Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 3, June 2025, pp. 1896~1904
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i3.pp1896-1904

A comprehensive access control model integrating zero trust architecture

Pattabhi Mary Jyosthna[1], Konala Thammi Reddy[2]
[1]Department of Computer Science and Engineering, B. V. Raju Institute of Technology (BVRIT), Narsapur, India
[2]Department of CSE, School of Engineering and Sciences, GD Goenka University, G D Goenka Education City, Sohna, India

Article Info

Article history:

Received Mar 4, 2024
Revised Dec 6, 2024
Accepted Feb 27, 2025

Keywords:

Attribute-based access control
Continuous monitoring
Principle of least privilege
Role-based access control
Trust-based access control
Zero trust architecture

ABSTRACT

In contemporary IT landscapes, trust in entities, whether internal or external, within organizations has become obsolete. Establishing and enforcing strict access controls, alongside continuous verification, is imperative to safeguard organizational resources from potential insider and outsider threats. The emergence of zero trust architecture (ZTA) addresses this need by advocating for a paradigm shift in security. This research proposes a comprehensive access control model aligned with the fundamental ZTA security principles, namely least privilege, conditional access, and continuous monitoring. The model integrates well-established access control paradigms, including role-based access control (RBAC) to uphold the least privilege principle, attribute-based access control (ABAC) to support conditional access, and trust-based access control (TBAC) to enable continuous monitoring. To determine the trust level of a user requesting access, an analysis of the user's log activities is conducted using the N-median outlier detection (NMOD) technique. This analysis aids in evaluating the trustworthiness of the user seeking access to resources. Furthermore, this research assesses the efficiency and efficacy of the proposed integrated access control model in comparison to existing access control models, primarily focusing on their respective functionalities.

Corresponding Author:

Pattabhi Mary Jyosthna
Department of Computer Science and Engineering, B. V. Raju Institute of Technology (BVRIT)
Narsapur, India
Email: jyosthna.p@bvrit.ac.in

1. INTRODUCTION

Nowadays organizations are running under a dynamic and decentralized IT environment where the resources of the organizations are hosted by some trusted third party and those resources can be accessed by the users of the organization remotely. The secure accessing of these resources became a challenging task for the organizations. According to Syed *et al.* [1], perimeter-based network security is insufficient since, if an attacker breaches the perimeter, they are free to travel laterally. So, the zero-trust architecture (ZTA) has been introduced to secure enterprise assets and subjects. The core principle of zero trust is to never automatically trust any user, device, or network, regardless of whether they are insiders or outsiders to the corporate network. Instead, it enforces strict access controls and continuously verifies and validates user identities and device characteristics before granting access to resources. It should mainly include the security components like least privilege, continuous monitoring, and conditional access. least privilege ensures that users and devices are granted the minimum level of access necessary to perform their duties, reducing the potential impact of a security breach. continuous monitoring of user behaviour and device status is performed to identify the suspicious activities or anomalies. Conditional access ensures access policies are based on

contextual information such as user location, time of access, and security posture of the device. So, organizations must use an efficient access control models that take zero-trust architecture into consideration [2].

Organizations utilize the appropriate access control models based on their requirements such as identity based access control (IBAC), role based access control (RBAC), attribute based access control (ABAC), risk based access control (RBAC), and capability based access control (CBAC). If a person aquired multiple access permissions in any of the access control model, it may cause internal threats [3] in the organization. To avoid the threats due to this excess access rights problem, trust-based access control (TBAC) models have been introduced. TBAC is a security model that determines access permissions based on the level of trust an entity has within a system or organization. Fujun *et al.* [4] calculated the trust value based on feedback from users' peers. Celikel *et al.* [5] assigned a priority number to each user by calculating risk value based on the user' role misuse and role abuse. The researchers in [6]–[8] calculated the trust value of a user from direct observations or from user access history. Ma *et al*. [9] assess the risk of assigning user to role in the traditional RBAC model. They add a risk function (RF) as a component to the RBAC model. A risk value between [0,1] is calculated by analyzing the level of confidence between user and role. Baracaldo and Joshi [10] calculated the trust value based on the possibility of misuse with their actions. Few researchers [11]–[13] have used machine learning techniques to analyze the possibility of risk and risky behaviours to calculate the trust score.

In recent years, some of the applications adapted ZTA for providing better security practices. Mehraj and Banday [14] have discussed a conceptual model to adapt ZTA in a cloud environment for establishing trust-based authorization for granting access to the cloud resources. Chen *et al*. [15] proposed a 4-Dimensional security framework for 5G smart healthcare organization that leverages the zero-trust architecture. subject, object, behaviour, and environment are the 4 dimensions, it has been considered for establishing trustable, dynamic access control models. Yao *et al* [16] proposed a dynamic trust based access control and authorization model based on zero-trust architecture. They have calculated a user trust score based on the user's historical behaviour and the current behaviour. User's activity on systems like login behaviour, operation behaviour, network behaviour is considered as their behaviour. Dimitrakos *et al*. [17] incorporated evaluated trust level as a condition along with the existing authorization policies. That is the fusion of Trust-level evaluation with ABAC model. The trust levels and attributes are continuously monitored and update dynamically if required. This authorization model used in ZTA for consumer IoT. Trust level is calculated using Bayesian method.

Zhang *et al*. [18] proposes a zero trust framework for power IoT that incorporates contextual information like time, location, and user behavior for access decisions. Alagappan *et al.* [19] Enhances ZTA for virtual power plants by integrating policy-based controls that adapt to different security needs and conditions. Federici *et al.* [20] proposed an architecture where a fine-grained access control model with two level authentication for industrial internet of things (IIoT) infrastructures that collaborate teams through remote access. Feng and Hu [21] introduced cyber-physical ZTA model which includes a multi-layer access control engine and an integrated physical model-based and data-driven policy optimizer. The multi-layer access control engine can evaluate the trust scores for each component considering their cross-layer impact, while the integration of data-driven and model-based approaches can improve efficiency in optimizing access policies. Hong *et al.* [22] proposed a framework called Sys Flow to provide a fine-grained control for system resources. The comparative analysis of all these existing research in terms of combination of access control models is shown in the Table 1.

Table 1. Comparative analysis of existing research in terms of access control model

Research article	Access control models					
	DAC	RBAC	ABAC	RAdAC	CAAC	TBAC
Mehraj and Banday (2020) [14]		√				√
Chen *et al*. (2020) [15]		√	√			
Yao *et al*. (2020) [16]	√			√		
Dimitrakos *et al.* (2020) [17]					√	
Zhang *et al*. (2021) [18]					√	√
Alagappan *et al*. (2022) [19]		√		√		
Federici *et al.* (2023) [20]		√			√	
Feng & Hu (2023) [21]					√	√
Hong *et al.* (2023) [22]			√			√

According to the national institute of standards and technology (NIST) report on ZT [23], zero trust architecture is not a single product or technology; rather, it is a comprehensive security framework that combines various technologies, policies, and practices to create a more secure environment. From the

literature review, it is identified that a comprehensive access control model is not existed to leverage the ZTA security principles. The existing works are not supporting all three components as they combined atmost two access control models. The details are shown in the Table 1. User's work behavioural analysis is also not considered for finding the trust score in trust based access control (TRBC) models. The objective of this research is to propose a comprehensive access control model which integrates RBAC, ABAC, and TBAC models to enforce strict access control for resource access by analyzing the user attributes and behavioural analysis. The priority level for TBAC model is calculated based on their deviation score in their allotted roles using N-median outlier detection technique.

The Remainder of the paper is organized as follows. Section 2 describes the proposed model and their components for preventing unauthorized access. Section 3 explains the results obtained from the proposed model, the "Comprehensive access control model". Section 4 concludes the research work with key points that are done in the work.

2. PROPOSED METHOD

With ZTA, organizations can build strong authentication and authorization rules to allow access to resources based on the user's attributes. But, to achieve the least- privilege principle, organization's roles are the main concept to determine access [24]. So, the proposed model uses the combination of RBAC, ABAC, and TBAC models to fulfil the ZTA requirements. The components of the proposed model is shown in Figure 1. Which is the highlevel view of proposed comprehensive access control model. When a user requests access to a resource, the key generation engine evaluates the request with the user role-based permissions, the attribute-based policies, and user priority level of the user to determine whether the access to the resources should be granted or denied.

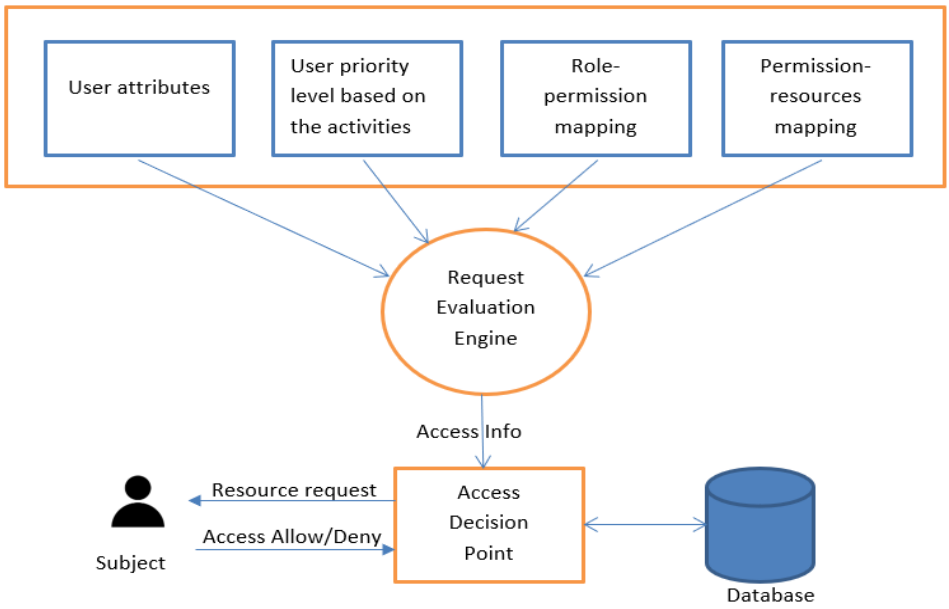


Figure 1. Block diagram of zero-trust aware access control model

2.1. User attributes

ABAC model uses attributes to determine access to resources. The list of user attributes such as user id, user role, resource attributes such as resource name, sensitivity level of access, action attributes such as operations (read, write, and update) to be performed on the requested resource, and contextual attributes includes time &location, network.

2.2. User priority levels by analyzing user's activity behaviour

The analysis of the user behaviour in his assigned role is used to define the user's priority level. Because, organization's tasks may change dynamically and role groups must work according to fulfill the organization's tasks. As a result, the role behaviour is not fixed at every time. However, members in that role

should act in the same manner. The outlier detection techniques can only be used to determine whether the user behaviour is normal or anomalous. N-median outlier detections algorithm [25] is used for this purpose. The datasets logon.csv, device.csv, file.csv, and LDAP.csv provided by the CERT organization [26] are considered for analyzing the user's activity behaviour using NMOD algorithm. N-median outlier detection is a statistical method used to identify outliers or anomalies in a dataset based on the median. Unlike traditional outlier detection methods that use mean and standard deviation, N-median outlier detection utilizes the median and other robust measures of central tendency and dispersion. A step-by-step procedure for N-median outlier detection:

- Compute the euclidian distance matrix for a role (D)
  Let us consider each member in a role is a data point (x_i, y_i), where i=1, 2, ….n. The Euclidian distance between (x_1, y_1) and (x_2, y_2) is:

$$\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (1)$$

- Calculate the median distance of each member in a role (M) and set the threshold value of that role.
  a) Arrange all the euclidian distances of a data point in the specified role in ascending order.
  b) Find the median distance of that data point in its role.
  c) The mean of the median distances of the data points is considered as the threshold value of that role group.
- Find the absolute deviation score (ADS) of a member
  The absolute difference between a median distance of a data point and role threshold.
  If M>T then ADS=|M-T|. Otherwise, ADS=0.
- Assign the priority level
  If ADS is 0 assign priority level as H.
  If ADS is 0<ADS<0.5 assign priority level as M.
  If ADS is >=0.5 assign priority level as L.

2.3. Role based access control model (RBAC)

According to the RBAC model users are assigned to the organizational roles based on their job functionalities. Each role is associated with specific permissions (e.g., read, write, update, delete, view) related to their job responsibilities. The requested user's role and its associated permissions to the requested resource are verified using RBAC model to allow access to the resources.

2.4. The process of user's request evaluation

The evaluation process starts by enforcing RBAC, ABAC, and TBAC models for preventing unauthorized access and leveraging zero-trust architecture within the organization. The detailed steps of this process is mentioned in Algorithm 1. The algorithm takes user's attributes, deviation score, role-permissions, and priority level as input to decide whether the requested permissions should be granted or rejected.

Algorithm 1. Policy check for access control

```
Input:
- user_attributes: User attributes including role, location, and resource sensitivity.
- requested_permission: The permission requested by the user.
- user_id_to_check: User ID for which deviation score is to be obtained.
- csv_file_path: Path to the CSV file containing deviation scores which are obtained by
analyzing the user behaviour using N-Median Outlier detection method
- required_priority: The required priority level for access.
Output:
- True if access is granted, False if access is denied.
Steps:
1. Retrieve Deviation Score and Determine User Priority:
- Call get_deviation_score_from_csv (user_id_to_check, csv_file_path) to obtain the
deviation score for the user.
- Call determine_user_priority(deviation_score) to determine the user's priority level
based on the deviation score.
2. Check Priority Using TBAC:
- Call PBAC.check_access (user_priority, required_priority) to verify if the user's
priority level allows the requested access.
3. Check Access Based on RBAC and ABAC Policies:
- Call rbac.check_permission(user_attributes["role"], requested_permission) to check RBAC
policy and see if the user's role allows the requested permission.
- Call abac. check_permission (user_attributes, requested_permission) to check ABAC policy
and see if the user's attributes allow the requested permission.
4. Access Decision:
```

```
- If all the access control mechanisms (TBAC, RBAC, and ABAC) grant access, return True
(access granted).
- If any of the mechanisms deny access, return False (access denied).
```

The evaluation engine checks the requested user's role and its permissions on the resource. If the user request is "access required to update the financial records for the Finance department". Financial records, the attributes userid, user job title, resource security level, time, location are verified with user attributes, and the requested user's deviation score and its priority level are verified with user priority level.

If role='finance department' AND resource='financial records' AND permission='update' are matched with the user-role and role-permission mappings according to RBAC, then the user is authorized based on RBAC rules. If userid='userid' AND job_title='finance manager' AND Time='systime' AND location='Remote' are matched with the ABAC policy, then the user's attributes are verified. The user's priority levels are evaluated using NMOD algorithm based on the user behaviour and assign with one of the priority levels 'L' (low), 'M' (medium) and 'H' (high) based on their deviation score. Decision engine allows the user to access the requested resource if the user's priority level is M or H.

To support the least privilege principle, permissions should be granted to users based on their roles in the organization to perform their tasks. The continuous monitoring aspect is related to tracking and analyzing user behaviour. The NMOD method is used to analyze the user behavior and to find the "deviation Score". The algorithm used deviation score of a user to determine the user's priority level. The result of the algorithm is stored in .csv file and that file can be accessed by get_deviation_score_from_csv function. Conditional access means granting or denying access based on certain conditions (e.g., time of day, location). The user's "location" and "resource_sensitivity" attributes are considered for conditional access. The proposed model using attributes such as "location" and "resource_sensitivity" for conditional access, and the "deviation score" obtained from user log activities can be interpreted as a form of continuous monitoring. Therefore, the proposed comprehensive access control model leverage the security principles of zero trust architecture.

3. RESULTS AND DISCUSSION

User request is processed to get the attributes from that request. The user request may contain the attributes user_id, role, time, location, resource and required operation on those resources. The user request is shown in the Figure 2.

```
# User attributes
user_attributes = {
    "role": "ITAdmin",
    "time": "9am-5pm",
    "location": "Office",
    "resource_sensitivity": "High",
}
requested_permission = "ManageITAssets"
user_id_to_check = 'FFT0048'
csv_file_path = '/content/Updated_devscore_ZTA.csv'
required_priority = 'H'
```

Figure 2. The details of user attributes and requested resource

The user_attributes and requested_permission are evaluated as per the ABAC policies defined for the organization. The role, and requested_permission are evaluated as per the RBAC policies. The user_id_to_check is the User ID for which deviation score is to be obtained. The deviation score of a user is calculated using NMOD and store it in devscore_ZTA.csv file. The merged dataset considered for calculating deviation score is shown in the Figure 3. It is obtained by merging logon.csv, device.csv, and LDAP.csv files. The logon.csv file contains login and logout of the system details, device.csv contains thumbdrive connectivity details, and LDAP.csv contains organization roles. The Figure 3 is a normalized merged dataset.

When NMOD algorithm applied on the data shown in the Figure 3, the deviation scores of users are obtained and stored in the devscore_ZTA.csv file which is shown in the Table 2. From the Table 2 it is observed that the user in the ITAdmin role with FFT0048 UserID having deviation score 0.02. That is the

priority level is 'M' but the required_priority level in the Figure 2 is H to access the 'ManageITAssets' resource. So, the permission for the user is denied. The same process will repeat for every user request.

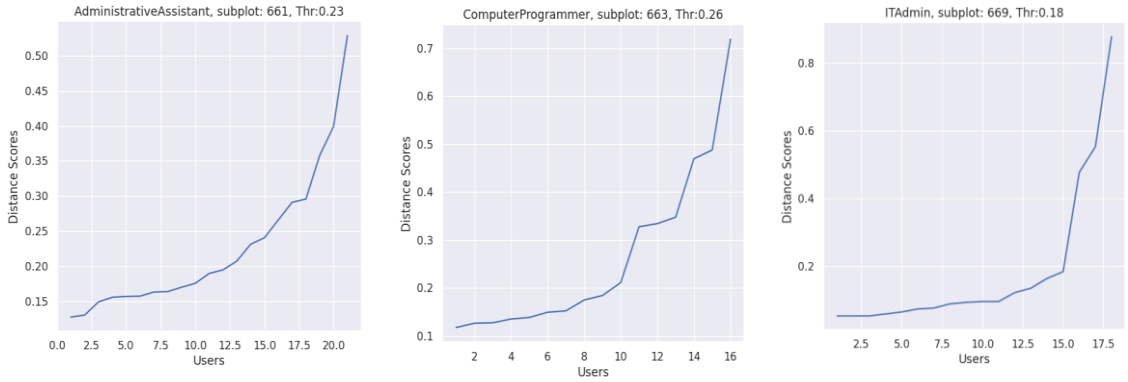
user	role	pc	date_only	hour_only	activity	Logoff_hour_only	Logon_hour_only	Timeduration
BCB0272	AdministrativeAssistant	1	9	2.166667	0.666667	0.333333	0.000000	0.333333
GHL0128	AdministrativeAssistant	1	16	2.028957	0.602080	3.591077	1.250000	2.943920
JBP0156	AdministrativeAssistant	1	17	2.498529	1.091410	4.400033	1.172604	3.551098
BVD2689	ComputerProgrammer	1	6	3.619392	0.408248	0.516398	0.547723	0.752773
CIB1224	ComputerProgrammer	1	7	2.760262	0.487950	0.000000	0.000000	0.000000
COL0740	ComputerProgrammer	1	19	2.734873	1.370107	5.639253	2.294157	4.280378

Figure 3. Merged dataset of user logon, device connectivity, and role details

Table 2. Sample user roles and their deviation score

User ID	Role	MedianDist	DevScore
GHL0128	Administrative assistant	0.19	0.06
PAB0200	Administrative assistant	0.10	0
RCA2575	Computer programmer	0.13	0.01
ITC0015	Director	0.25	0
MQW0054	Director	0.34	0.08
FFT0048	IT admin	0.05	0.02

The deviation score of each requested user is calculated using the NMOD procedure as mentioned in section3. First the eucleadian distance of a user with other users in his respective role. The median distance of each user is calculated and plotted as shown in the Figure 4. The mean of all these median distances is the thrshold value of that role group which is displayed on top of every role plot shown in Figure 4. The threshold value of the administrative assistant, computer programmer, and IT admin roles are 0.13, 0.11, and 0.04 which are shown in the Figures 4(a)-4(c). The x-axis of each graph is no.of users and y-axis is their median distance of each user in that role.



(a) (b) (c)

Figure 4. Threshold value of role groups (a) administrativeassistant (b) computerprogrammer, and (c) IT admin

The priority level of a requested user is obtained based on this deviation score which allows them for granting resource access. The priority level of a user is compared with the required_priority on the requested resource. If the user priority is greater than or equal to the required_priroty, then the function returns true otherwise returns false. All the details of the requested user are verified with the proposed comprehensive access control model to decide whether the permission to access the requested resource is to be allowed or denied. The implemented access control algorithm was tested using different user requests'scenarios. Table 3 shows a comparison of access decisions for different priority levels.

Table. 3 Comparison of access decisions for different priority levels

Scenario	User Id	User attributes	Expected access	Actual access	Pass/ fail
1	GHL0128	role: Administrative assistant, time: 9am-5pm, location: Office, resource_sensitivity: high, requested_permission: update financial records, required_priority: 'M', user_deviation score: 0.06	Access granted	Access granted	Pass
2	GHL0128	role: administrative assistant, time: 9am-5pm, location: Office, resource_sensitivity: low, requested_permission: update financial records, required_priority: 'H', user_deviation score: 0.06	Access denied	Access denied	Pass
3	ITC0015	role: director, time: 6pm-10pm, location: remote, resource_sensitivity: medium, requested_permission: manage employees, required_priority: 'H', user_deviation score: 0	Access granted	Access granted	Pass
4	FFT0048	role: IT admin, time: 9am-5pm, location: office, resource_sensitivity: High, requested_permission: manage IT assets, required_priority: 'M', user_deviation score: 0.02	Access granted	Access granted	Pass

The results are showing that the comprehensive access control model is able to check the user role permissions, user contextual situations, and user work behavior before granting access to resources. Therefore, the proposed model can leverage the ZTA security principles whereas individual models cannot do all as shown in the Table 4. The proposed model defined priority levels for TBAC model by analyzing user work behavior using NMOD algorithm whereas existing TBAC models [4]–[9] used risk factor which is calculated by considering the reviews/feedback from other users of the same role group or others. When employees in the organization working based on the job roles and in different locations, it is necessary to define the Priority levels based on the users'work behavior. So, the NMOD algorithm helps to clearly determine the deviation score of a user and then defined priority levels based on that.

Table 4 Comparison of access control models

Functionality	RBAC	ABAC	TBAC	Proposed model
Least privilege	Yes	No	No	Yes
Conditional access	No	Yes	No	Yes
Continuous monitoring	No	No	Yes	Yes

4. CONCLUSION

A comprehensive access control model is proposed for embracing the foundational principles of ZTA, namely least privilege, conditional access, and continuous monitoring. The proposed model unites established access control paradigms, incorporating RBAC, ABAC, and TBAC. The proposed model used N-median outlier detection technique to analyze the users'work behavior in their allotted role to define priority levels. The priority levels are used as a trust level in TBAC model and that are considered after verification of role and context values of a user to allow or deny the resource access. Different user request scenarios are verified using proposed model and identified that the obtained results are as expected results. This research not only conceptualizes the integrated access control model but also endeavours to evaluate its efficiency and effectiveness in comparison to existing access control models. By advancing access control mechanisms aligned with ZTA, this study aims to fortify organizational security and adapt to the evolving complexities of modern IT environments.

FUNDING INFORMATION

No funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Pattabhi Mary Jyosthna	✓	✓	✓		✓	✓		✓	✓		✓			
Konala Thammi Reddy	✓	✓		✓		✓				✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. There is no conflict of interest.

DATA AVAILABILITY

The data that support the deviation score findings of a user for this research are openly available at https://doi.org/10.1184/R1/12841247.v1.

REFERENCES

[1] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): a comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[2] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to zero trust architecture: reviews and challenges," *Security and Communication Networks*, vol. 2021, pp. 1–10, May 2021, doi: 10.1155/2021/9947347.

[3] M. Jouini, L. B. A. Rabai, and A. Ben Aissa, "Classification of security threats in information systems," *Procedia Computer Science*, vol. 32, pp. 489–496, 2014, doi: 10.1016/j.procs.2014.05.452.

[4] F. Fujun, L. Chuang, P. Dongsheng, and L. Junshan, "A trust and context based access control model for distributed systems," in *Proceedings - 10th IEEE International Conference on High Performance Computing and Communications, HPCC 2008*, IEEE, Sep. 2008, pp. 629–634. doi: 10.1109/HPCC.2008.37.

[5] E. Celikel, M. Kantarcioglu, B. Thuraisingham, and E. Bertino, "A risk management approach to RBAC," *Risk and Decision Analysis*, vol. 1, no. 1, pp. 21–33, 2009, doi: 10.3233/RDA-2008-0002.

[6] R. Yang, C. Lin, Y. Jiang, and X. Chu, "Trust based access control in infrastructure-centric environment," in *IEEE International Conference on Communications*, IEEE, Jun. 2011, pp. 1–5. doi: 10.1109/icc.2011.5963329.

[7] V. Oleshchuk, "Trust-aware RBAC," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7531 LNCS, pp. 97–107, 2012, doi: 10.1007/978-3-642-33704-8_9.

[8] R. A. Shaikh, K. Adi, and L. Logrippo, "Dynamic risk-based decision methods for access control systems," *Computers and Security*, vol. 31, no. 4, pp. 447–464, Jun. 2012, doi: 10.1016/j.cose.2012.02.006.

[9] J. Ma, K. Adi, M. Mejri, and L. Logrippo, "Risk analysis in access control systems," in *PST 2010: 2010 8th International Conference on Privacy, Security and Trust*, IEEE, Aug. 2010, pp. 160–166. doi: 10.1109/PST.2010.5593248.

[10] N. Baracaldo and J. Joshi, "A trust-and-risk aware RBAC framework," in *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, New York, NY, USA: ACM, Jun. 2012, pp. 167–176. doi: 10.1145/2295136.2295168.

[11] A. Almehmadi and K. El-Khatib, "On the possibility of insider threat prevention using intent-based access control (IBAC)," *IEEE Systems Journal*, vol. 11, no. 2, pp. 373–384, Jun. 2017, doi: 10.1109/JSYST.2015.2424677.

[12] D. Zhang *et al.*, "Role-based log analysis applying deep learning for insider threat detection," in *Proceedings of the ACM Conference on Computer and Communications Security*, New York, NY, USA: ACM, Jan. 2018, pp. 18–20. doi: 10.1145/3267494.3267495.

[13] F. Shan, J. Liu, X. Wang, W. Liu, and B. Zhou, "A smart access control method for online social networks based on support vector machine," *IEEE Access*, vol. 8, pp. 11096–11103, 2020, doi: 10.1109/ACCESS.2020.2963932.

[14] S. Mehraj and M. T. Banday, "Establishing a zero trust strategy in cloud computing environment," in *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, IEEE, Jan. 2020, pp. 1–6. doi: 10.1109/ICCCI48352.2020.9104214.

[15] B. Chen *et al.*, "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021, doi: 10.1109/JIOT.2020.3041042.

[16] Q. Yao, Q. Wang, X. Zhang, and J. Fei, "Dynamic access control and authorization system based on zero-trust architecture," in *ACM International Conference Proceeding Series*, New York, NY, USA: ACM, Oct. 2020, pp. 123–127. doi: 10.1145/3437802.3437824.

[17] T. Dimitrakos *et al.*, "Trust aware continuous authorization for zero trust in consumer internet of things," in *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, IEEE, Dec. 2020, pp. 1801–1812. doi: 10.1109/TrustCom50675.2020.00247.

[18] X. Zhang, L. Chen, J. Fan, X. Wang, and Q. Wang, "Power IoT security protection architecture based on zero trust framework," in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP 2021*, IEEE, Jan. 2021, pp. 166–170. doi: 10.1109/CSP51677.2021.9357607.

[19] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting zero trust network architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, pp. 1309–1320, Nov. 2022, doi: 10.1016/j.egyr.2021.11.272.

[20] F. Federici, D. Martintoni, and V. Senni, "A zero-trust architecture for remote access in industrial IoT infrastructures," *Electronics (Switzerland)*, vol. 12, no. 3, p. 566, Jan. 2023, doi: 10.3390/electronics12030566.

[21] 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, doi: 10.1109/ticps.2023.3333850.

[22] S. Hong, L. Xu, J. Huang, H. Li, H. Hu, and G. Gu, "Sysflow: toward a programmable zero trust framework for system security," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2794–2809, 2023, doi: 10.1109/TIFS.2023.3264152.

[23] V. A. Stafford, "Zero trust architecture," *NIST Special Publication 800-207*, 2020, doi: 10.6028/NIST.SP.800-207.

[24] K. Delbene, M. Medin, and R. Murray, "The road to zero trust (security)," *Defense Innovation Board*, pp. 1–10, 2019, [Online]. Available: https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF

[25] P. M. Jyosthna and K. T. Reddy, "Threat analysis using n-median outlier detection method with deviation score," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, pp. 568–575, 2021, doi: 10.14569/IJACSA.2021.0120866.

[26] CERT, "Insider threat test dataset," Software engineering institute, carnegie mellon university, 2016, [Online]. Available: https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247/1?file=24844280.

BIOGRAPHIES OF AUTHORS

Mrs. Pattabhi Mary Jyosthna received B.Tech.(CSE), M.Tech.(CS) from JNTUH and Ph.D. in the department of computer science and engineering from GITAM University (Deemed to be University), Visakhapatnam, Andhra Pradesh. At present she is working as an assistant professor in the department of CSE at B.V.R.I.T, Narsapur, Hyd., Telangana and she has 19 years of teaching experience. Her research interests include information security, cloud computing, and machine learning. Life member of CSI. She can be contacted at email: jyosthna.p@bvrit.ac.in.

Dr. Konala Thammi Reddy received M.Tech (CST) from Andhra University and doctoral degree from JNTUH, in the area of data mining. Having 28 years of teaching and research experience with an expertise in artificial intelligence, data mining and security. Published good number of papers in the indexed journals. He is professor in the dept. of CSE and dean, school of engineering and sciences, GD Goenka University, G D Goenka Education City, Sohna Gurgaon Road, Sohna, Haryana. Life member of CSI, ISCA, IE, ISTE. He can be contacted at email: kthammi.reddy@gdgu.org.