BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

AI-Powered Zero Trust Smart Shopping Mall Security System: A Review and Proposed Framework

[1]Yadav Varun Nitin, [2]Prof. Varsha Babar

[1]Student, TE-C (AI & DS), PRN: 72426676L, [2]Mentor, SPPU Technical Seminar ELC342CSD
[1,2]Dept. of Artificial Intelligence and Data Science
[1,2]Ajeenkya DY Patil School of Engineering, Pune, India

Abstract

Modern Shopping Malls consist of many Payment Terminals, CCTV Cameras, IoT Devices, Cloud Services and Public Wi-Fi. While this provides convenience for the user it introduces many potential entry points making traditional security methods inefficient. By applying real time behavioural analysis to detect anomalies and improve the Zero Trust solution using Artificial Intelligence. This paper looks at seven papers that were published between 2024-2025 on AI anomaly detection, continuous authentication, AI Security Operations Centre, Zero Trust in Smart Cities, Fraud Detection in Payments, Threat Analysis in IoT and Micro-segmentation in IoT. Each study only focuses on one aspect of this area and does not provide security across the entire smart mall. Findings have lead to the development of a multi layered framework to apply AI powered Zero Trust in smart malls. This looks into the applications, benefits and challenges.

Keywords: artificial intelligence; cloud security; identity and access management; internet of things; multi factor authentication; security operations centre; smart shopping mall; threat detection; zero trust architecture; zero trust network access.

I. Introduction

Shopping Malls have developed into Smart environments providing a safe, convenient and personal service. Modern Shopping Malls can have many hundreds or thousands of devices including CCTV Cameras, Biometrics, Parking Sensors, Payment Systems, POS Systems, Staff Devices, Mobile Applications, Public Wifi, Cloud Databases, Digital Displays and Building Management.

This can increase security (CCTV), automatic monitoring (Sensors), faster payments (Digital Payments), better way finding, offers and parking (Mobile Applications). There can be too many new points of entry [4]. If any of these devices are compromised (CCTV, Staff Devices, IoT Devices and Network Devices) they can act as a point of entry [3].

Traditionally the Shopping Mall would have had a secure network within but if attackers can get valid credentials it gives them full access to the system as they are seen as a legitimate user [5]. The Shopping Mall should attempt to put a system in place where users and devices are not automatically trusted [1].

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Contribution:

1) This paper is a review of seven articles from 2024-2025 which look at how to improve security using AI and/or Zero Trust in the retail, IoT and smart building sectors.

2) Outstanding problems with Smart Shopping Malls.

3) Multi layered Framework for implementing AI powered Zero Trust.

This paper has some background information in section II and also contains a literature review within section III. Section IV discusses comparing the research, section V outlines the research gaps. Section VI shows a framework and section VII looks at applications, benefits and challenges. Finally section VIII gives a conclusion..

II. Background

A. Attack Surface of Smart Mall

There are many areas within a shopping mall that would need protection. These would include Payment Systems, Security Systems, Building Systems, Guest WiFi, Staff/Tenant Network and Cloud Based Services. These can face threats such as Ransomware, Phishing, Payment Fraud, Data Theft, Insider Threats, Compromised IoT Devices and Unauthorised Access [6]. Vulnerabilities that can occur would be compromised firmware on IoT Devices, Insecure API's on Cloud, Insecure Payments and Compromised CCTV [6].

B. Zero Trust Security

The concept behind Zero Trust is that we should be applying the principle of 'Never Trust, Always Verify'. Continuous verification of users, devices and applications occur [1]. The core concepts of Zero Trust include Multi-Factor Authentication (MFA), Identity and Access Management (IAM) and segmentation of networks and endpoints [2][4].

C. AI

Traditionally this can be challenging but AI can be used to identify a normal pattern and detect anomalies [1]. There are 3 ways that AI can be utilised within Zero Trust [5]:

- Behavioral analytics – Understand what normal activity looks like for a user/device and score them
- Intrusion Detection – ML can be used to detect anomalous activity
- Automated Incident Response – Contain threats

III. Literature Review

A. Scope & Methodology

The literature reviewed is from 2024-2025. Papers were reviewed based on what security they offer, what part of the security they protect, artificial intelligence implementation, contextual based policies and what limitations were present. A narrative review has been conducted and therefore isn't a systematic review. This means results can be viewed as a summary of the literature.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

B. Evidence

AI & Zero Trust are complementary technologies. AI can be used to determine there may be anomalies by using an anomaly score however this doesn't prove anything malicious. Zero Trust can be used to support policies however it may not be quick enough as policies are static. A solution should include a policy engine that uses identity, device health, resource sensitivity, network context and risk score. If there is uncertainty or an action could cause interruption to essential services a human will be required.

C. AI & Zero Trust Authentication

Anomalies can be detected by creating a baseline of 'normal' behaviour using statistical models or ML. This can be used to detect anomalies throughout the retail network. For example, login, payment frequency & device fingerprinting. Any requests outside the normal parameters will trigger an alert. The anomaly score is passed to the Zero Trust policy engine. This means only users who pass identity and risk checks can log in. This provides greater accuracy for detecting anomalies however the model was only trained on simulated data. We don't know how it would perform with real data such as CCTV/IoT.

This provides continuous authentication [9]. Users receive a confidence score based on their behavioural biometrics such as typing speed, mouse movement or touch pressure. If the score drops below the threshold the user will need to reauthenticate using MFA. This reduces trust over time. It helped reduce insider threats and improve accuracy however it wasn't applied at a large scale (e.g. mall). The data was sampled from a small enterprise. It didn't look at CCTV or smart sensors.

D. AI Based Security & Scaleable Zero Trust

Lee et al used AI to consolidate from multiple sources during the log collection phase [10]. Classification models based on ML can be used to correlate multiple sources over time. For example Gradient Boosting Algorithms or Deep Sequence Models. This helps detect multi-stage attacks which couldn't be detected using single sources. Playbooks can be created to automatically take action e.g. isolate host or revoke token. This provides quicker response times however requires large volumes of logs. This would require large compute resources. It wasn't designed to be used in a mall.

Singh et al implemented continuous contextual authorisation in a distributed city [11]. Everything is centralised, however data can be collected from different sub networks. For example traffic systems, public wi-fi & municipal IoT. This provides user authorisation. Each sub network has some local control but follows the same trust model which is constantly updated. This improves control & monitoring. However it was based on case studies from smart cities. It didn't look at specific scenarios. For example tenant store isolation. Little use in real world scenarios.

E. Fraud Detection & Threat Analysis

Supervised learning was used to detect fraud [7]. Features such as amount, location, merchant type & time were used to train classifiers. Ensemble methods or neural networks can be used to understand complex spending patterns. We were able to detect fraudulent transactions and suspicious activity. Unfortunately there is no confirmation of users/devices so it only provides security at payment layer. It wasn't trialled in a real world scenario.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

A threat analysis was performed on the IoT, Cloud & Retail infrastructure [6]. Attack vectors were mapped to areas of concern. For example vulnerable firmware on IoT devices, insecure API's on the Cloud, insecure payment platforms & exposed CCTV. This gave us a clear understanding of the attack surface. We have a broad framework for the mall. It was a concept study so provided no recommendations for secure architecture.

F. Identity Verification & Micro Segmentation

Each IoT device had a unique identity (X.509 Certificates) [3]. Heathy checks were performed to ensure the IoT device could connect to the network (firmware version/configuration). The network was broken down into smaller VLAN's. This meant if a device was compromised it could not access anything outside of the zone. This meant less damage would occur if the device failed to authenticate. IoT devices are more secure with less attack surface. However no behavioural analysis was performed.

G. Summary

There are 4 main areas to consider. None of the papers looked at all areas. Risk adaptive identity verification [9], Device level micro segmentation [3], Behavioural anomaly detection [7,8] & Centralised automated responses [10,11].

IV. Comparative Analysis

A. Evaluation Metrics:

There were five metrics used to evaluate the techniques; 1. Device/user coverage, 2. Continuous/contextual, 3. Anomaly detection, 4. Isolation and 5. Applicable in a hybrid retail environment. IoT based solutions had greater information on device identification and segmentation. Authentication focused solutions only focused on users. Fraud based models can be useful during payments. AI security can correlate events across multiple sources. However, these cannot completely guarantee security across all areas of the mall.

B. Implications of using in a Mall:

A mall will have specific zones with clear implications of failure. Public WiFi clients should be restricted to using point of sale terminals if compromised. Cameras should not be able to connect to tenant systems. Staff accounts should not automatically have access to customer databases. This means policies should be set based on what their role is doing and how sensitive the data is. The main requirement is to have a unified system controlling users, devices, network, applications and monitoring.

Overall, as seen in table I, all the papers focused on securing just one aspect of the issue. All techniques had limitations. They lacked real world testing, limited CCTV/IoT coverage and did not focus on shopping malls.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Table I: Literature Survey Matrix

Author/Year [Ref.]	Methodology	Key findings	Limitations
Sharma et al. 2025 [8]	AI anomaly detection and Zero Trust authentication in retail	Improved threat detection accuracy. Reduced unauthorized access.	Limited CCTV/IoT coverage. Model only tested on simulated retail networks.
Patel et al. 2025 [9]	AI continuous user authentication and MFA	Reduced insider threats. Improved authentication accuracy.	Did not secure CCTV or smart sensors. Small enterprise dataset.
Lee et al. 2025 [10]	AI-powered SOC to detect threats in real time	Improved response times. Automated mitigation.	Not designed for malls. High computing power required.
Singh et al. 2025 [11]	AI-assisted Zero Trust framework in smart cities	Improved access control and continuous monitoring.	No focus on use cases for malls. Limited real-world use.
Wang et al. 2024 [7]	ML models to detect payment fraud and customer behaviour	Detected fraudulent payments and suspicious activity.	No Zero Trust. Limited real-world testing.
Verma et al. 2024 [6]	Threat analysis of IoT, cloud, payment and CCTV in retail	Identified key vulnerabilities in smart mall infrastructure.	Conceptual. No AI or Zero Trust framework suggested.
Khan et al. 2024 [3]	Identity verification, authentication and micro-segmentation for IoT smart buildings	Improved IoT security. Reduced attack surface.	No AI behavioural analytics. Focused on IoT.

V. Research Gaps

A. Contextual Risk Scoring

There is no clear risk model. We need to be able to combine the risk signals across different sub systems. For example if a health check fails, login location is unusual, multiple payments are denied and camera traffic is spiking. We need to be able to normalise the signals and understand how critical the assets are and how they will affect the access. The score needs to be understandable and depend on what impact it may cause.

B. Operational Resilience

Carrying out a certain security action may have a negative impact. If we cause issues with the checkout, emergency communication, access control and/or cameras due to high false positives. If there was a high number of false positives this could cause alert fatigue. Within our research we need to ensure we have

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

some way of balancing detection and resilience. We could automatically contain high confidence malicious actions but for ambiguous events in critical services we want to limit the actions so they can be validated by a human.

C. Privacy

There could be privacy and governance concerns as behavioural analytics may involve login details, device ID, location, transaction metadata and interactions. We would need to ensure we have a legitimate reason to collect each data point within the mall. We want to limit how long we keep data for, ensure the logs are secure and ensure we aren't using security monitoring for non relevant customer profiling. We would also like to limit access to sensitive telemetry. We would need to design our system to ensure we are carrying out privacy preserving analytics and keeping data to a minimum.

After some research into the literature I found there were 6 gaps:

1. No overall security. Most research was looking into using AI for threat detection and zero trust. Very little research was done into both areas to secure the smart shopping mall.

2. Not specific to shopping malls. Many solutions look into securing enterprise networks and the cloud.

3. Not overall. Most research focused on securing one aspect (IoT, CCTV, Payment).

4. No real time automation. Many had no automation, real time monitoring or risk assessment.

5. No focus on insider threats. None looked into detecting malicious and compromised employees/vendors using behavioural AI.

6. No scalable real world solution. We need a solution which can be provided at a low cost to help secure the cloud, public Wi-Fi, smart security, IoT and customer data

VI. Proposed Framework

A. Logical Architecture & Trust Boundaries

This separation of policy enforcement and analytics means policy enforcement can be applied to key trust boundaries like Identity Aware Application Gateways, Network Access Controls, Device Gateways, Cloud Access Brokers etc. The policy decision service will use the identity, device health status, resource requested, zones & risk factors. The analytics service will consume the approved telemetry data to generate alerts/risk factors. The security operations workflow will allow investigation of the alerts. This ensures there is no direct control over resources by the AI model. The mall can easily swap out/upgrade detection components without having to reconfigure all the access controls.

B. Trust Boundaries

The architecture should identify trust boundaries between the services. This includes the public facing services, tenants, mall administration, payments, physical security, building, and cloud services. Each of these services will have different availability & confidentiality requirements. Guest Wi-Fi is deliberately accessible by unknown parties, Building systems may control lighting, lifts & environment. Payment & customer information needs a high level of confidentiality & auditing. The policies should ensure that no

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

access can be given freely from a low trust boundary to a high trust boundary. If any integration is required, this should be done via a documented API, with limited credentials, limited network paths & monitored activity.

C. Data Quality & Explaining Decisions

To ensure risks are being made correctly, input data should be accurate & up to date. If timestamps are incorrect, it can cause events to appear not related. Multiple or missing logs can cause inaccurate anomaly scoring. Asset names should be mapped within all identity, endpoint, network & application systems. Evidence should be retained and an explanation provided as to why a risk was made. This can be an unknown destination, unhealthy device & prohibited network path. This should clearly identify if the risk was a policy breach or a probability based alert. This will help analysts investigate & improve documentation. It also reduces the chances of operators trusting the model too much.

D. Exceptions & Break Glass Access

Exceptions are required in the operating environment. However, if these are not managed they can become a security weakness. Each exception should be documented with who owns it, business reason, assets affected, compensating controls, expiry date & review date. Break glass access should be done via unique identities, stronger authentication & detailed logging. If immediate access is required to save a life or keep vital services running, the system may allow a controlled break glass process which should be reviewed promptly. The aim is not to remove all exceptions but to make them clear & have control. The policy engine should raise an alert if an exception is used outside of the intended use or after the approved expiry date.

E. Identity Management, Asset Inventory & Policy Ownership

Identity management should be in place for employees, contractors, tenants, service providers, administrators & machine identities. Each identity should have an owner, role, resources they are allowed to access & expiry/review date. Vendor identities should be temporary & only have access to the systems required to complete their contract. Machine identities should be linked to an inventory with details of what type of device it is, location, team owning, expected communication & if it is maintained. Accurate ownership & inventory management will ensure the policy engine is applying rules to the correct asset. Policy ownership should be assigned to the operating teams. Security teams should own common standards, exception reviews & audits.

F. Network Segmentation & Least Privilege

Network segmentation should be based on the least amount of communication required. For example payment terminals may only be allowed to communicate with approved payment services & not initiate communication with camera management. CCTV devices should only be allowed to communicate with the recording server & management interface but not tenants POS. Guest Wi-Fi should be isolated from internal applications. Tenants should be isolated based on contractual & operational boundaries. Where possible rules should be set to deny by default. Exceptions should be documented & reviewed. This should not replace identity verification but reduce the impact of a compromised account/device.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

G. Model Lifecycle & Drift

AI models will be impacted by changes in business patterns, seasonal traffic, new stores, device replacement & software updates. If a model is trained during a quiet period, it may raise alerts for legitimate activity during a festival or large sale. Model management should include documented data sources, version control, pre-deployment validation, drift monitoring & rollback. Analyst feedback can be used to improve labelling. However, this shouldn't be done in such a way that every alert that isn't raised is assumed to be incorrect & every alert that is raised is assumed to represent all future attacks. Models should be tested with known attack scenarios & normal high volume mall traffic.

H. Incident Handling

The detection platform will only be useful if the alerts are linked to clear processes. The security operations team should determine the severity levels, escalation, evidence retention & remediation. Playbooks could be used to remove session tokens, require step up authentication, block destination, isolate non critical devices or raise an incident. Before automating any actions, consider how it will impact the business. Isolating a camera in a public area could impact safety monitoring. In this case it may be appropriate to put it into a restricted mode or require manual approval. Once contained, the team should verify the integrity of the device, change credentials on the affected devices, return to an approved configuration & document the incident.

I. End to End Request Process

When a user/device requests a resource, the principal is identified & credentials verified. The device is identified & health checked. This includes checking the validity of the certificate, patch/firmware status if available & if it is part of an approved inventory. The policy engine will check what resource is being requested, role of the user, current network zone, time/location context & recent risk factors. A decision will be made based on the evidence. This can allow, block or challenge with stronger authentication. This will be logged.

J. Risk Based Decision

The framework should be risk based. If the risk is low & the device is a healthy managed device, the request can be allowed with normal controls. If the risk is medium, step up authentication, short lived sessions & restricted access can be applied. If there is a high risk, it can be blocked & escalated to security operations. The thresholds should be set for each asset type. Guest Wi-Fi will have a different acceptable risk than payments or systems supporting safety. Actions should be able to be reversed & logged.

K. Data & Telemetry

The telemetry data could include events from identity providers, endpoint/device health, firewall & network flow, application logs, payment alerts & security camera management. Only collect the data required for the security purpose. The data will be normalised, duplicate events removed & asset criticality & zone added. AI models can be used to analyse patterns. If there are limitations with connectivity/latency, light detection can be used at the edge. This will raise higher level alerts.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

L. Implementation

A practical implementation would start with asset discovery & network mapping. The first pilot should be a small section which poses a lower risk. This could be staff having access to certain admin applications. The next phase would be adding device identification & segmentation. This could be cameras & sensors. Payment alerts, cloud & log correlation can be added in the third phase. Once the detection models & remediation have been tested, high impact containment actions can be automated. This will reduce disruption & each phase can be compared to a documented baseline.

M. Example Threat

If a camera starts communicating with an unknown external address & tries to connect to a staff subnet. Device health checks show the firmware is out of date & network monitoring shows new communication. The AI layer raises the risk. The policy engine doesn't just rely on the AI model. The device identity, destination, zone & asset role all show it shouldn't be accessing this. The system can block the connection, isolate the camera into a restricted zone, retain the relevant logs & alert the security team. This is an example of how it would work & is not a measured experiment.

A multi layered zero trust framework incorporating AI has been designed to overcome these issues.

1) Identity Layer – Multi factor authentication & Identity Access Management. This includes Continuous Authentication using behavioural biometrics. Users will be asked to complete MFA if the confidence levels drop [9].

2) Device Layer – Cryptographic identities on all IoT devices (CCTV, sensors & payment terminals). Health checks will be completed [3].

3) Network Layer – Payment systems, CCTV, public Wi-Fi, staff & stores will be micro segmented. This means if an IoT device becomes compromised, it won't impact other devices [3] [11].

4) AI Analytics Layer – The behavioural profiles & anomaly scores are sent to the central policy engine. Payment fraud models are used [7] [8].

5) Security Operations Layer – The logs are correlated using the SIEM pipeline. An AI based Security Operations Centre will be used. This will include automated playbooks to isolate hosts/tokens [10].

All requests will pass through the identity, device & network layers. The AI layer will give a risk score & the policy engine will decide to allow, challenge or block. Any suspicious behaviour will be passed to the SOC. All information will be logged. Light AI models can be used at the edge to help reduce costs & latency [1] [7].

VII. Applications, Benefits and Challenges

A. Governance

A small cross functional team should be responsible for deploying the solution. The team should contain key stakeholders within cybersecurity, IT infrastructure, physical security, mall management, privacy and vendors. The team will be responsible for deciding on asset categorisation, risk levels, playbooks, data

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

retention and emergency policies. The team will decide what can be automated. This is important as the technical controls may affect customer experience. For example, the security team may want to automatically isolate but the operations may want to keep the camera/terminal online. Having a set criteria for decision making will remove any confusion when incidents occur.

B. Prototype Elements

For the proof of concept the solution could be built using the following components; Identity Provider (to authenticate users), Certificate/Inventory Service (device identities), Network Segmentation, Central Event Pipeline, Policy Engine. Anomaly detection could be achieved through basic statistical analysis. The security operations dashboard should have a view on the event timeline, asset owner, resource requested, policy outcome, risk signal and recommended action, allowing the solution to be tested individually. The prototype should use synthetic or authorised data. Customer data shouldn't be used unless absolutely necessary and must follow the approved process.

C. Testing

Obtain a baseline, this will show how many requests, traffic and device communication would be seen. Set some controlled attack scenarios, this could include brute force attacks, devices communicating to unauthorized endpoints or requesting resources outside of their role. Check that the solution correctly identifies the event, applies the correct policy and provides an audit trail. Create some benign scenarios, this will allow you to see how many false positives would occur, examples include shift changes, maintenance periods and peak times. Lastly measure how much impact the solution has on operations. How quickly decisions were made, the overhead, analyst effort and if any legitimate resources were impacted. After any changes to the model/policy repeat the tests to see if improvements have been made.the model/policy repeat the tests to see if improvements have been made.

D. Reporting

When reporting on any test results, ensure to describe the environment, data source, number of scenarios, training/test data split, model setup, policy thresholds and metric definitions. Where possible break the information down into the key sub sections. This will highlight if the solution isn't picking up any low frequency high impact events. Include the false positives and missed detections. If the solution was only tested in a lab environments this should be mentioned.

E. Ownership

There are usually many people involved with a smart mall, including mall management, security operations, IT admin, tenanted stores, payment providers, facilities management and cloud vendors. In the security architecture ensure you know who has ownership of approving access to resources, maintaining different devices, receiving alerts and isolating systems. If third party equipment is used ensure it is clear who is responsible. This should be outlined in contracts and processes. This will ensure logs are available, alerts are raised, patching timeframes are known, access is reviewed and evidence is handled.

F. Deployment

Consider the bandwidth, storage, availability, legacy and resources required. A lot of telemetry could increase the storage and processing costs. Too much centralization could create a single point of failure.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Consider using a hybrid approach with real time local processing and aggregated events pushed to the analytics. Consider how the system will function when offline. Critical services may have strict policies to allow fall back. Try to ensure the system isn't too open or closed. Limit the fall back period.

G. Security & Audit

Before going live perform some threat modelling, config checks, penetration testing and walkthroughs. Test to understand if the identities can be reused in different zones, devices can communicate to unauthorised endpoints when compromised, logs can be changed and emergency access is controlled. Ensure the policy engine is very secure, this can be achieved by using strong authentication, least privilege, back-up and approvals for changes. Include information on the context of the request, decision, policy version, risk signals and any automated actions. This will help analysts understand why access was granted/rejected and allow them to investigate further.

H. Risks

If the telemetry is incomplete, the labelling is unreliable or attackers are trying to mimic legitimate users then the framework may not work well. There is a risk that there will be adversarial attacks, sensor compromise and training data poisoning. Ensure a layered defence is used. Use AI to provide evidence but still have checks in place for the identities, cryptography, network segmentation and deterministic rules. Don't make the deployment look like because it scores high it must have been attributable to the incident. Ensure analysts can easily understand what they're seeing, what the model is working out and what has been discovered.

I. Metrics

In the future when creating a prototype, test the solution with a defined dataset. Try using some controlled scenarios. Metrics could include precision, recall, false positive rate, detection time, containment time, authentication challenge rate, policy decision time and service availability. Detection should be broken down into payment systems, IoT devices, staff identities and guest networks. This is due to the distribution and cost of errors. Record computational overhead.

J. Baseline & Scenarios

Compare with a traditional solution, zero trust without AI risk scoring and AI detection without policy enforcement. Scenarios could include credential theft, anomalous account activity, camera compromise, multiple payment anomalies, lateral movement and suspicious cloud API request. All scenarios should include benign events to ensure the solution can identify legitimate exceptions. No performance stats claimed as this is future work.

K. Integration

This could be one of the main issues. A mall may have legacy cameras, POS systems, tenanted networks, 3rd party parking and multiple vendors to manage the cloud applications. Some devices may not be compatible with modern agents or strong cryptographic methods. Workarounds may be required such as network gateway, passive monitoring, limited zones and documented exceptions. The assets, certificates, policies and detection models will need to be maintained. As stores, devices and user roles change.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

L. Benefits & Trade offs

Having more visibility, less lateral movement opportunities, more contextual decisions and faster incident response. Depends on the quality of assets, events, policies and staff processes. The analytics could add some cost and delay to the system. Edge processing can be complicated. Policies could be too restrictive, causing disruption to genuine business or too lax so the security benefits aren't seen. It is important to have continuous monitoring and regularly review policies. This design could easily be applied to retail chains, airports, hospitals, smart buildings and smart city infrastructure. Benefits include continuous verification, fewer side attacks, faster response and real time fraud detection. However there are a few issues.

It will add cost, need skilled security staff and continual monitoring. Need to integrate with existing infrastructure. A lot of logs will be required [10], which will require a lot of processing power. Real world data wasn't tested in the studies [8] [9].

VIII. Conclusion and Future Work

A. Future Work

The future work should include developing a prototype and setting up a controlled environment which should simulate a smart mall. This should include real users, IoT devices, network segments, payment activity and a central log. An algorithm should be developed to provide explainable risk scores and privacy preserving analytics. Federated Learning and light-weight AI models should also be investigated to use in situations where data cannot be stored in a central location. The research should report on how secure the system is and its impact on operations (false positives, response times and service interruptions).

B. Limitations

This paper provides a framework using a targeted literature review. An actual system was not created meaning there is no original dataset, benchmarks or quantitative data. The papers used vary between different scenarios and methods. This means results cannot be generalised to all shopping malls. This paper provides a framework which must be implemented, reviewed by stakeholders and tested in a realistic environment.

Whilst AI and Zero Trust increases cybersecurity through continuous monitoring, threat detection and access control. Only one aspect of the framework was looked at within the studies and few looked at how they can work together. Smart malls can face issues with payment fraud, ransomware, phishing attacks, insider threats, vulnerabilities and unauthorised access. It seems an integrated approach is needed.

The framework will be expanded upon and will be tested across different aspects including payments, IoT, CCTV, cloud, public Wi-Fi and customer data. Future work could look into creating an AI powered autonomous Security Operations Centre, privacy preserving AI, light weight AI models, digital twin security and quantum resistant Zero Trust Architecture [1][7].

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

References

[1] S. M. Nagarajan, G. G. Deverajan, S. T. M., T. V. Ramana, A. K. Bashir, and A. A. Alzubi, "Artificial intelligence based Zero Trust security approach for consumer industry," *IEEE Trans. Consum. Electron.*, vol. 70, no. 3, pp. 5411–5418, 2024.

[2] M. Hussain, S. Pal, Z. Jadidi, E. Foo, and S. Kanhere, "Federated Zero Trust architecture using artificial intelligence," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 30–35, Apr. 2024.

[3] S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt, and M. Gupta, "ZTA-IoT: A novel architecture for Zero-Trust in IoT systems and an ensuing usage control model," *ACM Trans. Privacy Secur.*, vol. 27, no. 3, 2024.

[4] "Zero-trust architecture for securing Internet of Things (IoT) networks: A review," in *Proc. 5th Int. Conf. Commun., Inf., Electron. Energy Syst. (CIEES)*, IEEE, 2024.

[5] "Blending shared responsibility and Zero Trust to secure the industrial Internet of Things," *IEEE Secur. Privacy*, vol. 22, no. 5, Sept.–Oct. 2024.

[6] "Verify and trust: A multidimensional survey of Zero-Trust security in the age of IoT," *Internet of Things*, vol. 27, Art. no. 101227, Elsevier, 2024.

[7] W. Wang, P. Zhang, C. Sun, et al., "Smart customer service in unmanned retail store enhanced by large language model," *Sci. Rep.*, vol. 14, 2024.

[8] A. Sharma, P. Rao, and N. Iyer, "AI-based anomaly detection with Zero Trust authentication for retail environments," *Int. J. Comput. Appl. Retail Secur.*, vol. 12, no. 1, pp. 22–31, 2025.

[9] R. Patel, S. Joshi, and A. Menon, "Continuous user authentication using AI and multi-factor authentication," *J. Cybersecurity Identity Manage.*, vol. 9, no. 2, pp. 45–58, 2025.

[10] J. Lee, H. Kim, and D. Park, "AI-powered security operations center for real-time cyberattack detection," *IEEE Access*, vol. 13, pp. 11023–11035, 2025.

[11] K. Singh, R. Gupta, and M. Chawla, "AI-assisted Zero Trust framework for smart city infrastructure," *Smart Cities J.*, vol. 8, no. 1, pp. 77–90, 2025.