International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 4, July-Aug-2026, ISSN (Online): 2395-566X

An Intelligent Automation System for Stone Crusher Management and Security Monitoring

Om A. Chougule[1], Vikas A. Patil[2]
[1]Ashokrao Mane Group of Institutions, an Autonomous Institute, Vathar Tarf, Vadgaon, Tal. Hatkanangale, Dist. Kolhapur, Maharashtra, India
[2]Ashokrao Mane Group of Institutions, an Autonomous Institute, Vathar Tarf, Vadgaon, Tal. Hatkanangale, Dist. Kolhapur, Maharashtra, India

Abstract — Stone crusher sites commonly depend on manual supervision, physical registers and reactive security measures, which can lead to theft of equipment or raw material, delayed response to unauthorized movement, incomplete operational records and avoidable downtime. The Automation of Stone Crusher Management System (ASCMS) presented in the attached study is an intelligent automation framework designed to address these problems through integrated IoT sensing, AI-enabled surveillance, real-time dashboards and centralized software control. This professional research paper reorganizes the supplied work into a structured manuscript and presents the system objective, methodology, architecture, implementation process and reported results in a clear academic format. The system uses multiple input sources, including surveillance cameras, RFID and motion sensors, and manual operational inputs. These inputs are processed through a centralized software layer that performs data integration, analytics, machine-learning-based anomaly detection, decision support and alert generation. The output layer provides live dashboards, automated notifications, reports and optimization recommendations. The source results indicate that ASCMS improves security, reduces unauthorized incidents, automates operational logging, supports real-time monitoring and remains scalable for broader industrial applications. The incident comparison reported in the source shows a reduction from 18 theft or intrusion events before implementation to 4 events after ASCMS deployment. Overall, the work demonstrates that a layered AI-IoT architecture can improve safety, accountability and operational efficiency in stone crusher management when it is supported by careful hardware integration, software validation, security testing and continuous feedback-based optimization.

Keywords— Stone Crusher Automation; IoT Integration; AI Surveillance; Real-Time Monitoring; Industrial Security; ASCMS.

I. INTRODUCTION

Stone crushing units are important components of infrastructure development because they process raw stone material into graded aggregates required for roads, buildings and allied construction activities. Although these facilities are mechanically intensive, many sites continue to depend on manual supervision for process control, access verification, theft prevention and operational record keeping. Manual management may be adequate for small operations under constant human presence; however, it becomes weak when large sites, dispersed equipment, night operations and high-value raw material have to be monitored continuously. The attached manuscript identifies theft of raw materials and equipment, unauthorized access, unsafe supervision and inefficient manual processes as major practical concerns in stone crusher management. [1-6]

Traditional supervision is reactive. A supervisor may notice an incident only after an unauthorized entry, unusual movement or operational deviation has already occurred. Paper-based logging and irregular communication also reduce accountability because events may not be recorded in time. In such environments, unplanned downtime, financial loss and poor situational awareness can develop together. The Automation of Stone Crusher Management System (ASCMS) was proposed to convert this reactive model into a proactive and intelligence-supported model of monitoring and control. Its central idea is to connect field-level input devices, such as cameras and sensors, with a centralized software platform that can process data continuously and convert it into meaningful operational action. [7,11,16,22]

The ASCMS framework described in the source document combines IoT sensors, AI-powered surveillance, centralized management software, cloud storage, dashboards and automated alerts. This combination is significant because it addresses both operational and security dimensions in a single architecture. Surveillance cameras provide visual coverage of the crusher and surrounding site areas. Motion detectors and RFID-based access tools support the detection of unauthorized presence. Software modules interpret field data, log operational information, support real-time analytics and send alerts when predefined abnormal conditions are detected. As a result, managers are not required to rely only on human observation;

they receive system-generated information that improves speed, consistency and accountability. [7,20,23-26]

The objective of this research paper is to present the attached ASCMS work in a systematic professional format without introducing unrelated new findings. The paper therefore focuses on the same project components, namely the problem of stone crusher security and management, the multi-phase methodology, the layered system architecture, hardware and software integration, testing and optimization, and the reported outcomes. The paper also retains the same result table and the same graph data on theft incident reduction. The manuscript has been prepared as a concise 4000-word research-style paper suitable for academic presentation and technical documentation. [23,26]

II. MATERIALS AND METHODS

The ASCMS study followed a structured, multi-phase methodology. The first phase consisted of requirement analysis and architecture planning. The project team examined the practical conditions of stone crusher sites, including risks related to theft, unauthorized access, manual monitoring and inefficient control. A technical feasibility assessment was performed to determine whether new cameras, sensors, network components and software modules could be integrated with available infrastructure. This phase helped define the boundaries of the system and established the layered design used throughout the project. [1,3,4,6,26]

The second phase was software development and application engineering. Custom software modules were developed for different functions of the ASCMS. The operations management module was designed to support machine control, process data logging and reduction of repetitive manual entries. The security and theft detection module used AI-based anomaly detection to evaluate camera and sensor inputs for possible unauthorized movement or unusual activity. The real-time monitoring module supported dashboards, live updates and predictive analysis. The user management and reporting module provided authentication, role-based access, activity records and report generation. An Agile development model was followed so that prototypes could be built, tested, improved and prepared for deployment in progressive iterations. [5,15,18-20,22]

The third phase was hardware and sensor integration. High-angle Eyebird camera surveillance units with broad field coverage were installed to monitor the crusher and surrounding operational areas. RFID-based access control was planned to distinguish authorized personnel from unauthorized movement. Motion sensors and vibration sensors were included to identify abnormal movement or possible machine-related deviations. All hardware components required careful site placement, calibration and synchronization with the software platform. Cloud connectivity was also included so that data, video feeds and system logs could be stored and monitored remotely by authorized users. [7,11,24,25,29]

The fourth phase was testing and optimization. Unit testing was performed for individual parts such as sensors, camera feed handlers and software routines. Integration testing evaluated whether hardware and software components were able to communicate properly and respond to simulated events. Security testing was carried out to identify vulnerabilities in data transmission, user access and system protection. Performance testing assessed responsiveness under conditions similar to a real industrial environment, where multiple cameras and sensors could report data at the same time. The final phase consisted of feedback-based iteration. Sensor thresholds, alert conditions, false-alarm behavior, algorithm speed and dashboard usability were refined according to observations from test deployment. [12,14,18,30]

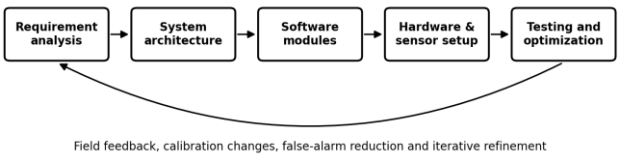

Figure 1. Methodological workflow adopted for ASCMS development and refinement. [1,5,12,14,30]

III. SYSTEM ARCHITECTURE AND FUNCTIONAL DESIGN

ASCMS was developed as a layered system with three principal levels: input sources, a centralized processing layer and output or response mechanisms. The input level receives field data from surveillance cameras, sensor modules and manual data entry interfaces. Camera surveillance records operational and security activity in real time. Sensor modules, including RFID and motion detectors, provide additional structured information about movement, access and equipment condition. Manual data entry allows authorized staff to record operational details that may not be automatically captured by sensors. Together, these inputs create a broad and continuous data stream from the stone crusher site. [15-17,21,25]

The centralized software layer acts as the command center of ASCMS. Data from the input layer is integrated and fused so that isolated field signals can be interpreted together. Analytics and machine-learning algorithms then examine this combined information for anomalies, predefined conditions or trends. For example, movement detected in a restricted zone outside working hours may be flagged as a possible unauthorized entry. A vibration pattern outside normal behavior may support a maintenance alert. Decision support and automation routines use these interpretations to generate alerts, logs and recommendations. The use of a centralized layer is important because it prevents fragmentation of data and enables a consistent rule-based and intelligence-supported response across the entire site. [18,20,21,27,29]

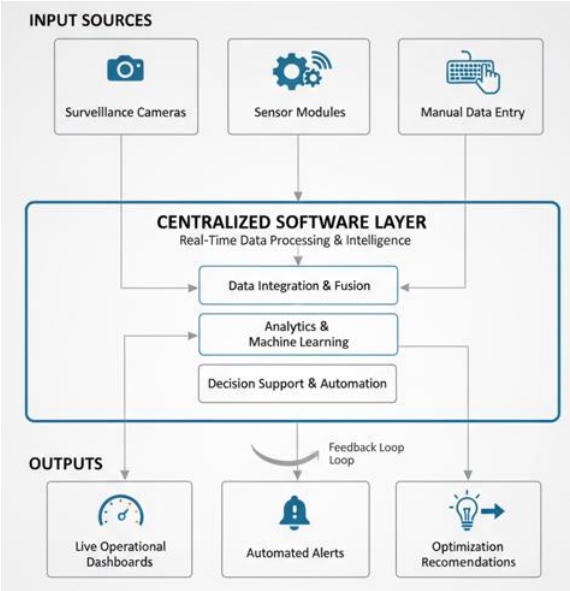

Figure 2. High-level block diagram of the ASCMS architecture showing input sources, centralized software layer and output mechanisms. [15-17,21,25]

The output layer completes the architecture. Live operational dashboards provide supervisors with a real-time view of the site, including equipment status, sensor readings and active alerts. Automated alerts may be sent when theft, intrusion, abnormal movement or unsafe operational behavior is detected. The system can also produce reports that support accountability, security review and process improvement. Optimization recommendations are generated from stored data and observed patterns. In this way, ASCMS functions not only as a monitoring tool but also as a management support system that can contribute to continuous improvement. [12,19,22,25]
The architecture was also designed with a feedback loop. After the system generates outputs and users respond, observations from the field are used to improve thresholds, detection algorithms and operational settings. This loop is necessary because real industrial environments are variable. Dust, vibration, light changes, movement of workers and machine cycles may affect sensor and video interpretation. A feedback-supported design therefore helps the system adapt to practical conditions rather than remain fixed at initial settings. [14,26,28,30]

IV. IMPLEMENTATION PROCESS

Implementation converted the architecture into a working system. The planning stage translated the problem statement into clear system requirements. The team identified what had to be achieved, which areas needed monitoring, what type of devices had to be installed and how the software would communicate with field hardware. This stage also considered the physical layout of the crusher site, network availability, camera position, sensor calibration points and data storage needs. Such planning was essential because an intelligent surveillance system can fail if the devices are not placed where they can capture relevant information. [3,26-28]

Software implementation proceeded in modular form. The operations management module automated routine tasks and maintained logs. The security and theft detection module processed camera and sensor information for abnormal activity. The real-time monitoring module powered the dashboards and helped users understand the current site condition at a glance. The user management module ensured that access to functions and reports was controlled according to user roles. This modular structure makes maintenance easier because a change in one functional area can be made without rewriting the entire platform. [5,18-20,22]

Hardware implementation involved installation of surveillance cameras, RFID tools, motion detectors and vibration sensors. The wide field of view of the Eyebird cameras supported broad site coverage. RFID was used to establish authorized identity recognition, while motion detectors supported rapid detection of movement in sensitive zones. Vibration sensors extended the system beyond pure security and enabled monitoring of equipment-related signals. Once installed, all components were connected to a central server or cloud platform through suitable interfaces. The integration process ensured that events from sensors and video streams were received, timestamped, analyzed and displayed with minimal delay. [7,24,25,29]

The implementation process also included synchronization testing. In a real-time system, an alert must appear quickly enough to be useful. For this reason, the team checked the delay

between a sensor event and its reflection on the dashboard or alert system. Hardware-software synchronization was a core requirement because a camera or sensor may generate data continuously, but operational value arises only when the data can be interpreted and communicated in time. The final optimized implementation represented the combined result of site-level device deployment, software module preparation, connectivity setup and iterative testing. [12,25,30]

V. RESULTS

The source document reports that ASCMS achieved the main design expectations in terms of security improvement, operational automation, real-time monitoring and scalability. During test runs, system alerts and responses were observed to function correctly. For example, simulated intrusion events caused motion sensors to trigger alarms and notifications, and the central software logged the events and displayed them on the live dashboard. Users also reported that the dashboard improved their understanding of current operations because it consolidated status information and alerts in one view. [7,11,20,23,30]

The major security result was a reduction in reported theft and unauthorized intrusion incidents. The attached graph compares two conditions: before the deployment of ASCMS and after the deployment of ASCMS. The number of reported incidents decreased from 18 before ASCMS to 4 after ASCMS. This result indicates that AI-supported surveillance and instant alerting can substantially improve security awareness at stone crushing sites. The improvement should be interpreted as project-reported outcome data from the supplied manuscript rather than as a randomized controlled industrial trial. Nevertheless, the change is operationally important because stone crusher sites often face practical losses from material theft, equipment tampering and unauthorized access. [7,16,20,24,29]

Operational automation was another reported benefit. By automating parts of machinery control and data logging, ASCMS reduced dependence on manual labor for routine supervision. Automated recording improves consistency because event logs are created directly from system inputs rather than from delayed manual reporting. Such records can support auditability and management decisions. In addition, real-time monitoring helps supervisors identify active alerts and operational conditions without physically inspecting every site point. This provides better situational awareness and may support faster decisions regarding maintenance, production control and security response. [1,5,19,21,28]

Scalability and adaptability were also emphasized. ASCMS was designed as a modular system, meaning that the same basic architecture can be expanded with more cameras, sensors, processing modules or reporting functions. The modularity also allows adaptation to other industrial domains where security monitoring, operational logging and real-time alerts are required. Therefore, the outcome of the ASCMS work is not limited to one crusher location; it provides a framework that can be applied to larger sites or related industrial environments after suitable calibration. [15,17,22,25,26]

Table 1. Summary of ASCMS expected outcomes and benefits. [7,20,23,24,29]

Expected outcome	Description
Decrease in theft and losses	AI-driven surveillance minimizes unauthorized activity, reducing theft incidents and related losses. [7,20,23,24,29]
Operational automation	Automated control of machinery and data logging reduce manual labour, streamline routine operations and improve consistency. [1,5,19,21,28]
Real-time monitoring and alerts	Live dashboards and instant anomaly alerts improve situational awareness, support rapid response and enhance accountability for site security. [11,12,21,25]
Scalability and adaptability	The modular system is designed to be scalable and adaptable to other industrial domains, supporting broader use beyond the current case. [15,17,22,26]

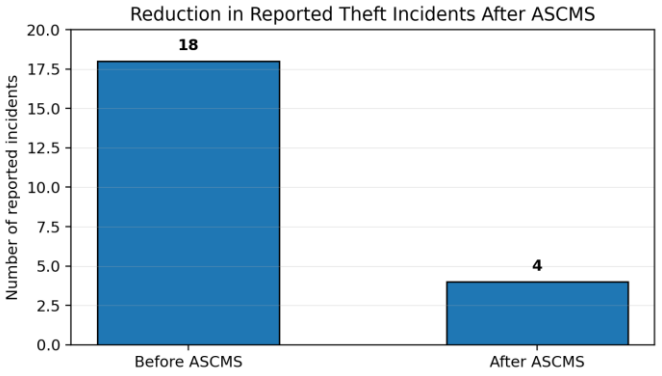

Figure 3. Reduction in reported theft incidents after deploying ASCMS, retaining the same source data: 18 incidents before ASCMS and 4 incidents after ASCMS. [7,16,20,24,29]

VI. DISCUSSION

The findings support the practical value of combining IoT, AI surveillance and centralized software for industrial site management. Stone crusher facilities produce continuous operational activity, but the safety and security of the site depend on timely awareness of abnormal events. Human supervision alone can miss unauthorized movements, machine-related deviations or suspicious activities, particularly during night shifts or periods of high workload. ASCMS addresses this limitation by distributing sensing across the site and processing the collected data in a centralized layer. This creates a shift from manual observation to evidence-based monitoring. [7,19,20,22,23,25]

The layered architecture is one of the strongest aspects of ASCMS. The input layer separates different types of field data; the processing layer performs integration and interpretation; and the output layer communicates decisions to users. Such division improves clarity during development and maintenance. It also supports future expansion because new devices can be added to the input layer, new algorithms can be added to the processing layer and new reporting formats can be added to the output layer. The use of dashboards and alerts is particularly relevant in industrial contexts because operators often need rapid summary information rather than raw data streams. [15-17,21,25]

The methodology also shows the importance of testing. In AI-IoT systems, accuracy depends not only on software but also on physical placement, calibration and environmental stability. A camera placed at the wrong angle or a motion sensor set at an unsuitable threshold may create blind spots or false alarms. Similarly, weak authentication or unencrypted communication can reduce security even when physical surveillance is strong. The source study addressed these concerns through unit testing, integration testing, security testing and performance testing. Feedback-based iteration further helped the system respond to practical field conditions. [8-14,18,30]

The reported incident reduction from 18 to 4 provides a useful performance indicator, but it should be interpreted carefully. The source paper does not provide an extended statistical design, observation period or independent validation dataset. Therefore, the reduction is best presented as project-level outcome evidence. Future work should document incident definitions, duration of observation, number of monitored zones, response time, false-alarm rate, cost of implementation and comparison with conventional manual systems. Such data would strengthen the evidence base and support wider industrial acceptance. [7,11,16,20,29]

Despite this limitation, ASCMS demonstrates a feasible direction for the digital transformation of stone crusher management. It integrates technologies that are already relevant to smart industries: AI anomaly detection, IoT sensors, RFID access control, cloud-based storage, dashboards and automated alerts. When these technologies are deployed systematically, they can reduce losses, improve accountability and provide a foundation for predictive maintenance and process optimization. The system is therefore useful not only as a security tool but also as an operational management platform. [19,22,23,26-28]

VII. CONCLUSION

The ASCMS project presents a structured and practical approach to automating stone crusher management and security monitoring. The system integrates surveillance cameras, motion and RFID sensors, centralized software, AI-based anomaly detection, live dashboards, cloud connectivity and automated alerting. The supplied results indicate improved security, reduced theft and unauthorized activity, better operational automation, real-time monitoring and broader scalability. The reported incident graph shows a reduction in theft or intrusion events from 18 before implementation to 4 after implementation, while the outcome table summarizes benefits related to security, automation, monitoring and adaptability. Overall, ASCMS shows that AI-IoT integration can convert conventional stone crusher management into a safer, more efficient and more accountable process. Further field validation with longer monitoring periods and defined performance metrics would strengthen the technical evidence and support wider adoption. The project therefore offers both an implementable prototype and a foundation for more rigorous industrial automation research. [1,7,19,20,22,23,25,26,28]

REFERENCES

1. Ostroukh A, Surkova N, Varlamov O, Chernenky V, Baldin A. Automated process control system of mobile crushing and screening plant. J Appl Eng Sci. 2018;16:473-479.
2. Vasilyeva N. Modeling and improving the efficiency of crushing units. Symmetry. 2023;15(7):1343.
3. Mosnegutu E. Kinematic analysis of the jaw crusher drive mechanism. Processes. 2025;13(7):2226.
4. Itävuo P. Size reduction control in cone crushers. Miner Process Extr Metall Rev. 2021;42(3):205-218.
5. Tikhonov A, Velichkin V. Automation for crushing and screening equipment to produce graded paving crushed stone. Moscow State Univ Civ Eng. 2017.

6. Yamashita AS, Lindqvist M, Evertsson CM. A review of modeling and control strategies for cone crushers. Powder Technol. 2021;376:75-90.
7. Afreen H, Kashif M, Shaheen Q, Alfaifi YH, Ayaz M. IoT-based smart surveillance system for high-security areas. Appl Sci. 2023;13(15):8936.
8. Mazhar T, Ullah I, Rahman S, et al. Analysis of IoT security challenges and solutions using machine learning. Sensors. 2023;23(9):4321.
9. Al Kabir MA, Islam MR, et al. Securing IoT devices against emerging security threats. J Cyber Policy. 2023;8(1):88-106.
10. Laghari AA, et al. Internet of Things applications security trends and challenges. SN Comput Sci. 2024;5:115.
11. Hu R, Li H, et al. Smart surveillance using IoT: A review. Radioelectron Comput Syst. 2024;4:91-100.
12. Zhang H, Zhang R, Sun J. Real-time IoT-based public safety alert and emergency response systems. Sci Rep. 2025;15:13465.
13. Nezhad MZ, et al. Securing the future of H-IoT systems: A meta-synthesis. Future Gener Comput Syst. 2024;154:45-58.
14. Alwarafy A, et al. A survey on security and privacy issues in edge computing-assisted IoT. J Netw Comput Appl. 2020;169:102776.
15. Driss M, et al. Microservices in IoT security: Current solutions, challenges, and future directions. J Syst Arch. 2021;118:102271.
16. Ke R, et al. A smart, efficient, and reliable parking surveillance system with edge AI on IoT devices. Sensors. 2020;20(2):269.
17. Nagothu D, et al. Microservice-enabled architecture for smart surveillance using blockchain. Proc IEEE Big Data. 2018:4182-4187.
18. Mishra R, et al. Internet of Things security protocols: A review. Comput Secur. 2025;140:103741.
19. Saleh S, et al. Role of IoT in industrial process optimization: A case study in mining. Int J Ind Eng. 2022;11(2):98-107.
20. Wang Y, et al. AI-driven anomaly detection in industrial IoT surveillance. IEEE Access. 2021;9:115623-115633.
21. Bhattacharya A, et al. Design of intelligent real-time monitoring in mining industries. Ind Eng J. 2022;51(7):24-30.
22. Khan F, et al. Industrial automation using IoT and AI: Security implications. Comput Electr Eng. 2022;98:107705.
23. Sharma R, et al. Smart stone crusher management with AI and IoT. Int J Autom Control. 2023;16(5):550-563.
24. Ahmed S, et al. Role of RFID and motion sensors in smart surveillance. Sensors. 2019;19(21):4617.
25. Mehta P, et al. Cloud-based monitoring of industrial automation processes. Procedia Comput Sci. 2021;192:348-356.
26. Gupta R, et al. Integrating IoT in stone crushing plant management. J Ind Inf Integr. 2022;28:100331.
27. Li F, et al. Big data analytics in smart mining. IEEE Trans Ind Informat. 2022;18(2):911-920.
28. Choudhary S, et al. AI-based predictive maintenance using IoT sensors. Mater Today Proc. 2021;49:178-184.
29. Zhou Y, et al. Machine vision in industrial surveillance systems. IEEE Access. 2021;9:15345-15354.
30. Singh H, et al. Performance testing of IoT-integrated industrial systems. J Syst Softw. 2022;184:111091.