20		35	2021-12-31 20:43:52.000	2023-03-09 14:40:45.000
24499045	Bhanjapur	2023-01-09		89	2023-01-13 12:35:31.000	2023-03-31 19:00:00.000
24503064	TRAFFIC PS, CHANDIKHOL					
24503074	SPECIAL PS, ENERGY					
24861003	Airport Police Station, Jharsuguda	2022-12-01		35	2023-01-16 13:05:00.000	2023-03-31 20:20:00.000
24863028	Sadar	2023-01-09				
24864064	SPECIAL PS, ENERGY					
24865038	SPECIAL PS, ENERGY					
24867031	Traffic PS-2, Chandrasekharapur	2023-03-23				
	Total			210		

Source : CCTNS database

Out of these 16 Police Stations, 5 Police Stations had registered 210 FIRs during January 2018 to March 2023 through CCTNS. In the absence of static IP addresses, synchronisation of the data entered into the local offline servers was not possible.

Government stated (September 2024) that separate IPs have been allocated to the Police Stations. However, the fact remained that IPs had not been assigned to the above 16 Police Stations.

7.3 Deletion of key records in tables of CCTNS database, with inadequate maintenance of DBA logs to record such deletion of sensitive data

System design document specified that for each master data, there would be a user interface from which the administrators will be able to perform create, update, activate and de-activate a master record based on his privilege. The de-

activation would adopt soft deletion provision by marking 'D' in the appropriate status field of a record rather than deleting or removing the record. Audit noted hard deletion without any logs, contrary to the design documents as discussed below.

Audit examined records maintained by SCRB and noticed that SsP of Districts had raised requests to delete the FIRs/Complaints *etc.*, from the CCTNS database and the SI had deleted these FIRs/Complaints at the back end, through SQL script blocks. Audit analysed the database and noticed that there were 66 SQL procedures available which had been used for deletion of records from tables such as FIR master, chargesheet/ final form, accused, victims, witnesses, seizures *etc.*

Audit analysed the SQL procedure 'deletion of complete FIR' which was created on 17 January 2014 and observed that the procedure hard deleted the original records of the 332 FIRs of 148 Police Stations along with related complaints, accused, victims, witness records *etc.*, instead of soft deletion as prescribed above. The date and time of deletion, the FIR number and the user ID for the super-user were recorded in a log table, without preserving the original data deleted.

Further, detailed log details such as the old value stored in a database record when it was updated, were also not being recorded in the log table. The log table contained 890 records of deletions as shown below:

Table 7.4: Table showing details of types of deletions

Sl. No	Type of deletions	Number of Deletion	Starting date of deletion process	Last occurrence of deletion (Up to July 2023)
1	SEIZURE	59	2022-10-13 17:14:07.920	2023-06-07 11:46:20.363
2	Dead Body Registration	103	2022-10-13 19:03:20.653	2023-07-04 16:19:04.843
3	ARREST	93	2022-10-12 16:36:26.390	2023-06-17 19:08:59.837
4	Final Form	247	2022-10-12 17:55:07.830	2023-07-05 17:50:11.803
5	Missing Person	56	2022-10-13 18:46:02.187	2023-06-19 16:58:50.187
6	FIR	332	2022-10-12 16:41:15.230	2023-07-05 17:29:46.590
	Total	890		

Source: CCTNS Database

- There was hard deletion of original records of FIRs, accused, victims, chargesheets *etc.* Instead of deletion, the original records should have been marked or flagged as 'D', as per system design documents.

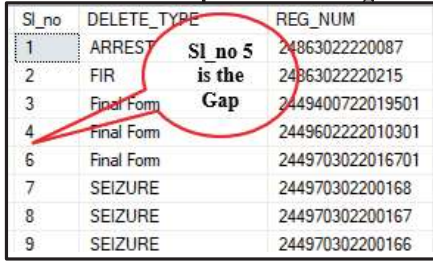
- The first log capture date in the log table was 12 October 2022 and log for the prior periods (17 January 2014²⁰ to 11 October 2022) were not available. This indicated either purging of earlier records or non-maintenance of logs for the prior period. As a result, Audit was unable to derive assurance that no unauthorized deletion of data had taken place during the period from January 2014 to October 2022.
 - As per table design, every log was assigned a sequential number, beginning with one, and each subsequent log was assigned a number one higher than the previous one. However, the log sequence of the log table revealed that there was a gap in the sequence. This indicated that the log had been deliberately deleted.
- Figure 7.3: A sample showing gap in the sequence of the log**
- 
- | Sl_no | DELETE_TYPE | REG_NUM |
|-------|-------------|------------------|
| 1 | ARREST | 24863022220087 |
| 2 | FIR | 24863022220215 |
| 3 | Final Form | 2449400722019501 |
| 4 | Final Form | 2449602222010301 |
| 6 | Final Form | 2449703022016701 |
| 7 | SEIZURE | 244970302200168 |
| 8 | SEIZURE | 244970302200167 |
| 9 | SEIZURE | 244970302200166 |
- Source : Database analysis*
- During inspection of the selected 10 SP offices, Audit collected and test checked 100 request letters for deletion of FIRs from five SsP in respect of 49 Police Stations which were deleted by the DBA. Audit compared these requests with the FIR deletion data in the database and observed that only 28 FIRs were shown deleted in the 'FIR Delete Log' table. The remaining were deleted using raw SQL rather than using the procedure 'deletion of complete FIR'. Due to this, the log trails in such deletions were not recorded or captured in the 'FIR Delete Log' table.
 - In case of three Police Stations²¹, eight FIRs had been deleted using the system procedure without any written requests from SsP, as logs of these eight FIRs were in the 'FIR Delete Log' table.
 - There were 'orphan records'²² in different tables, as mentioned below:

Table 7.5: Showing orphan records

Master Table	Transaction Table	Number of records not in Master Table but present in Transaction Table	Number of Police Stations involved
FIR Registration	Crime details	22	20
FIR Registration	Arrest Memo	06	06
FIR Registration	Seizure Memo	11	10

²⁰ Date of creation of the procedure for deletion of FIR

²¹ Chauhiaganj (4 FIR Nos: 24862004230029, 24862004230030, 24862004230031, 24862004230032), Mancheswar (2 FIR Nos: 24867011230007, 24867011230008) and Balipatna (2 FIR Nos: 24867017220325, 24867017220326)

²² Orphan records are database entries that reference non-existent parent records due to deletion or missing parent data, compromising data integrity.

Master Table	Transaction Table	Number of records not in Master Table but present in Transaction Table	Number of Police Stations involved
FIR Registration	Final Report/Chargesheet	18	16
General Diary	FIR Registration	163	23
General Diary	Arrest Memo	1,563	256
General Diary	Seizure Memo	54	20

Source: CCTNS database

The presence of orphan records indicated that records of master table were deleted but the transaction table still had references to the deleted master records.

- **Absence of user IDs in system logs:** Whenever a record is created or updated, the system typically logs the user ID responsible for the action. However, data analysis revealed 7,350 instances from the four key tables of CCTNS where the system failed to record the user ID, as shown below.

Table 7.6: Showing instances where user ID who updated records was not recorded

Table Name	Number of Police Stations affected	Instances where user ID was not recorded
1. FIR Master	474	3,583
2. Crime Details	81	169
3. Accused Master	93	461
4. Chargesheet Master	206	3,137
Total		7,350

Source : CCTNS Database

In conclusion, there should have been no provision for deletion of FIRs from the system (as there is no legal provision for tearing off pages from the physical FIR Register). This practice was highly irregular and the FIRs with incorrect details should have only been marked in the system as ‘incorrect/ closed’.

Absence of recording user IDs when changes are made to the key tables or in sensitive data fields related to police investigation, deletion of records at the back end without authorisation from the competent authority, deletion of records in an improper manner resulting in creation of ‘orphan records’, hard deletion of records and purging of records from the database instead of soft

deletion, lack of full details of old contents/ values of records in tables when they are updated - all indicated avoidable risk areas related to harassment of complainants and collusion with the accused individuals.

In reply, Government stated (September 2024) that the SI is being instructed to ensure that appropriate log data are captured in log tables for maintaining proper audit track.

Recommendation

Government should ensure that

- *appropriate application log and DBA log should be maintained to track users' actions and fix responsibility in case of gross errors/ manipulation of records;*
- *appropriate validation and input controls are implemented to maintain data consistency;*
- *synchronisation process should be rectified to maintain consistency of data between the offline and online database apart from ensuring data backups of the offline servers at police stations;*
- *no primary record should be deleted and in case deletion is required, soft deletion method as mentioned in the system design documentation is adopted along with appropriate application and system logs; and*
- *a supervisory tool is developed to identify exceptional events by the technical team at headquarters and take necessary action. Further, periodic exception reports may be monitored by higher authorities.*