Policy Design in Zero-Trust Distributed Networks: Challenges and Solutions

Fannya R. Sandjaja, Ayesha A. Majeed, Abdullah Abdullah, Gyan Wickremasinghe, Karen Rafferty and Vishal Sharma*

***Abstract*—Traditional security architectures are becoming more vulnerable to distributed attacks due to significant dependence on trust. This will further escalate when implementing agentic AI within the systems, as more components must be secured over a similar distributed space. These scenarios can be observed in consumer technologies, such as the dense Internet of things (IoT). Here, zero-trust architecture (ZTA) can be seen as a potential solution, which relies on a key principle of not giving users explicit trust, instead always verifying their privileges whenever a request is made. However, the overall security in ZTA is managed through its policies, and unverified policies can lead to unauthorized access. Thus, this paper explores challenges and solutions for ZTA policy design in the context of distributed networks, which is referred to as zero-trust distributed networks (ZTDN). This is followed by a case-study on formal verification of policies using UPPAAL. Subsequently, the importance of accountability and responsibility in the system's security is discussed.**

***Index Terms*—Zero-Trust, Agentic AI, Policy design, Security, Formal verification**

I. Introduction

Security is undoubtedly one of the most critical issues in consumer technology seen from the sharp rise in attacks against enterprises. Puthal et al. (2017) [1] have mentioned that traditional perimeter-based security can no longer sustain the improvement of cyber attacks in recent years. Hence, more novel solutions are needed to defend against new types of cyber security threats, such as those generated by data breaches [2]. A security model, namely the zero-trust architecture (ZTA), proposed in 2010 by Kindervag et al. [3], has been gradually gaining more traction lately because it can help solve most of the current security scenarios, particularly in the context of distributed networks, which are explored in this paper as zero-trust distributed networks (ZTDN). Zero-trust (ZT) operates based on the *trust nothing, verify everything* concept, which assumes that nothing in the system is inherently trustworthy [1], [4]. The security model in [3] adopts a few principles, namely least privilege, trust no one, micro-segmentation, and always verify. Applying this concept to distributed networks can help strengthen the defense against vulnerabilities. Distributed networks are widely used for migrating services to the cloud and creating separate data centers. This raises security concerns, such as malicious attackers gaining access to all resources through a loophole from a single-point entry that can be addressed with ZT, for example, through its principle of micro-segmentation [5]. Figure 1 displays an example of a use case for implementing ZT in distributed networks.

The components of ZTA include the policy enforcement point (PEP) and the policy decision point (PDP), which consist of the policy engine (PE) and policy administration (PA). A PEP is defined as a system that oversees every connection request that comes through the network. It communicates with the PA to forward requests from the user and receive updates on whether the user is trusted based on the policies [6]. Here, the PA can be trusted, and the summary of individual components is provided in Figure 1.

In the given Figure 1, a user is someone who wants to gain access to enterprise systems, whether that is an enterprise's private or hybrid network. System grants trust to the user to allow entry. For this purpose, security policies must be in place to protect the network and be selective of who gets admission to the resources that are being requested, and in ZTDN, policies play a vital role in allowing and denying access to a system's resources.

For each network and its resources, a PEP is in place as a point of authentication and authorization. This is done even though the user has been authenticated and authorized when initiating access to the enterprise network via user login credentials or other methods. This is a part of the ZTA principle of continuous monitoring and constantly verifying the actions of the user.

Jung et al. (2022) [7] have explained that a PA acts as an administrator for the network connection. This includes communicating with the PE on whether the policy is recognized and whether the user identity is authorized to access the resources that have been requested. PA can create user access certificates, credentials, and per-session authentication. When a user is trusted and their access is authorized, the PA commands the PEP to open the communication channel for the user to the resources. However, if the user is untrustworthy and their credentials are unauthorized, the PA will instruct the PEP to block all communication channels for the user. PE also has the capability to revoke user access using supplemented policies, and it records the history of access requests, which can help in making future decisions [7].

Even with the claims of being able to defend against the developments of attacks, there are still some challenges that can be faced while utilizing ZT in distributed networks, such as setting suitable access policies for the authorized user or

F. R. Sandjaja, A. A. Majeed, A. Abdullah, G. Wickremasinghe, K. Rafferty and V. Sharma are with the School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast QUB), Email: {fsandjaja, ayesha.abdulmajeed, abdullah.abdullah, gwickremasinghe01, k.rafferty, v.sharma}@qub.ac.uk.

Manuscript received ...

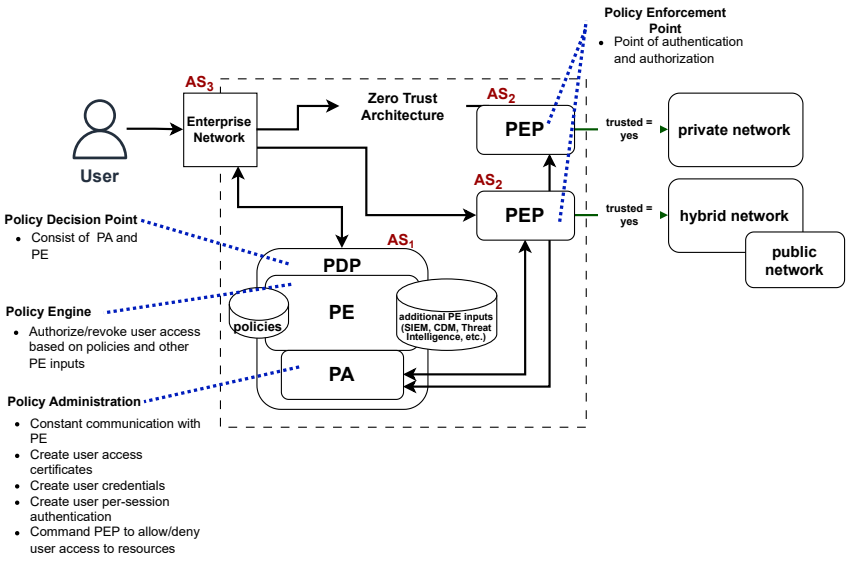


Fig. 1: An exemplary illustration of stand-alone zero-trust distributed network (ZTDN) (AS_x: Attack Surface x).

insider threats that have initial access to the system [8].

Most recently, Cisco has published its ZT network security architecture, which mainly focuses on ZT security in its distributed networks-related products. Other applications include the implementation of ZTA in cloud networks by Netskope and internal infrastructure networks initiated by Google's BeyondCorp [9].

Rais et al. (2024) [10] have explained that there has been no standardization for ZT policies, and industry-wide standards to define policies are still an ongoing development. It is understandable that policies in ZT are distinguishable mainly because they focus more on the logical components of the network. Further research on policies specifically in ZTDN is necessary to tackle the ever-evolving threats in this domain.

This article discusses the current development of ZTA, specifically in the context of distributed networks (ZTDN). It explores the challenges of ZT in distributed networks and discusses existing solutions to these challenges. This article also highlights the importance of responsible policy for ZTDN. Finally, an exemplary case study of formally verifying policies in ZTDN is presented using UPPAAL, an open-source tool that act as a protocol verifier and can be applied to verify and validate policies [11], followed by future research directions.

II. Securing Agentic AI With Zero-Trust (ZT)

The increasing usage of the buzzword agentic AI has been prevalent in the technology industry lately. However, what agentic AI is and how it can help impact the security of the system are still critical questions to answer. Agentic AI is a term in which AI act as agents, replacing human administrators in performing tasks and automating processes. This can improve the efficiency of the system while at the same time reducing operational costs. Placing AI agents in the system can also help in making decisions faster. However, some issues regarding utilizing agentic AI in a system must be considered, which include security, privacy, and trust of the resources, and in the long-term operations, the issues would include traceability and auditability of agents.

There are quite a few security and privacy issues that have yet to be explored in terms of agentic AI. Firstly, there is the possibility of private information inside the resources being exposed by the agents. This also ties in with the second problem, which is how AI queries and results can be manipulated. For example, a malicious attacker can access AI agents to bypass the security system and obtain sensitive data and/or manipulate the system itself. This also leads to the third point, where AI agents can increase the likelihood of an attack by expanding the attack surface. For example, if an agent is compromised, it can be used as a gateway to access and exploit private information. Lastly, from the user's perspective, there is a social assumption that users can be impacted if AI handles sensitive data. AI requires access to data, as it needs it to train on to produce intelligent results. This can diminish users' confidence as they may not feel secure with the future developments of agentic AI and its role in distributed systems.

The idea of securing agentic AI with ZT can be explored to address these concerns. If an agent is placed as a point of contact for users before being able to access resources, ZT can be implemented on top of that to ensure that the results of the agent regarding access requests align with the policies that the PE has in place. This means ZT and its principles can benefit the system when incorporated into agentic AI systems. From the CAPEX/OPEX point of view, latency problems might arise in this case when the server for AI agents is overwhelmed with the number of request queries, which can lead to potential DoS attacks.

III. Challenges and Solutions in ZTA in the Context of ZTDN

ZTA promises a better security structure than traditional security architecture, but there are some associated challenges when implementing it in distributed network scenarios. The

TABLE I: Key challenges in ZTDN (AS_x: Attack Surface x).

Area of Impact	Key Challenges	Potential Attacks	Rule-based ZTDN		Agentic AI	
			SLAs	KPIs	SLAs	KPIs
Policy Engine	No quantitative trust evaluation [12]	Conflicting network access (Figure 1 (AS_1))	Policies for trust evaluation algorithm	Unauthorized attempts frequency analysis	Procedure for AI forensics	Activity log
	No thresholds for trust score [13]	Data manipulation (Figure 1 (AS_1))	Policies for enterprise trust score threshold	Response time and Incident prevention ratio	Procedure of default behavior	Results analysis and Misbehavior detection
	Lack of access control rules [14]	Brute-force attacks, Compromised access credentials, and Insider threats (Figure 1 (AS_1,AS_3))	Rules for enterprise access policy	Device availability and Device inventory log	Procedure of agents' identification	Availability and Accessibility
	Lack of trust awareness in policy language [15]	Malware, Social engineering attacks, and Phishing (Figure 1 (AS_1, AS_3))	Configurable and responsible policy design with defined attributes	Regulatory requirements, Latency, and Breach attempt counts	Procedure of interrupting/terminating process	Response time
Policy Enforcement Point	Component failure [16]	Brute-force attacks, DDoS (Figure 1 (AS_2, AS_3))	Component failure management and resolution	Breach attempt counts and Response time	Continuous monitoring of AI agents	Response time, Availability, and Accessibility

primary challenge is the lack of research on the policy engine, which can lead to confusion about who is responsible for approving access and associated accountability. Earlier literature has stated some challenges that are faced when trying to implement the concept of ZT, which include the lack of methods for quantifying trust in users, the lack of defined thresholds for said trust, the lack of clearly defined rules for the access control, the lack of trust awareness in policy language, and scenarios where ZT component fails.

Ge and Zhu (2024) [12] have focused on a few challenges when dealing with ZT in the context of a 5G Internet of things (IoT) network and have mentioned that one of the problems is the lack of quantitative definition and measurement of trust from the agent, which might impact how the policies are planned and designed. In their paper, agent refers to an entity in an agent-centric trust evaluation framework. Trust is a vital part of defining policies to ensure that access permission is only granted to continuously authenticated and authorized users. This means that a distinct responsible policy should be in place, in particularly dealing with the ZTDN scenarios. In their paper [12], the authors have proposed a mathematical approach to quantify trust, exploring the possibility of utilizing game theory as part of the policy engine plan and design.

Further down the challenges in the trust aspect, Bradatsch et al. (2023) [13] have discussed the gap in the available list of attributes that can be placed into the policy engine. Their work has focused on the trust algorithm and addressed the challenge of not having a clear threshold to be compared with the trust scores attained through the policy engine. Further, the authors have highlighted the need for novel solutions in trust algorithms and emphasized how access decisions can be made from specific actions [13]. They have considered a novel solution for defining trust in policy engines that quantifies the attributes needed to allow access to enterprise resources by defining a new method for setting the threshold for trust scores.

Another perspective on the challenges in ZTDN comes from a paper by Spanier et al. (2023) [16], who have mentioned that while ZTA can reduce the damage caused by malicious attacks in the networks, it is often observed that centralized authentication and PEP can be a hindrance that causes a single point of failure. Taking this into consideration in ZTDN, it is essential to be critical of the failure of components at the individual level. There is a lack of solutions for hosts to communicate with each other when a particular element fails in the network. Thus, the architecture must be resilient so that when one component fails, another component can still be available. However, it is unclear whether a backup component will be available in the system and if this will result in additional overheads or redundancy. The authors in [16] have explored the prospect of applying blockchain authentication for user verification, which may be fed into a policy validator. In distributed networks, to ensure that all systems adhere to the same policy, a policy validator can be implemented to emphasize the responsibility of the policies in the engine. Their approach includes decentralizing the policy engine to make the system more efficient in decision-making.

From the access control and policy perspectives in ZTA, Huber and Kandah (2024) [14] have discussed some challenges related to maintaining access policy. They have emphasized the lack of rules in the ZTA's access control system. Malicious attacks can compromise the system due to existing vulnerabilities without a clear definition of who, what, when, and how a user can access the network. The authors in [14] have suggested a solution of integrating a trust management component into ZTA, expecting to increase the architecture's security posture. Their proposed architecture, Zero Trust+, focuses on dynamically authenticating and authorizing users in real-time with adjustments according to the user's behavior.

This direction of research is further supported by the works of Dimitrakos et al. (2020) [15], who have explored the possibility of further enhancing ZTA because of found weaknesses, namely, the lack of certification or service level agreements (SLAs). In their work, the authors have emphasized these weaknesses as a significant concern in unpredictable security or privacy issues. Their work further suggests that the current policy language does not include trust awareness as one of its main components, hence limiting the trust and access policy. Considering such aspects of strengthening ZTA, it is further advisable to explore policy agreements for scenarios that encounter unpredictable adversaries. Dimitrakos et al. (2020) [15] have recommended incorporating attribute-based access control with a trust level evaluation engine for a policy evaluation engine in ZTA. Their solution, in particular, focuses on consumer IoT. Their security posture combines dynamic authorization, usage control (UCON), and probabilistic trust assessment, which is referred to as UCON+, simultaneously supporting policy and trust level evaluation, attribute value retrieval, and policy parsing.

Most key challenges from earlier research show a correlation between the need for better policy design and cultivating trust in the user. These new solutions have been impactful in the field of ZTDN. However, the PE component, particularly the policies itself, has not yet been broadly explored. This is critical in ensuring the user is deemed trustworthy to access requested resources. This leads to the current issue of developing and implementing responsible policy design. With the increasing usage of artificial intelligence (AI) tools to design policies, responsible policy design ensures that all policies to secure enterprise networks comply with each specific country's regulations. This is where SLAs may come into play, with an explicit agreement between the network and users, as it can be helpful to provide transparent terms and conditions about the usage and how users can access resources, as the least privilege tenet is applied. From the enterprise perspective, setting up these SLAs would also help set the baseline on how the services use users' personal data. Additionally, continuously monitoring the system's key performance indicators (KPIs) can be beneficial as an alert if unexpected metrics show up.

In this regard, setting up individual agents could be efficient and offer better control of systems design. However, the recent developments in agentic AI suggest that improper configurations can make the system more vulnerable. Here, SLAs that can be beneficial to be put in place include, SLAs for AI agent's default behavior, reliable tag identifier of each AI agent, a procedure to interrupt or terminate the process of agentic AI, consent of using AI agents, regulations of AI, what data protection law is being used for the agentic AI and which law enforcement documents does the agentic AI comply with.

On the system side, KPIs can be monitored continuously to safeguard the accessibility of the AI agents. These include the response time, availability, activity log, and result analysis of these agents in the system. This ensures that whenever the response time is longer or shorter than normal usage, that could be an indication of suspicious activity. This also applies to the availability and activity log of the agents. One of the KPIs could be result analysis that can provide a more in-depth observation of how the AI agents return a response to a user's query. Here, semantic analysis can be used if there might be sensitive information being exchanged between the user and agents, which could be an indication of a malicious act in the system. Table I summarizes all critical challenges in rule-based and agentic AI driven ZTDN, the potential attacks that could occur, and provides insight into what type of SLAs can be implemented with the KPIs that could be monitored continuously.

IV. Challenges in Responsible Policy Design

There are several problems when it comes to responsible policy design. Firstly, the methodology by which the system gives access to entities. Different ways have been explored to determine trust scores and levels, ranging from mathematical approaches to utilizing novel technology solutions like blockchain and game theory. But how are the standards defined for these attributes? How can different systems adjust their thresholds? These are incredibly challenging questions in distributed networks particularly where the trust threshold may not be the same for every entity. Hence, a responsible policy, possibly in the form of an SLA, is needed as enterprise networks are vastly different and include diverse requirements, structures, and compulsory policies [17].

Secondly, the methodology by which the same user is treated differently across different network components, which is also provided as an exemplary illustration of ZTDN architecture in Figure 2. Here, in this scenario, a user tries to access three different enterprise networks, where the first enterprise network evaluates the user trust score to be above the threshold. In that case, the user is allowed access to resources. However, in enterprise network 2 and 3, the user trust scores are below the threshold, which means the user is untrusted. This can be a vulnerability in the system if the data centers are shared across these enterprise networks. It might make the system more prone to attacks, especially from within the networks. As such, a policy design solution that can be implemented industry-wide would be helpful for the future development of ZT in distributed networks [18].

Lastly, there is an issue with accountability in ZT policies. There are no clear rules on who is responsible for the policies fed into the PE. This could also be related to network evidence gathering and, depending on the use of agentic AI, it may additionally require AI forensics. In this regard, who will be responsible if there is a policy design flaw? Such concerns need a clear structure of people overseeing decisions on creating, monitoring, and removing policies in ZTDN [19].

Today, many policies are AI-generated; therefore, ensuring these policies comply with country-specific regulations is necessary. Responsible policy means that all attributes inside the policy have been thought of for all related components and have been defined clearly, and methods of due diligence must be in place. Ensuring these policies comply with local and international regulations and standards is also essential [19]. This involves the transparency of policies and rules, which can be achieved by clearly presenting these in SLAs, as discussed earlier. In addition, the sustainability of these components

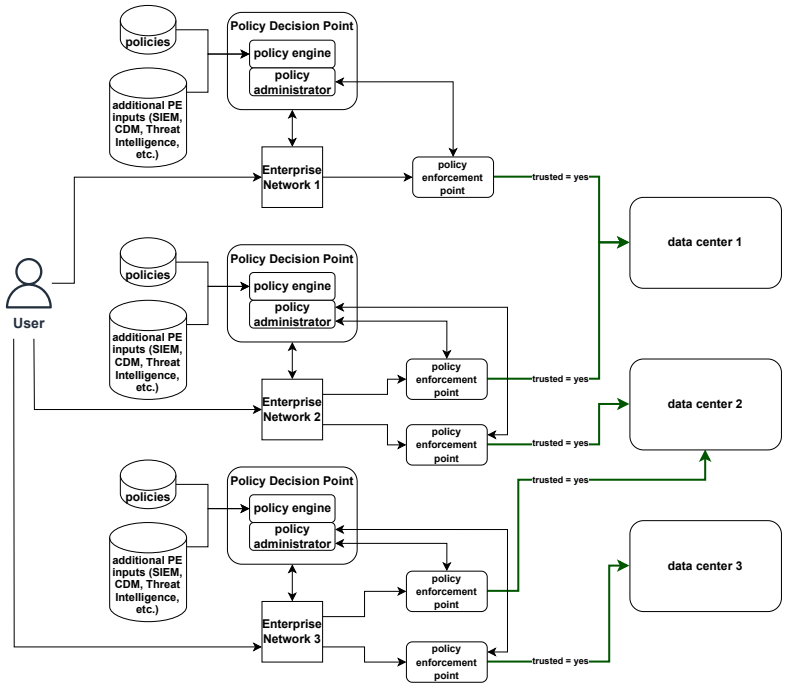


Fig. 2: An exemplary illustration of ZTDN architecture.

is vital to the growing digital footprint in technology and understanding their impact in real-world situations. Figure 3 summarizes critical points when designing policy for enterprises and raises critical questions to form SLAs. Considerable issues regarding AI-generated policies are transparency and the associated biases, and it is essential to ensure ethical policy-making when AI is used for this purpose.

Jawhar *et al.* (2024) [20] have developed a module to generate policies by AI systems using Open AI API. Their module which contains requirements on international standards compliance and list of controls in the security framework results in a prompt that are being fed into Chat GPT-4. Their experiment resulted in effective generated access control policies that are dynamically dependent on organization infrastructure and adhere to the international standards of NIST 800-171 and ISO 27001/27002. However, they have mentioned that these generated policies have to be audited and monitored to ensure that organizations are still in control of their security operations. Another example have been discussed by Fu *et al.* (2025) [21] where they have used AI algorithms to detect and implement policies in order to produce better policies for the system in real time.

V. Fitting Zero-Trust (ZT) Into Current Standards

ZT, in its application, may complement the already implemented cyber security standards in organizations. Current standards in cyber security include ISO 27001, which covers guidance for establishing, implementing, maintaining and continually improving an information security management system [22]; NIST CSF ID.GV-1, which covers the establishment and communication of organizational cybersecurity policies and NIST Special Publication 800-53 contains a guide on Information Security Testing and Assessment [23]; and ISA/IEC 62443 that covers cybersecurity requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS) [24]. ZT standard for enterprises' cyber security itself is highlighted in NIST Special Publication 800-207, which explains in depth the definition of ZTA for enterprises and the different types of implementation [19].

Taking an example of relating ZT to ISO 27001 standard, the book by Jahankhani et al. (2020) [22] have mentioned that ZT concepts do not cover physical security, culture, and governance, which are the core aspects of ISO 27001. Hence, ZT must be viewed as an augmentation to these standards, not a replacement. Adopting ZT can strengthen access control and network security control, which are key principles of ISO 27001. The standard requires regular review and improvement of the information security management system (ISMS). This aligns with the ZT principle of continuous monitoring. With ZT, it is always assumed that attackers are already inside the system, which aligns with a control category that ISO 27001 have: information security incident management (ISIM). Key ZT principles like verifying everything and implementing least privilege access can be beneficial in enhancing ISO 27001's access control category. Additionally, ISO 27001 requires information segregation, which can be done by micro-segmentation, an aspect of ZT. This demonstrates effective access control implementation, network security management, and system acquisition, development, and maintenance, which shows the organization's risk management.

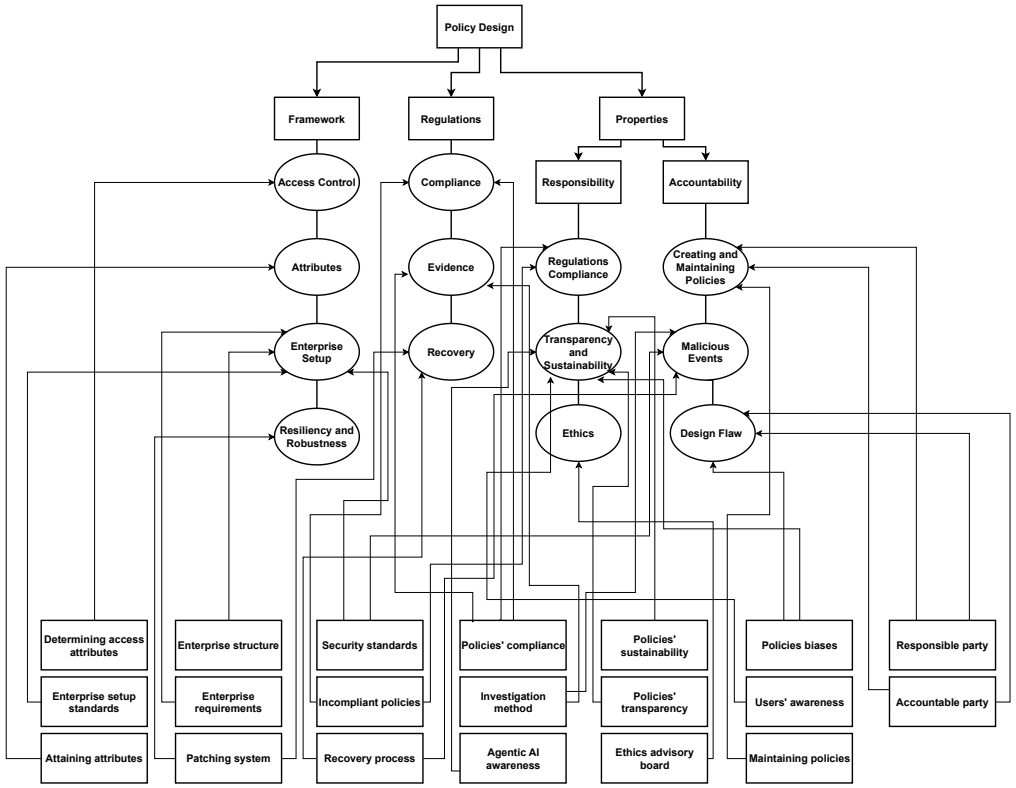
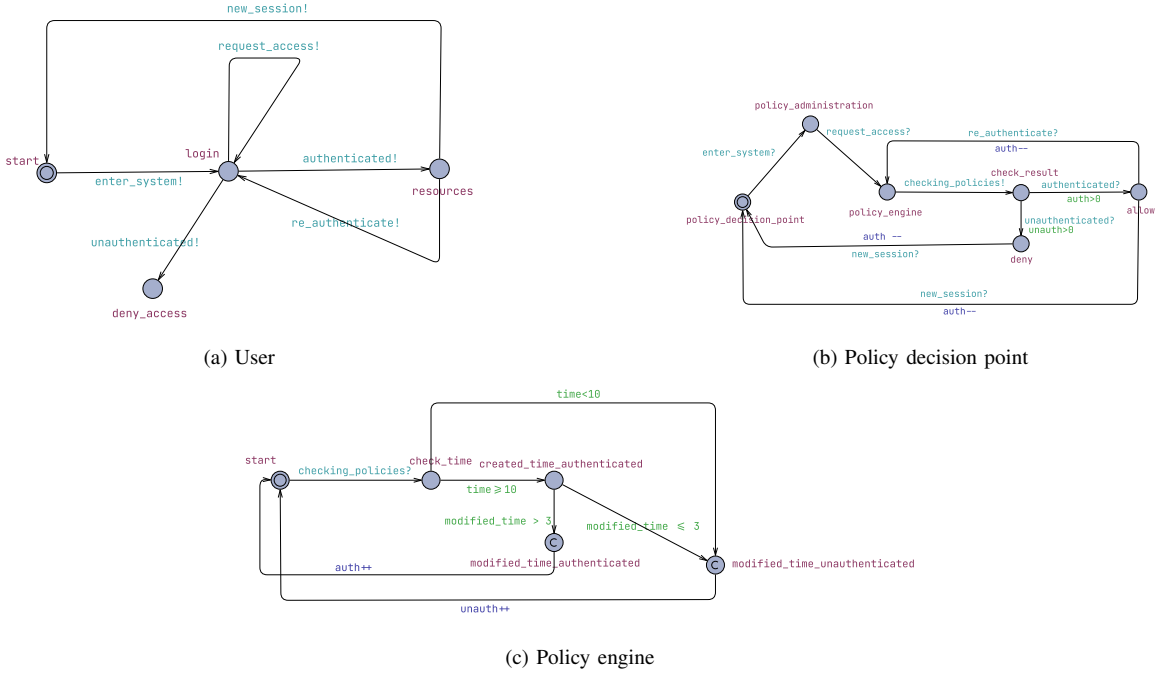


Fig. 3: An illustration of challenges of policy design in ZTDN.



(a) User

(b) Policy decision point

(c) Policy engine

Fig. 4: An example of ZTDN's state diagram for a single user.

VI. Formal Verification of Policies in ZTDN

With the number of policies that enterprises have for input to the PE, as shown in Figure 1, formal verification of those policies is crucial. This ensures that there are no errors in the policies that might affect the working of the system while also reducing the probability of malicious attacks in the system.

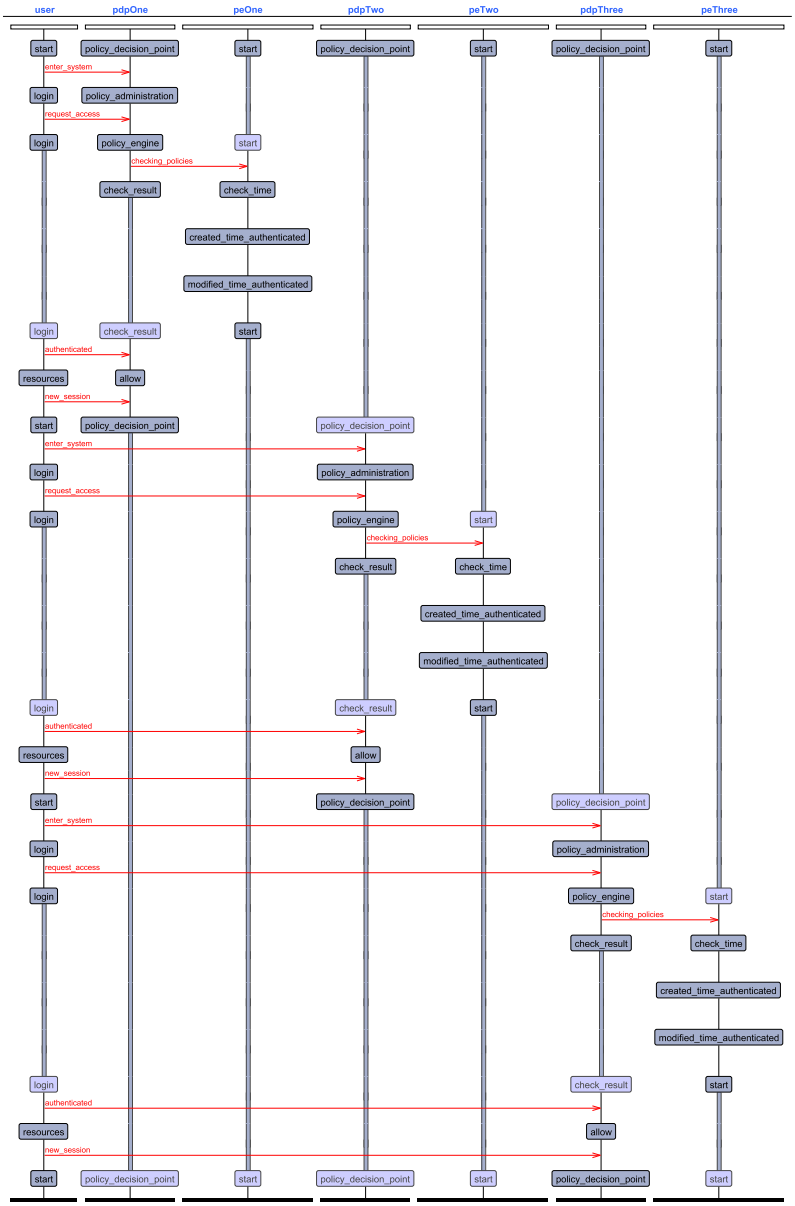


Fig. 5: ZTDN's state diagram showing the authenticated request flow.

However, with the rapid increase of usage of AI in this space, it does get more complicated to maintain policies in organizations, along with the dynamic adaptive policies, which is a part of ZT's tenet. This can be further impacted with generative AI (GenAI). Hence, formally verifying these dynamic policies is beneficial for enterprise systems. This is supported by the research done by Kanner and Kanner (2021) [25], where it has been mentioned that verification of policies, especially access control policies, is a helpful step in the development of the system to guard unauthorized access. Verification also includes formally establishing an explanation for every single case of implementation in the system. The authors [25] have explained the pros of verifying policies, which include automatically finding errors in the design/implementation of the system.

Implementing micro-segmentation is a way to apply ZT in enterprise systems [26]. With different locations hosting networks for the enterprise, it becomes natural to implement micro-segmentation, and AI-generated SLAs can drive the decision to implement this micro-segmentation. This can help prevent all servers from being maliciously attacked at the same time. For example, by having all enterprise-distributed networks micro-segmented, an attack on a component can be compartmentalized in a specific area without spreading laterally through the system. This also aligns with the service migration in the enterprise network, as compartmentalization can benefit them by ensuring the system's security through micro-segmentation of its components and allowing for gradual service migration.

A method that can be used to do formal verifications of policies in ZTDN can be attained using timed automata (TA) [27]. Using this theory, it can trace back the time when policies are made, as well as if there is any point after that time when the policies have been changed. This can be helpful to verify policies that are fed into the PE, and ensure these are legitimately valid and have not been tampered with by any party. This is particularly useful if AI generates some of the policies, and time stamping is required against them.

It has not been widely explored whether policies created using AI-powered tools are deemed trustworthy. Further, aligning this concept with ZT, it is essential that at every step in the network, no access is trusted and must be authenticated and authorized. To complement the use of TA, tools like, UPPAAL [28] can be helpful. UPPAAL is an open-source tool that act as a protocol verifier and can be applied to verify and validate policies. In this paper, a case-study of formally verifying policies using UPPAAL is explored in the context of ZTDN.

Figure 4 illustrates an example of UPPAAL state diagrams from the user, PDP, and PE perspectives related to the distributed scenario in Figure 2. Figure 4a shows the system for users, which shows the process to request access to resources, and it synchronizes with the processes in the PDP. Figure 4b depicts the process that takes place in the PDP component of a ZTDN. This shows that the PDP will always re-authenticate users even after being authenticated to access resources the first time.

The Figure 4c illustrates how a policy can be verified in the PE. If the policy has been altered recently without any traceability component and missing log, there is reason to believe that malicious activity has occurred. Users will not be able to access resources as a result. When access is requested, there will also be checks to determine whether policies have been modified since the request has been received. This can enhance the PE's level of security. Simulating these processes would make it possible to detect occasions in which policies have been violated or altered by malicious actors or compromised AI agents.

To further demonstrate the flow of the PE in the PDP component of a ZTDN, Figure 5 shows the detail of the processes of each state in each template and how all of the components are interconnected. It also shows that there are no deadlock processes, as the re-authentication process of the user after getting access to the resources is always available and ready to be executed. This Figure 5 is particularly relevant to the scenario in Figure 2 where a user attempts to gain entry to three different enterprise networks.

VII. Policy Decision and Enforcement in ZTDN

When discussing policy decisions and enforcement in ZTDN, security and functional safety are both the focus of the technology in ensuring straightforward interaction between users and the service. There are a few properties in each focus that should be monitored, followed by the metrics by which each property is measured, as shown in Table II. These include availability, which can be observed by service and policy check time; integrity by doing data checksums and policy mapping; confidentiality by measuring the number of access attempts to service; authorization, which can be considered from the number of access violations; auditability viewed by logs and compliance; traceability which is considered by entity behaviour logs; authentication by doing identity verification; and robustness by measuring the amount of entity compromise.

On the other side, there are also a few functional safety properties that should be considered in terms of making decisions and enforcing policies in ZTDN. These include tolerance, which can be seen by faults observation; dependencies and diagnosis, which both can be observed by service availability; capacity, shown by the safety rate and planning; migration, which can be observed by service availability; containment, which can be observed by both service availability and compartmentalization; and recovery which the number of faults and failures of service can be measured.

Risks will always be present for any service, and in terms of the security and functional safety of policy decisions and enforcement in ZTDN, there are a few notable risks. Hence, there needs to be cautionary measures to ensure that the service is constantly monitored to check for any suspicious activity. These efforts are all vital in guarding the services against adversaries such as entity misbehaviour, policy misconfiguration, PE exploitation, insider threats, and multi-factor authentication failure. Another crucial part is accountability within policies in ZTDN, which can be managed by looking into policy vs. third-party infrastructure, enterprise network, compliance and regulations, and agentic AI forensics.

VIII. Open Problems and Research Directions

There are several open questions related to the expansion of ZTDN and its integration with agentic AI, in particular, where the focus is on having a responsible policy design. One of the critical directions that remains open is the runtime verification of the policies that are used as inputs for the PE component. Niu *et al.* (2022) [29] have proposed a ZT security policy detection method based on online verification to evaluate the effectiveness and security of policies in the PA component. It is worth researching other methods of formal verification for policies by considering the trade-off between the complexity of verification and the number of properties checked. Other methods of policy verification can help to improve the security and efficiency of policies. Using UPPAAL as a tool is just one way to perform formal verification of policies, and there are other methods that can be employed to ensure policy compliance and prevent malicious events [29], [30]. Another direction to explore is having a clearly defined methodology specifically catered to ZTDN that can be implemented industry-wide. An example of this is provided by Li *et al.* (2025) [31], who used ZT as a verifier to address security issues found in Compute First Networks (CFN) to be used as a platform for AI-generated content (AIGC) services. However, there is still a gap in the literature when it comes to implementing ZT on agentic AI systems. Another less explored yet critical dimension of policy design is establishing a clear structure for those overseeing decisions on creating,

TABLE II: Policy decision and enforcement in ZTDN.

Focus	Properties	Metrics and Influences	Adversarial Risks	Entities	Instances	Accountability
Security	Availability	Service and policy check time (internal)	Entity misbehavior Policy misconfiguration Policy engine exploitation Insider threats Multi-factor authentication failure	End users Policy decision points Policy enforcement points Payload in disaggregated Scenarios	Better load sharing Trust within zero-trust Application-specific policing Adaptive and flexible properties Robust integrations	Policy vs Third-party infrastructure Enterprise network Compliance and regulations Agentic AI forensics
	Integrity	Data checksums and policy mapping (internal)				
	Confidentiality	Access attempts (external)				
	Authorization	Access violations (external)				
	Auditability	Logs and compliance (internal)				
	Traceability	Entity behavior logs (internal)				
	Authentication	Identity Verification (internal)				
	Robustness	Entity compromise (internal)				
Functional Safety	Tolerance	Faults (internal and external)				
	Dependencies	Service availability (external)				
	Diagnosis	Service availability (external)				
	Capacity	Service rate and planning (external)				
	Migration	Service availability (external)				
	Containment	Service availability and compartmentalization (internal and external)				
	Recovery	Faults and failures (internal and external)				

monitoring, and removing policies in ZTDN, ensuring stability and accountability. This is supported by research conducted by Køien (2024) [32], which stresses the urgent need to assess transparency and accountability in the system, especially when AI is involved. It is vital to ensure ethical policy-making when AI-driven policies are involved. This includes associated biases that come with generating policies using AI. The above open problems are summarized as follows:

- **AI-driven policies**: The ethical side of having AI-driven policies needs to be further investigated, including their impact on the systems. Here, the impact can be positive or negative, and it will be driven by the set of requirements used for deriving the policies [21], [33]. Further, AI-driven policies can help run scenarios before any changes are reflected in the system.
- **Responsibility and accountability for policy design**: This is a large area to explore when dealing with policy design in ZTDN. There needs to be clear legislation on the responsibility and accountability of creating, designing, and implementing policies, especially when AI is involved and may present security risks. Some points to explore include having a traceability system for policies [32], [34]. The use of agentic protocols, along with telemetry information gathering, could help build solutions that are traceable and offer accountability over policies.
- **Agent orchestrator for ZTDN**: Agentic AI leverages an orchestrator for managing tasks and associated agents. However, when operating in ZTDN, the roles of PE and orchestrator can be combined for better visibility and control over agents, which may help reduce the complexity of having two separate entities that can be unified for better CAPEX/OPEX. Further exploration of the actual implementation of this can be conducted by examining the findings on the effectiveness and security of agentic AI systems when combined with ZT [31], [35].
- **Standards for policy design in ZTDN**: A major aspect of ZT is the standards that are being used currently in this field. As previously mentioned, current standards have not yet accounted for state-of-the-art technology advancements. Hence, there needs to be discussions on updating these standards to tailor them towards security risks in policy design [19], [36]. A clearly defined standard for attributes that takes into account policy design elements, such as trust scores or levels, thresholds, and when a user is allowed access to systems, is another associated

area to address. Standards [19] that are available do not account for factors such as agentic AI, and with recent AI advancements, guidelines for AI forensics could be a major open issue.

IX. Conclusion

This article has discussed the challenges and solutions of policy design in zero-trust distributed networks (ZTDN). Details of where ZTDN fits into the current standards and possible solutions for verifying policies are also discussed. The article further presents aspects of agentic AI and the enforcement and decision-making process within ZTDN. It further details about the formal verification of policies in ZTDN, which is shown by a case-study using timed automata through UPPAAL. This shows the feasibility of formally verifying and validating policies, emphasizing the policies have not been modified or tampered with. Future work on leveraging agentic AI for this purpose can be done along with the important aspects of accountability, traceability and forensics.

References

[1] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 4, pp. 24–27, 2017.

[2] A. Poirrier, L. Cailleux, and T. H. Clausen, "Is trust misplaced? a zero-trust survey," *Proceedings of the IEEE*, 2025.

[3] J. Kindervag, S. Balaouras, and L. Coit, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," *Forrester Research*, vol. 3, p. 56682, 2010.

[4] B. Dhruva, M. Mummigatti, D. Krishnamurthy, H. Namratha, U. Apoorva, and P. Ramakanthkumar, "Exploring zero trust architecture in interview bots: Mechanisms and challenges," in *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, pp. 1–6, IEEE, 2024.

[5] S. Lee, J.-H. Huh, and H. Woo, "Security system design and verification for zero trust architecture," *Electronics*, vol. 14, no. 4, p. 643, 2025.

[6] E. B. Fernandez and A. Brazhuk, "A critical analysis of zero trust architecture (zta)," *Computer Standards & Interfaces*, vol. 89, p. 103832, 2024.

[7] B. G. Jung, Y.-S. Yoo, K. Kim, B.-S. Kim, H. Lee, and H. S. Park, "ZTA-based Federated Policy Control Paradigm for Enterprise Wireless Network Infrastructure," in *27th Asia Pacific Conference on Communications (APCC)*, pp. 1–5, 2022.

[8] M. Tsai, S. Lee, and S. W. Shieh, "Strategy for Implementing of Zero Trust Architecture," *IEEE Transactions on Reliability*, vol. 73, no. 1, pp. 93–100, 2024.

[9] X. Feng and S. Hu, "Cyber-Physical Zero Trust Architecture for Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 394–405, 2023.

[10] R. Rais, C. Morillo, E. Gilman, and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, ISBN: 9781492096559, 2024.

[11] J. Bengtsson, K. Larsen, F. Larsson, P. Pettersson, and W. Yi, "UPPAAL – a tool suite for automatic verification of real-time systems," in *Hybrid Systems III*, (Berlin, Heidelberg), pp. 232–243, Springer Berlin Heidelberg, 1996.

[12] Y. Ge and Q. Zhu, "GAZETA: GAme-Theoretic ZEro-Trust Authentication for Defense Against Lateral Movement in 5G IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 540–554, 2024.

[13] L. Bradatsch, O. Miroshkin, N. Trkulja, and F. Kargl, "Zero Trust Score-based Network-level Access Control in Enterprise Networks," in *IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1422–1429, 2023.

[14] B. Huber and F. Kandah, "Zero Trust+: A Trusted-based Zero Trust architecture for IoT at Scale," in *IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, 2024.

[15] T. Dimitrakos, T. Dilshener, A. Kravtsov, A. La Marra, F. Martinelli, A. Rizos, A. Rosetti, and A. Saracino, "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1801–1812, 2020.

[16] A. Spanier, R. Zhao, and P.-C. Huang, "Securing Zero Trust Networks: the Decentralized Host-to-Host Authentication Policy Enforcement," in *IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1518–1523, 2023.

[17] Y. Ge and Q. Zhu, "Trust Threshold Policy for Explainable and Adaptive Zero-Trust Defense in Enterprise Networks," in *IEEE Conference on Communications and Network Security (CNS)*, pp. 359–364, 2022.

[18] M. H. Davis, U. Lang, and S. Shetye, "A Cybermodel for Privacy by Design: Building privacy protection into consumer electronics," *IEEE Consumer Electronics Magazine*, vol. 4, no. 1, pp. 41–49, 2015.

[19] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication*, vol. 800-207, 2020.

[20] S. Jawhar, J. Miller, and Z. Bitar, "Ai-based cybersecurity policies and procedures," in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, pp. 1–5, IEEE, 2024.

[21] Y. Fu, Y. Xie, W. Yi, B. Poudel, J. Cao, and H. Li, "Ipo-zta: An intelligent policy orchestration zero trust architecture for b5g and 6g," *Computer Networks*, p. 111450, 2025.

[22] H. Jahankhani, L. M. O'Dell, G. Bowen, D. Hagan, and A. Jamal, *Strategy, Leadership, and AI in the Cyber Ecosystem: The Role of Digital Societies in Information Governance and Decision Making*. Academic Press, ISBN: 9780128214596, 2020.

[23] "NIST Cybersecurity framework-Identify — nist.gov." https://www.nist.gov/cyberframework/identify, 2021. [Last Accessed 20-03-2025].

[24] "ISA/IEC 62443 Series of Standards - ISA — isa.org." https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Last Accessed 20-03-2025].

[25] A. M. Kanner and T. M. Kanner, "Special Features of TLA + Temporal Logic of Actions for Verifying Access Control Policies," in *Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, pp. 0411–0414, 2021.

[26] S. Keeriyattil, *Zero Trust Networks with VMware NSX: Build Highly Secure Network Architectures for Your Data Centers*. Apress, 2019.

[27] R. Alur and D. L. Dill, "A Theory of Timed Automata," *Theoretical Computer Science*, vol. 126, no. 2, pp. 183–235, 1994.

[28] J. Bengtsson, K. Larsen, F. Larsson, P. Pettersson, and W. Yi, "Uppaal—a tool suite for automatic verification of real-time systems," in *International hybrid systems workshop*, pp. 232–243, Springer, 1995.

[29] Z. Niu, L. Dong, and Y. Zhu, "The runtime model checking method for zero trust security policy," in *Proceedings of the 7th International Conference on Cyber Security and Information Engineering*, pp. 8–12, 2022.

[30] J. Liu, Y. Cao, Z. Zhou, and T. Tian, "A data security formal verification framework for iot application systems," in *2025 8th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, pp. 279–283, IEEE, 2025.

[31] Y. Li, D. Zheng, H. Fang, H. Xing, X. Chen, and X. Cao, "Towards prompt chain deployment in zero trust-enabled compute first networks," *IEEE Transactions on Consumer Electronics*, 2025.

[32] G. M. KØien, "The road to a trustworthy 6g; on the need for a "zero trust 6g" paradigm," *Journal of Mobile Multimedia*, vol. 20, no. 1, pp. 45–68, 2024.

[33] Y. Sharma, P. Kaushik, and I. Malhotra, "Enhancing fpga security: An ai-driven approach to root of trust architecture," in *2025 7th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 1080–1085, IEEE, 2025.

[34] I. Adom, M. Awais, M. Raza, U. Khan, and O. Chughtai, "Enhancing access control, authorization, and accountability in cyber-physical systems using machine learning," in *2024 International Conference on Frontiers of Information Technology (FIT)*, pp. 1–6, IEEE, 2024.

[35] E. Haque, K. Hasan, I. Ahmed, M. S. Alam, and T. Islam, "Enhancing uav security through zero trust architecture: An advanced deep learning and explainable ai analysis," *arXiv preprint arXiv:2403.17093*, 2024.

[36] S. Al-Tamimi, Q. A. Al-Haija, and K. Alrawashdeh, "Zero-trust architecture for securing internet of things (iot) networks: A review," in *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, pp. 1–6, IEEE, 2024.