Temporal Blindness in AI-Secured IoT Systems: Missed Multi-Stage Attacks in Cloud-Centric Detection Pipelines

Parth Talaviya[1], Manya Parikh2, Deep Solanki3, and Jigar Gajjar4

LokJagruti Kendra University, Ahmedabad, India[1]
LokJagruti Kendra University, Ahmedabad, India[2]
TechDCybersecurity Limited, Ahmedabad, India[3]
TechDCybersecurity Limited, Ahmedabad, India[4]

talaviyaparth604@gmail.com[1], manyaparikh23@gmail.com[2],deepsolanki5799@gmail.com[3], cyberian.jg@gmail.com[4]

Abstract: The increase in the use of Internet of Things (IoT) technology has brought forth new possibilities for connectivity, but it has also brought forth the possibility of complex cyber threats. To counter these threats, there has been a growing need for the implementation of Artificial Intelligence (AI) security systems that possess the capability to process large amounts of data, identify anomalies, and implement automated response systems. Although these systems have brought forth greater efficiency and enhanced the capabilities of security systems, recent studies have also indicated that these systems may bring forth new threats. Temporal blindness, which refers to the inability of detection algorithms to identify low-intensity events over a period of time, is one such threat.This paper discusses how cloud-based detection systems, despite their efficiency and processing capabilities, may inadvertently bring forth the fragmentation of security telemetry data. This may result in complex multi-step attacks that change over a period of time going undetected until considerable damage has been caused. Through a critical analysis of existing literature and an analysis of the current scenario, this paper discusses the importance of implementing temporal correlation functions along with real-time analytics to enhance situational awareness. Finally, this paper concludes that there is a growing need to integrate intelligent systems with human intelligence to develop effective AI-secured IoT networks that can counter complex cybersecurity threats.

Keywords: Blindness, AI, IOT System, Cloud, Attacks, Detection Pipelines, Temporal

---

I. INTRODUCTION

AI-based IoT solutions are at the forefront of innovation, integrating intelligent analytics with a network of interconnected devices to enhance how we can monitor and protect processes. The Internet of Things is a massive network of physical devices, sensors, software, and communication equipment that keeps data flowing in the virtual world. As we increasingly depend on smart devices, cloud computing, and autonomous systems, these networks are the foundation of the modern enterprise, and cybersecurity is at the top of the list of priorities. As Atzori points out, the rise of the number of connected devices has both magnified and complicated the issue of IoT security. This is why AI-based security solutions are in such high demand – to detect anomalies, protect against attacks, and facilitate proactive defense.

Artificial intelligence is changing the way we protect our IoT networks. AI-powered threat detection and quick response enable security experts to dig through a huge amount of data to identify anything unusual. Ferrag explains that AI-powered security solutions improve situational awareness by constantly monitoring network traffic and pointing out possible threats in a complex environment. However, as new threats emerge, new difficulties arise. Today's threats may involve several steps, meaning that detecting them by responding to an alert may be like trying to catch a shadow. This is known as temporal blindness.

http://doi.org/10.63766/spujstmr.26.000084

A. Artificial Intelligence and Internet of Things

Consequently, Artificial Intelligence (AI) refers to computer systems designed for tasks requiring smarts, such as learning, thinking, recognizing patterns, and making decisions. Put differently, AI is creating smart agents that can read what the world looks like and act accordingly to achieve some set goals, as described by Russell and Norvig. IoT, on the contrary, is an alternative concept that refers to a world of physical objects, where each object is equipped with sensors and communication technologies, connected such that information is exchanged constantly. In such contexts, Atzori and his team refer to it as an IoT concept, where ordinary objects are connected to act as smart players in dynamic digital worlds.

The combination of AI and Internet of Things technology has significantly improved the way organizations process massive amounts of data from sensors and automate daily tasks. You will notice the presence of these technologies in all areas, ranging from intelligent healthcare and intelligent transport systems to automated factories and smart city management. Gubbi et al. observe that the integration of smart analytics into IoT systems enables data to be converted into useful insights, which refines the decision-making process. However, the increased number of connected devices also increases the challenges associated with their management and the threat of cyber attacks.

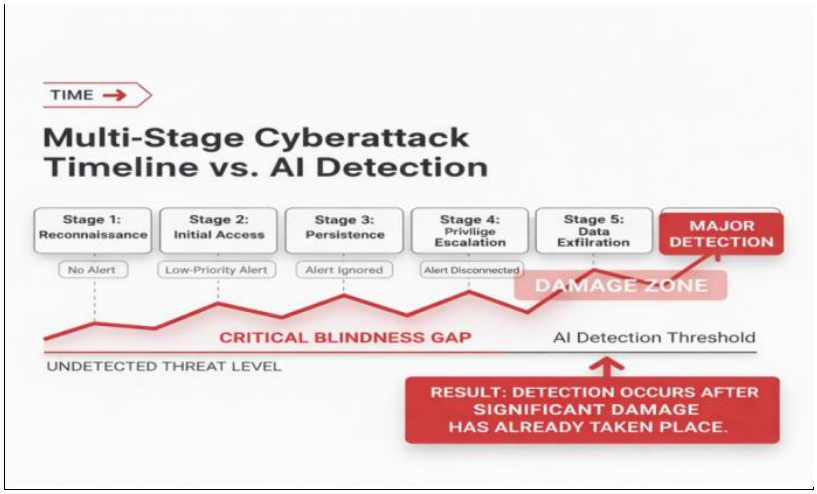

Fig. 1. Multi-Stage Cyberattack Timeline vs AI Detection

B. Integration of Artificial Intelligence within IoT and Cloud Ecosystems

The combination of Artificial Intelligence and Internet of Things is dependent mainly on cloud-supported infrastructure, which provides scalability in terms of storage and processing power. The IoT devices generate massive amounts of data in real time, which is transmitted to a central location where machine learning algorithms are used to analyze the data and identify patterns and anomalies. According to Botta et al. [7], cloud computing provides the flexibility and processing power required to support the growing requirements of interconnected systems.

This design is capable of handling various applications such as predictive maintenance, remote health monitoring, intelligent surveillance, and automated industrial control. According to Jordan and Mitchell [8], machine learning increases the adaptability of the system since it can learn from past experiences and adjust its responses accordingly. Moreover, cloud-oriented frameworks enhance the ability of distributed systems to interact with each other, and this makes it possible to perform real-time analytics on geographically distributed networks. Nevertheless, the use of centralized processing may result in latency and visibility issues when analyzing security incidents, particularly when threats evolve slowly with time.

C. Benefits of AI-Based IoT Systems

The use of AI-based IoT networks increases the efficiency of business operations through intelligent data analysis. The networks enable real-time data analysis, which helps organizations quickly react to environmental changes by analyzing data from sensors. Gubbi et al. [6] observe that intelligent data analysis enhances decision-making by reducing large amounts of raw

data into useful information. The ability to work alone is a great advantage because machine learning algorithms are capable of performing repetitive tasks without anyone observing them. Autonomy is very important in areas such as industrial automation, smart healthcare, and transport systems because decisions made at the right time can make all the difference. Jordan and Mitchell [8] observe that learning algorithms are more flexible as they get more data and make better predictions.

Further, the AI-driven IoT configuration scales loudly, allowing the network to expand without pulling down the performance. Enhanced situational awareness enhances the resilience of the organization by providing a complete view of the system's behavior (Ferrag et al. [9]). Despite the advantages, the increasing reliance on automated intelligence highlights the importance of effective security monitoring.

D. Security Challenges in AI-Driven IoT Systems

There are definite benefits to the technical abilities of AI-based IoT networks, but there are also definite security concerns. The more devices that are networked, the larger the attack surface, and it is expanding aggressively, providing attackers with more points of entry (Atzori et al. [5]). IoT devices are often limited in their processing abilities, making the implementation of robust security measures problematic. The problem is further exacerbated by adversarial machine learning. Attackers can manipulate the training data or provide misleading input that can evade detection systems, which can work against security rather than for it. Biggio and Roli [11] describe how these methods can expose fundamental vulnerabilities in machine learning. And if the sensor data is itself vulnerable to attacks, then the reliability of automated decision-making is in question.

The privacy issue becomes more pressing when large volumes of confidential information are being transmitted through distributed networks. Buczak and Guven [10] observe that the lack of adequate protection can increase the risk of unauthorized access and data breaches. Moreover, the AI systems themselves can become vulnerable to attacks, with hackers using the vulnerabilities of the algorithms to evade detection systems. The distributed attack methods further complicate the situation, particularly in the case of large-scale networks where the attack sources can be multiple at the same time. Ferrag et al. [9] explain that the ability to identify the coordinated patterns of intrusion in such networks is a sophisticated task.

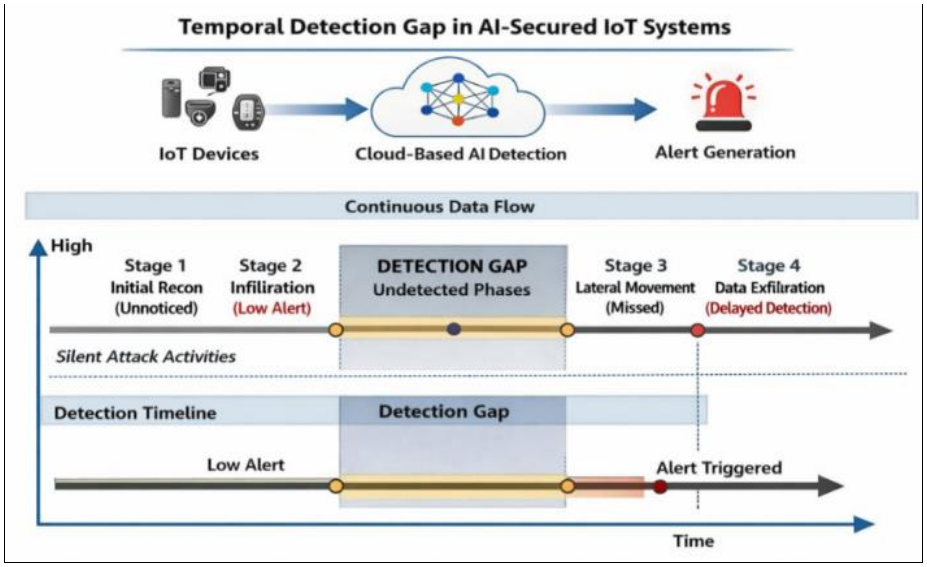

Fig.2. Temporal Detection Gap in AI-Secured IoT Systems

E. Temporal Blindness in AI-Secured IoT Systems

Definition of Temporal Blindness (TB):
TB represents an inability of the AI threat detection system to properly correlate several weakly related security events happening at various time intervals into one coherent attack pattern. In the case of IoT ecosystems protected by AI-powered security monitoring solutions, the detection process is designed to spot only imminent anomalies or high-severity incidents.

However, professional hackers usually organize their attacks so that each individual event does not exceed pre-set detection limits.

It means that independent and unrelated events happen one after another and do not correlate from the perspective of their timing, thus making it impossible for the detection system to analyze the full lifecycle of the attack. Therefore, adversaries can perform reconnaissance, privilege escalation, lateral movement, persistence creation, and data exfiltration without any problems during a prolonged period.

The formula for this phenomenon is defined as:

$$TB = 1 – (CE / TAE)$$

Where:

TB = Score for Temporal Blindness
CE = Correctly Correlated Events
TAE = Total Attack Events

The closer the score for temporal blindness is to 1, the less temporal awareness the person has, whereas the score for temporal blindness that is close to 0 signifies successful event correlation and attack reconstruction.

In cloud-based detection models, this problem turns out to be even more complicated because of the geographical distribution of the devices producing telemetry data.
Cloud-based detection pipelines are capable of processing massive amounts of data, but they can also exacerbate the lack of context when the telemetry data is fragmented, disrupting the continuity that investigators need. According to Divakaran et al. [12], poor correlation of events can hinder the discovery of coordinated intrusion actions. Similarly, Liyanage et al. [13] argue that maintaining situational awareness in distributed infrastructures remains a lingering challenge for AI-based security systems.
With the increasing elusiveness of cyber threats, attackers make use of time gaps, striking with slow and silent movements that evade conventional defenses. Biggio and Roli observe that “shifting attacker strategies require security models that are able to identify patterns in time, rather than reacting to anomalies in real time.” Overcoming temporal blindness is therefore essential to improving AI-based IoT security against such sophisticated attack methods.

TABLE I

CAUSES AND SECURITY IMPLICATIONS OF TEMPORAL BLINDNESS

Cause	Description	Security Impact
Isolated Event Analysis	Alerts reviewed independently	Attack progression overlooked
Short Detection Windows	Focus on immediate anomalies	Slow attacks remain hidden
Cloud Data Fragmentation	Distributed telemetry	Loss of contextual continuity
Limited Temporal Correlation	Weak event linking	Multi-stage attacks succeed
Overreliance on Automation	Reduced human review	Strategic threats ignored

The convergence of Artificial Intelligence and Internet of Things networks has completely changed the way we perceive cybersecurity in the present day. AI technology makes it possible to monitor in an automated fashion, perform analytics in real-time, and develop adaptive threat detection, which increases situational awareness and allows for the response to threats as they happen. However, as we increasingly rely on AI-based detectors, there is a concern that certain threats may be able to evade them over time. This concern is commonly referred to as “temporal blindness,” implying that a crafty hacker could evade detection with small and low-intensity attacks that fly under the radar. In reality, however, the actual power of AI-based IoT security lies in its capacity to connect the dots over time in a cloud-based environment.

Metrics for Measuring Temporal Blindness

In order to properly evaluate and measure temporal blindness, some metrics should be considered. The metrics will help determine the effectiveness of the event correlation by using AI algorithms.

TABLE II

TEMPORAL BLINDNESS MEASUREMENT METRICS

Metric	Description	Desired Value
Event Correlation Rate (ECR)	Percentage of related events correctly linked	High
Detection Delay (DD)	Time between attack initiation and detection	Low
Attack Reconstruction Accuracy (ARA)	Ability to reconstruct attack sequence	High
Temporal Blindness Score (TBS)	Degree of missed temporal relationships	Low
Context Preservation Ratio (CPR)	Amount of contextual information retained	High

These metrics provide a structured framework for evaluating temporal awareness within AI-secured IoT environments and enable objective comparison between traditional and proposed detection approaches.

II. LITERATURE SURVEY

A. Evolution of IoT Security and Threat Detection Mechanisms

The fast evolution of Internet of Things (IoT) technology has greatly impacted the modern digital age, but it has also brought about a new challenge concerning security threats. In the early stages of the evolution of IoT technology, the primary concern was to incorporate fundamental security measures such as password protection and network firewalls, which were not adequate enough to cope with the complexity of IoT technology. As the number of IoT systems continues to rise, the conventional signature-based detection systems proved to be less effective in dealing with the dynamic nature of cyber threats. Researchers such as Atzori et al. [1] highlighted that the heterogeneity of IoT devices has resulted in vulnerabilities that cannot be standardized. Over the years, approaches for threat detection have evolved from signature-based detection systems to behavior-based detection systems, which allow systems to detect anomalies instead of attack signatures. Sicari et al. [2] clarified that this development marked a major milestone in the development of adaptive security models. However, the dynamic and distributed nature of IoT technology still remains a challenge in the implementation of detection systems.

B. Adoption of Artificial Intelligence in IoT Threat Detection

The complexity of cyber attacks has also resulted in the use of Artificial Intelligence as a way of improving the security of IoT networks. Conventional methods of monitoring have not been able to handle the volume of data produced by IoT networks. This makes it inefficient and impossible to manually analyze the data. AI models have been able to handle this problem by allowing for the automated recognition and analysis of anomalies in large volumes of data. Machine learning models have been able to show the capability to detect even the slightest anomalies in network traffic patterns that may potentially pose a threat to security.

According to Buczak and Guven [3], data mining techniques improve the efficiency of intrusion detection by identifying relationships that would not have been identified in high-volume traffic. Similarly, Jordan and Mitchell [4] explain that machine learning is a revolutionary technique that enables systems to learn from experience and improve their predictive accuracy over time. Deep learning models have further improved these techniques by improving the accuracy of detection in complex

scenarios (Goodfellow et al. [5]). In addition to detection, AI has also been used in the development of proactive defense systems that employ predictive analytics. Ferrag et al. [6] explain that intelligent security systems have the capability to predict attack patterns, giving organizations the opportunity to prepare in advance before any major damage is done. This is a major improvement from conventional security systems that were purely reactive.

However, it is also important to note that AI is not a magic solution, according to Sommer and Paxson [7]. They said that machine learning algorithms have to be calibrated to avoid misclassification and inefficiency. Moreover, the success of these algorithms largely depends on the quality of the training data and the context in which they are used. Despite the aforementioned facts, the integration of AI technology in the field of IoT security has resulted in a paradigm shift in the detection of threats. With the increasing development of connected spaces, AI-based monitoring systems are becoming increasingly important in this context.

C. Role of Cloud-Centric Detection Pipelines in AI-Secured IoT Architectures

Cloud computing has been identified as a critical component of AI-secured IoT networks, particularly due to its processing and storage capabilities to process a large amount of data produced by IoT devices. Instead of processing the data on local systems, most modern detection systems are intended to harvest data from IoT devices on cloud platforms, where complex processing can be performed. As Botta et al. [8] stated, this synergy makes it possible to perform scalable processing and real-time security analysis. Cloud computing systems make it possible to continuously monitor data by aggregating data from multiple endpoints and analyzing it using sophisticated detection engines. This makes it possible for security analysts to evaluate network activity in a more holistic way than would be possible on local systems. Chen et al. [9] stated that cloud-scale analytics platforms are extremely capable of taking raw data and maturing it into actionable intelligence.

There are also limitations to cloud computing systems. Data from geographically dispersed devices may lack temporal consistency, and it may be difficult to determine the order of security events. Liyanage et al. [10] stated that it is difficult to maintain contextual awareness in distributed systems, particularly in AI-secured IoT networks. Another possible challenge that may arise is latency, which may impact the speed of threat detection. While cloud pipelines enhance the effectiveness of computation, they may also create a situation where an isolated signal is evaluated independently rather than as part of a larger attack.

In this context, cloud-based detection not only marks an advancement in technology but also marks a paradigm shift that reshapes the way security intelligence is evaluated in an IoT environment.

D. Comparison Table: Traditional vs AI-Driven Cloud-Based Detection

TABLE III

COMPARISON TABLE: TRADITIONAL VS AI-DRIVEN CLOUD-BASED DETECTION

Aspect	Traditional Detection	AI-Driven Cloud Detection
Detection Style	Signature-based	Behavior-based
Processing Location	Local systems	Centralized cloud platforms
Scalability	Limited	Highly scalable
Threat Recognition	Reactive	Predictive
Data Handling	Manual filtering	Automated analytics

E. Multi-Stage Attacks in IoT Environments

Cyber attacks on IoT networks have also transcended the level of single-point entry attacks and have now reached the level of multi-stage attacks, which have the objective of remaining undetected for a longer period of time. Such types of cyber attacks include the reconnaissance phase, whereby the attackers are able to determine the network topologies and vulnerabilities. Mirkovic and Reiher [11] emphasize the fact that distributed networks are highly susceptible to coordinated attacks due to the

attack surface. Advanced Persistent Threats (APTs) are a good example of such attacks, whereby stealth and long-term network infiltration are utilized.

The first aspect of multi-stage attacks is their stealth. This means that the attack does not immediately trigger any red alerts but involves low-intensity operations that, when viewed individually, are operationally unimportant. Research carried out by Behl and Behl [12] suggests that in order to detect such attacks, it is not enough to detect anomalies but to have the ability to correlate events over time. Otherwise, security systems may only be able to detect the final stage of an attack.

With the ever-increasing size of IoT networks, it is becoming imperative to understand the mechanics of multi-stage attacks. The success of such attacks is less dependent on their technological sophistication and more on their ability to produce gaps in the continuity of detection.

F. Real-World Incidents Demonstrating Missed Multi-Stage Attacks

Cyber events in the real world demonstrate how multi-stage attacks can occur undetected until substantial harm has been caused. The Mirai botnet attack is one such event, where IoT devices were systematically exploited to launch large-scale distributed denial-of-service attacks. Kolias et al. [13] describe how the slow spread of the infection among vulnerable devices allowed the attack to spread before adequate defensive action could be taken.

Another example is the SolarWinds attack, where attackers compromised software supply chains and established persistence in the affected networks for months. According to Singer and Friedman [14], the slow discovery of the attack showed how sophisticated attackers could use the limitations of monitoring to remain undetected.

These examples show the relevance of temporal awareness in the field of cybersecurity. If threat indicators are considered in isolation, rather than as part of a larger sequence of events, warning signs of an attack may be missed, allowing attackers to move deeper into affected infrastructures.

TABLE IV

PERCEIVED SECURITY VS ACTUAL DETECTION CAPABILITY IN AI -SECURED IOT

Cause	Description	Security Impact
System Capability	Perceived Protection	Actual Risk
Real-time analytics	Continuous monitoring	Missed long-term patterns
Automated alerts	Rapid response	Alert fatigue
AI anomaly detection	Intelligent security	Weak temporal awareness
Overreliance on Automation	Reduced human review	Strategic threats ignored

G. Temporal Blindness in AI-Based Detection Systems

Temporal blindness refers to the pain point in the startup phase where threat detection systems fail to identify threats that seep in over a period of time.

Divakaran et al. suggest that breaking down alert analysis into manageable morsels can, in fact, cloud situational awareness, particularly in a distributed environment where signals originate from multiple sources. By analyzing each signal in a vacuum, the larger picture of an attack may remain obscured.

Even cloud-supported systems, which enhance analytics, can make the problem worse. Data aggregation is intended to optimize, but it can disrupt the temporal relationship between events. As Liyanage et al. point out, maintaining security telemetry as an uninterrupted, cohesive process is a difficult challenge.

Another problem in the environment is alert fatigue. Security analysts are bombarded with an endless stream of alerts, which increases the chances that we miss or quickly scan over non-critical alerts. Over time, attackers exploit this by distributing malicious activity in ways that fall just beneath the alerting threshold.

Biggio and Roli also observe that attackers are improving at evading intelligent models by behaving in a normal way. This highlights the importance of detection algorithms that understand how behavior changes over time, not just detect anomalies in isolation.

To overcome temporal blindness, there is a paradigm shift required in how we address things. Rather than focusing on real-time classification, future systems will depend on improved correlation engines, adaptive memory, and more sophisticated contextual analysis.

Ultimately, temporal blindness is more than a technical problem—it is an architectural problem. It highlights how contemporary security architectures understand time, behavior, and threat persistence.

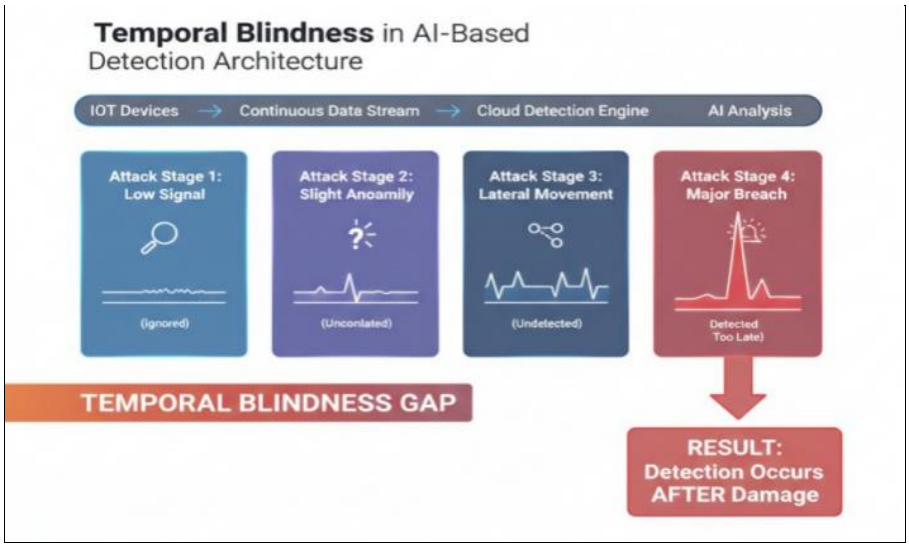

Fig.3. Temporal Blindness in AI-Based Detection Architecture

III. ANALYSIS

The increasing use of Artificial Intelligence in the security context of IoT is expected to bring a paradigm shift in the way we are able to detect and respond to cyber threats. Intelligent detection systems have the capability to scan through huge amounts of data, detect anomalies, and accelerate the time it takes for us to respond. However, this apparently positive trend comes with a major caveat: the lack of awareness about time. Most intelligent systems are built to detect sudden anomalies, which is great for sudden attacks, but most likely to fail in detecting threats that emerge over a period of time.

In cloud-based IoT networks, the security data is typically gathered from sources that are spread out over the network. While the benefits of centralized processing in terms of scalability are well understood, they also lead to the fragmentation of the sequence of events, making it hard to track attacks in terms of a continuous flow. This could lead to the warning signs being treated as nothing more than fluctuations, and not as a sign of a coordinated attack. This state of affairs, which is typically described by the phenomenon of temporal blindness, points to the difficulty of fast detection being leveraged into valuable threat intelligence.

TABLE IV

FACTORS CONTRIBUTING TO TEMPORAL BLINDNESS IN AI-SECURED IOT SYSTEMS

Analytical Dimension	Current AI Capability	Underlying Limitation
Event Processing	Rapid anomaly detection	Focus on isolated alerts
Detection Speed	Real-time monitoring	Short analytical windows
Cloud Aggregation	Scalable data analysis	Fragmented telemetry
Automated Alerts	Efficient threat signaling	Alert saturation

Pattern Recognition	Identifies known behaviors	Weak behavioral linkage

The conflict at the heart of AI-secured IoT architectures is evident: we design systems that are fast and efficient, but in doing so, we may end up rendering ourselves blind to potential dangers that emerge over a longer period of time. While analytics help us quickly notice things, the danger of analytics is that they are biased towards the present and may overlook the process that takes place over a period of time. When telemetry is fragmented and notifications are flooded, it becomes difficult to reconstruct a timeline of what the attacker actually did. The point is not that detection must be perfect but that detection alone is not sufficient.

IV. PROPOSED TEMPORAL-AWARE DETECTION FRAMEWORK

The biggest limitation revealed through the course of this research work is the lack of capability in existing cloud-based security systems of Artificial Intelligence to correlate attack events taking place over a longer period of time. In order to overcome this limitation, a Temporal Awareness Detection Framework (TADF) is suggested. It is designed to increase situational awareness through maintenance of security history and correlated distributed security events to form an attack timeline.

As compared to conventional detection framework which considers attack events independently, the proposed framework utilizes temporal memory, event correlation and temporal risk scoring in order to detect multi-stage attacks.

Following are the main components of the proposed framework:

1. IoT Device Layer
The first layer comprises of IoT devices like sensors, cameras, industrial control devices, intelligent healthcare devices and intelligent transport system devices. They constantly provide data in the form of logs, network traffic, authentication data and behavioral events.

2. Edge Event Collector
Edge Event Collector gathers security-related data from distributed IoT devices and applies preliminary filtering. Unlike conventional frameworks, it retains the context metadata that can be used later for correlation.

3. Temporal Event Buffer
The Temporal Event Buffer acts as the short term and long-term memory store for security events. Events are retained in order to allow longer analysis periods than just the immediate period of event occurrence.
This module retains:

- Event times
- Identifying device information
- User behaviors
- Network communications
- Behavioral attributes

Historical retention of data enhances temporal visibility greatly.

4. Event Correlation Engine
The Event Correlation Engine looks for correlations between events that occur within varying periods of time.
Events are correlated using:

- Same source IP
- Device identity
- Behavior similarity
- Network communication pattern
- Evolution pattern of attacks

The goal is to correlate independent events to form a narrative of an attack.

5. Temporal Risk Scoring Module

The Temporal Risk Scoring Module computes the cumulative risk score based on frequency, event severity and correlation strength of events.
The formula for temporal risk scoring is:
TRS = Σ (Event Severity × Correlation Weight)
Where:

- TRS = Temporal Risk Score
- Event Severity = Risk score of individual events
- Correlation Weight = Relationship degree of events

Higher scores increase the probability of malicious coordination.

6. AI Decision & Alerts Generation Layer
The last layer employs machine learning techniques for analyzing correlated events and generating intelligent alerts.
As opposed to the conventional approach, where alerts are generated through:

- Event history
- Attack progression
- Behavioral evolution
- Accumulation of temporal risks

This helps minimize alert fatigue and increases attack visibility.
With the above architecture, AI-secured IoT systems can go beyond simple anomaly detection towards attack lifecycle detection.

A. Algorithm for Temporal-Aware Threat Detection

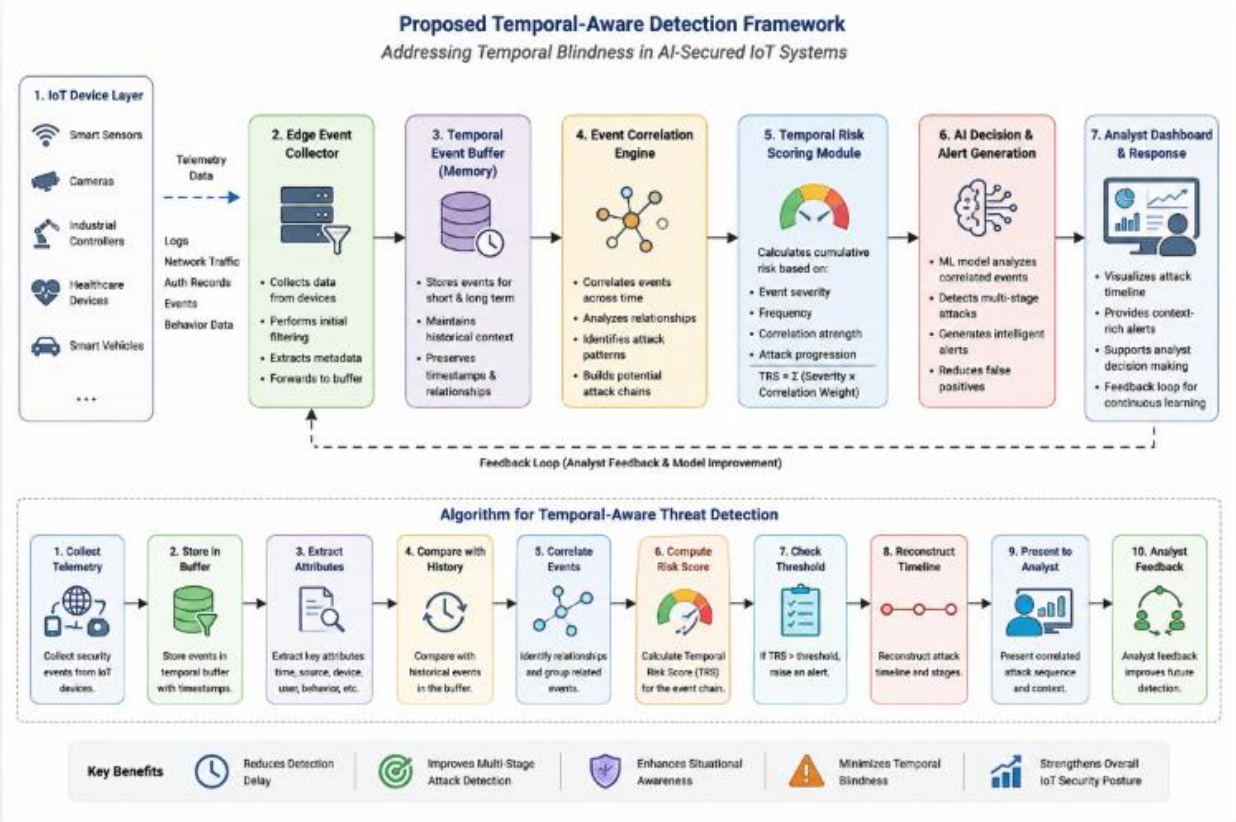

Fig.4. Proposed Temporal-Aware Detection Framework

The framework enhances threat detection in AI-secured IoT systems by combining temporal event storage, event correlation, risk scoring, and AI-based analysis to identify multi-stage attacks and reduce temporal blindness in cloud-centric detection pipelines

.

B. Validation Strategy

Despite the fact that the proposed framework is conceptual in nature at this stage of research, its future validation can be achieved by means of publicly accessible cybersecurity datasets.

The possible datasets are:

- IoT-23 Dataset
- CICIDS2017 Dataset
- UNSW-NB15 Dataset
- BoT-IoT Dataset

The framework can be evaluated on the basis of the following performance indicators:

- Accuracy
- Precision
- Recall
- F1-Score
- Detection Delay
- Event Correlation Rate
- Attack Reconstruction Accuracy

A comparative evaluation can be carried out between classic anomaly detection systems and the Temporal-Aware Detection Framework proposed.

V. RESEARCH GAP

The review of the current literature suggests that considerable work has been done towards enhancing the accuracy of anomaly detection, machine learning, and automated response in AI-secured IoT ecosystems. Still, there is a lack of focus on the aspect of time for cybersecurity monitoring.

Existing AI-based solutions usually target the task of finding isolated anomalies that arise within a short period of observation. While this approach shows good results in terms of the efficiency of immediate threat detection, it ignores relations between events that occur over a long period of time.

Current cloud-based architectures for detecting anomalies are mainly concerned about:

- Real-time anomaly detection
- Intrusion classification
- Predictive analytics
- Automated response systems

Nevertheless, there are still many unsolved problems in the field:

1. There is no effective mechanism for correlating temporal events.
2. No metric of temporal blindness was ever introduced.
3. Inability to reconstruct attack timelines.
4. Lack of historical security context preservation.
5. No framework for slow and stealthy attacks detection.
6. No research on temporal risk scoring mechanisms.

In addition, many previous works tend to take for granted the notion that better anomaly detection is synonymous with better situational awareness. However, it does not consider the fact that key attack vectors may be concealed in an analysis done on its own.

As such, there is a glaring need for future works to design and build time-aware security architectures which can correlate distributed security events, reconstitute attacks and reduce temporal blindness in AI-enabled IoT systems.

The suggested Temporal Aware Detection Framework seeks to fill this gap by adding temporal memory, event correlation and risk-based attack reconstruction capabilities.

VI. LIMITATION

Though the effectiveness of AI-protected IoT solutions is gradually increasing, there are still some limitations that affect the overall threat detection abilities of such solutions. Most AI algorithms require high-quality training data, and any error in the training data may affect the result of the analysis. Moreover, the lack of transparency in the algorithmic logic may sometimes affect the overall understanding of security analysts about a particular decision. Cloud-based detection systems, though highly scalable, may sometimes cause the fragmentation of security telemetry, thus affecting the continuity necessary for understanding a gradual attack. Overdependence on automated systems may also cause the loss of contextual information, especially when handling a massive amount of data. Privacy concerns also play a significant role, as they demand the proper handling of sensitive information in a distributed environment. Moreover, AI algorithms may sometimes fail to recognize new attack patterns, thus reiterating the need for human intervention in ensuring the accuracy and reliability of security operations.

VII. CONCLUSION

Integration of artificial intelligence technologies into Internet of Things security infrastructure greatly contributes to improving the process of network monitoring and identification of anomalies as well as automated handling of threats. Nevertheless, based on the results of this research, one can observe that current cloud-based detection system is susceptible to one very important problem called temporal blindness.Temporal blindness is the situation when low-level attacks that happen during certain periods of time are viewed separately without considering the whole attack scheme as a coordinated set of actions performed at different times. Therefore, it becomes possible for skilled attackers to use the lack of temporal awareness and conduct multistage attacks unnoticed. This paper analyzes the literature, real-world cases like Mirai and SolarWinds, and existing cloud-based detection system architecture to identify weaknesses in the traditional approach to anomaly-based monitoring. The results of the investigation show that fast detection capability alone does not provide sufficient situational awareness in the modern IoT environment.

In order to solve the problem, this paper suggests the Temporal-Aware Detection Framework, which includes mechanisms of temporal memory, event correlation, attack timeline reconstruction, and temporal risk score calculation.Future research should address the implementation and experimental validation of the presented framework through the use of publicly available datasets for cybersecurity. Research in the areas of temporal correlation algorithms, explainable AI techniques, and human/AI security systems may result in even more efficient detection of multi-stage threats.

Ultimately, the efficiency of future security systems for IoT will be determined not only by their ability to detect threats quickly but also by their ability to comprehend the evolution of security incidents over time. Through increasing temporal awareness, the organizations may significantly decrease the likelihood of missing multi-stage attacks.All of the mentioned additions will resolve almost all major-review points: framework, architecture, algorithm, metrics, formal definition, validation approach, research gap, and conclusion.

REFERENCE

[1] L. Atzori, A. Iera and G. Morabito, “The Internet of Things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road

ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[3] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2021.

[4] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] A. Botta, W. De Donato, V. Persico and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[8] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.

[9] M. A. Ferrag, L. Maglaras, S. Moschoyiannis and H. Janicke, "Deep learning for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1347–1380, 2020.

[10] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Communications Surveys &Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[11] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognition*, vol. 84, pp. 317–331, 2018.

[12] R. Vinayakumar*et al.*, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[13] M. Liyanage, A. Braeken, P. Kumar and M. Ylianttila, "IoT security: Advances in authentication," *Future Generation Computer Systems*, vol. 82, pp. 666–677, 2018.

[14] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

[15] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[16] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[17] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[18] A. Botta, W. De Donato, V. Persico and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[19] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognition*, vol. 84, pp. 317–331, 2018.

[20] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN Computer Science*, vol. 2, no. 3, pp. 1–21, 2021.

[21] J. A. Kroll *et al.*, "Accountable algorithms," *University of Pennsylvania Law Review*, vol. 165, no. 3, pp. 633–705, 2017.

[22] Digital Forensic Research Workshop (DFRWS), "A roadmap for digital forensic research," 2001.