British Journal of Computer, Networking and Information Technology
Volume 6, Issue 1, 2023 (pp. 20-34)
www.abjournals.org

COLLABORATIVE-BASED DYNAMIC TRUST MODEL FOR BRING-YOUR-OWN-DEVICE ACCESS CONTROL MANAGEMENT IN CLOUD ENVIRONMENT

Oluwafemi Oriola

Department of Computer Science, Faculty of Science, Adekunle Ajasin University.

E-mail: oluwafemi.oriola@aaua.edu.ng

Cite this article:

Oluwafemi Oriola (2023), Collaborative-Based Dynamic Trust Model for Bring-Your-Own-Device Access Control Management in Cloud Environment. British Journal of Computer, Networking and Information Technology 6(1), 20-34. DOI: 10.52589/BJCNIT-QAKC5NIJ

Manuscript History

Received: 2 June 2023

Accepted: 20 Aug 2023

Published: 13 Sept 2023

ABSTRACT: *The operation of bring-your-own-device (BYOD) in the cloud has not only opened cloud servers to more threats but inflicted additional costs on cloud security as it would have to monitor employee devices and their operations. Many organizations therefore have adopted zero trust scheme for BYOD access control management in cloud environment. However, zero trust model introduces extra cost and hostility against internal employees, who have a certain level of trust, as against outsiders. This paper posits that trust quantification for BYOD access control management should be determined by cloud service providers and employers in a dynamic and continuous manner based on session and information values. The paper therefore presents a collaborative-based dynamic trust model that fuses the perspectives of BYOD employer and cloud service provider agents (trustees) for BYOD Nodes (trustors) access control management. The trustees provide prior evidences about the BYOD requests from which plausible inferences are drawn. Three framing of trusts including employee, device and program trusts are formulated based on reliable trust metrics. Dempster-Shafer Belief Function is used to evaluate the belief scores of the trustors' requests from the probabilities assigned by the trustees. The model is applied to two BYOD nodes, with varying session and information values. The outcomes reveal that the collaborative-based dynamic trust model ensures reduced cost and improved usability compared to zero trust model.*

KEYWORDS: Cloud Services, Bring-your-own-device, Access Control Management, Trust Quantification, Dempster-Shafer Theory.

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

INTRODUCTION

Cloud service providers offer resources to clients using service oriented architecture, namely: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) systems (Almulla & Yeun, 2010). These have improved affordability, accessibility and management of valuable resources such as hardware, software, information and data. The service providers and the clients therefore ensure that they fulfil their parts of the service level agreements (SLA) as any event of violation may compromise their transactions.

The major form of risk to the cloud services are cyber threats, which exploitations against cloud servers have drastically increased in recent times. The Netskope Threat Labs reported that a higher number of cloud resources were targeted in 2022 than previous years (Netskope, 2022). SlashNext reported that the compromise was as a result of attacks via bring-your-own-device (BYOD), especially mobile devices (SlashNext, 2022). Specifically, BYOD contributed an additional 50% to phishing attacks in 2022.

Bring-your-own-device is an organizational scheme that allows employees to use their personal devices including personal computers, mobile phones and other personalized accessories to carry out corporate activities (Gökçe & Dogerlioglu, 2019). The system gained more popularity during the outbreak of COVID-19 when working from home increased. The advantages of the schemes include employees' convenience, work efficiency, cost saving as a result of employers' unlimited access to facilities, and improved productivity. As much as the system might be beneficial to the organizations and employees, the flexibility and weak control of the BYOD have exacerbated the risks of cyber threats, especially in cloud environments (SentryBay, 2022).

Cloud security governance involving BYOD clients deals with overseeing of client technologies and employee technologies and devices. It encompasses cloud security management practices such as access control management (Ramgovind et al., 2010; Almulla & Yeun, 2010; Iqbal et al., 2022 & Zhu et al., 2022), which ensures device security check, enforcement of access control policy, platform independence and security of access control policy (Almarhabi et al., 2018). In achieving these objectives, cloud security managers cooperate with the client organization and CIO without violating the SLA guiding the security management.

One of the popular ways employed in dealing with BYOD risks is zero trust security policy, which assigns zero trust value to all users, devices and activities initially and gives each of them access when the authentication and authorization standards are met (IBM, 2016). Anderson et al. (2022) and Alshomrani and Li (2022) have proposed zero trust architectures for BYOD access control management. However, zero trust policy conflicts organizational or corporate networks principle, where employees and devices might have a certain level of trusts. For example, long serving employees and known devices on the network should have higher trust than new employees or devices, otherwise hostility with negative consequence on the usability and operational cost might result. Thus, trust is temporal and session value should be a factor to consider its quantification.

In hybrid cloud networks, for instance, the cloud service providers have greater access on the public cloud than private cloud and vice versa for client organization. So the information available to them about the users varies, thereby affecting the trust values. Therefore, a reliable

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

trust model should be based on the information at the disposal of both trustees. The aim of this paper is thus to develop a collaborative-based dynamic trust model based on session and information values for BYOD access control management. The proposed architecture serves as precursor from which various levels of trusts, including zero trust, could be determined.

LITERATURE REVIEW

The review focuses on existing trust models that have been proposed for BYOD and cybersecurity environments.

Nwebonyi and Ani (2014) developed trust-aided dynamic access control approach. The system relied on probability density function to conjecture future action of nodes from their past interactions (interaction history). The permission decisions were taken when there was probability of safe interaction (trust) and denied when there was probability of unsafe interaction (mistrust). The decisions were taken at the entry points. The solution predicted malicious intents before propagation. A framework for access control in cloud-based BYOD was presented in Almarhabi et al. (2018). The proposed framework was based on a multi-agent system that was composed of client BYOD, user device, and security manager. The framework proposed was devoid of mobile device management, which achieved flexibility. By testing the framework with four use cases involving different combinations of trusted and untrusted users as well as trusted and untrusted devices, all attacks were detected.

Makokha et al. (2021) solved the problem of subjective assignment of weights, portability and exhaustive definition of states in cloud security management. The authors developed quality of service (QoS) trust model based on scalability, reliability, data integrity and turnaround efficiency with time over local and global trust states. The agents were said to be trustworthy if they transit from local to global trust states. The system validated both the offered services and customers' requirements by confidence interval. It relied on user reviews, like and dislike posts. Based on confidence interval of 95%, the model was applied to QoS results from Microsoft and Google cloud providers and the result showed trustworthiness of the providers. Anderson et al. (2022) proposed a comprehensive zero trust architecture for mobile device management in BYOD environment and prescribed language specification, enforcement architecture and continuous authentication and authorization. Alshomrani and Li (2022) presented a zero trust model for IoT edge device security on the cloud using function-based device continuous authentication. The system provided two means of authentication, namely static authentication at the entry and continuous authentication, to ensure the location of the device is not changed during the session. It used PUF based identifier for static authentication and wireless channel characteristics for continuous authentication.

The main limitation of the reviewed works is that much attention was not paid to collaboration and continuous authentication. The continuous authentication proposed by Alshomrani and Li (2022) focused on device authentication and neglected human and program authentication. The contributions of this paper include:

- development of collaborative-based trust quantification model involving cloud service provider and client organization perspectives.

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

- simulation of a continuous BYOD access control management framework involving employees, device and program authentication.

COLLABORATIVE-BASED DYNAMIC TRUST MODEL

This section describes the collaborative-based dynamic trust model for BYOD access control management in a cloud environment.

The framework for the collaborative-based dynamic trust model for BYOD access control management in a cloud environment is presented in Figure 1. It consists of BYOD nodes belonging to the employees, Client Network under the purview of the employers, Cloud Servers and resources provided by the cloud service provider, Probability Derivative Function that is used to determine the employer and service provider's probability of evidence, Dempster-Shafer Belief Function, and Combination and Trust Rating.

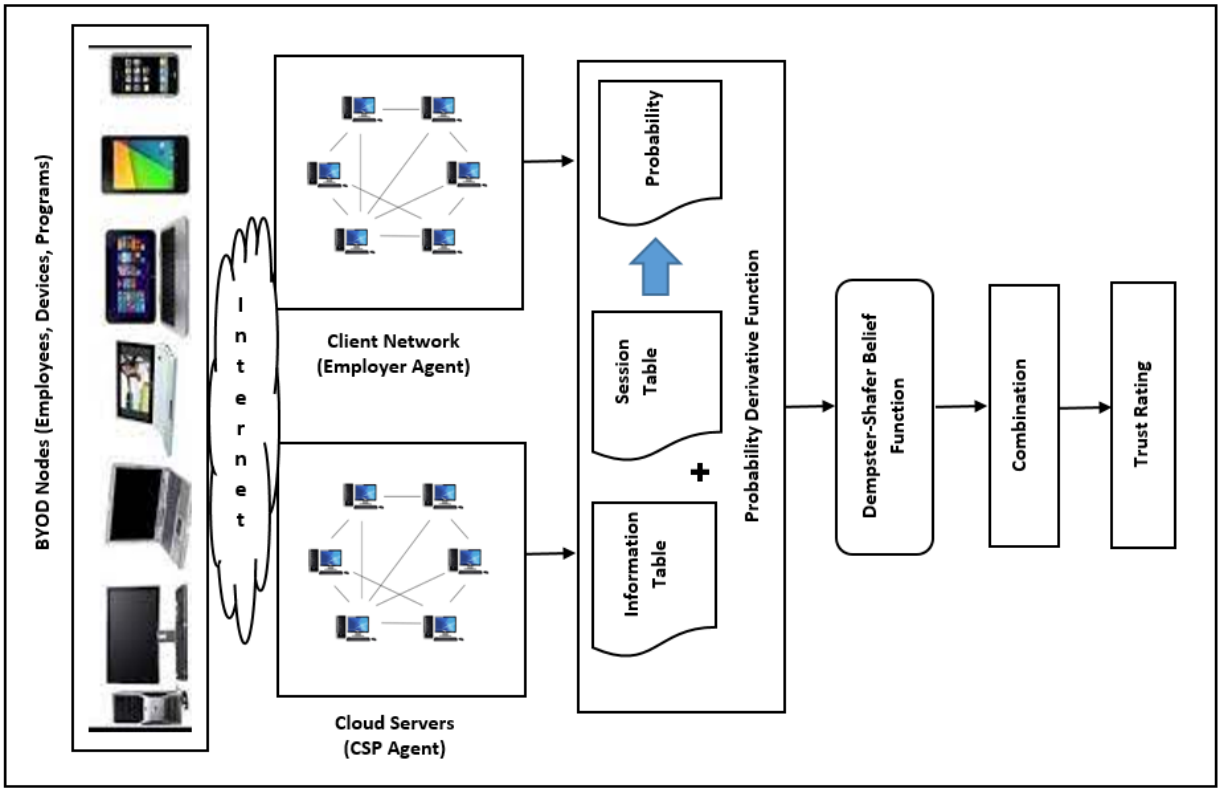


Figure 1: Framework for the collaborative-based dynamic trust model

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

BYOD Nodes

These consist of employees, personal devices and operating systems, and applications or programs that are used to request for services and implement corporate tasks on the client and cloud network. The devices may be mobile or desktop.

Client Network

The client network is the corporate or enterprise network system that houses the assets of the organization (employer) which is connected to BYOD nodes to perform corporate tasks. The assets include data center, internet service, and web resources, among others. The employer provides evidence about the employees' requests based on the information available to it. In this paper, the employer is referred to as Employer Agent (Emp. Agent).

Cloud Servers

These are the infrastructure, platform, software or web resources provided by cloud service providers either as public, private or hybrid cloud. The access privilege given to the clients depends on the cybersecurity governance policy and SLA. The cloud service provider provides evidence about the employees' requests based on the information available to it. In this paper, cloud service provider is referred to as CSP Agent.

Probability Derivative Function

The Employer Agent and CSP Agent provide permission status (evidence) about the employees' requests in relation to the the values of information and session in the information and session matrices (tables), respectively.

Given an Information System of 5 tuples (R, E, P, I, S), where R is the set of service requests (r_1, …, r_j), E is the set of evidences (e_1, …, e_k) about the service requests, P is the set of probabilities for the respective evidences (p_1, …, p_l), I is the table of information on the trust indicators about the respective evidences organized into matrix (i_{11}, …, i_{km}) and S is the table of sessions about the respective evidences organized into matrix (s_{11}, …, s_{kn}). Dempster-Shafer Belief Function, M, is applied to combine the probabilities of the observations (evidences) from the Employer Agent and CSP Agent to obtain the posterior probability, C.

$$C = M(P, E) \quad (1)$$

Such that

$$P = \sum i + \sum s \quad (2)$$

$\sum i \leq 0.5$ and $i \geq 0$;

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

$\sum s \leq 0.5$ and $s \geq 0$; and

$0 \leq p \leq 1$

For all

$r \epsilon R$

Dempster-Shafer Belief Function

The measure of Belief is derived from the combined basic assignments of the mass function (M). The Dempster-Shafer Rule of Combination ($M_{12\ldots n}$) is calculated from the aggregation of probability assignment functions M_1, M_2, … , M_n as presented in (6) - (10). The numerator represents the accumulated evidence for the sets *B, C, …, Z*, which supports the hypothesis *A*, and the denominator is the sum of the amount of conflict among the sets.

$$M_{12\ldots n} = M(A) \quad (3)$$

When $A \neq \emptyset$; (4)

and $M_{12\ldots n}(\emptyset) = O$ (5)

$$M(A) = \frac{\sum_{B\cap C\ldots\cap Z=A} M_1(B)M_2(C)\ldots M_n(Z)}{1-K} \quad (6)$$

$$K = \sum_{B\cap C\ldots\cap Z=\emptyset} M_1(B)M_2(C)\ldots M_n(Z) \quad (7)$$

where *B, C, A* $\underline{C}$ A. M are the mass functions. A is the hypothesis.

In Table 1, the various trust metrics (Oriola et al., 2020) and their respective probability range based on employee, device and program are presented.

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

Table 1: Trust Indicators and Description

Perspectives	Metric	Description	Probability Range
Employee	1. Integrity (HI)	It is defined as the extent to which a trustor is believed to adhere to ethical principles.	0 to 1
	2. Ability (HA)	It captures the "can-do" component of trustworthiness by describing whether the trustor has the skills needed to act in an appropriate fashion.	0 to 1
	3. Benevolence (HB)	It is the extent to which a trustor is believed to want to do good for the trustor.	0 to 1
	4. Trust Propensity (HP)	It is the dispositional trust that is associated to what the trustor 'will do' instead of 'can do'.	0 to 1
Device OS	5. Confidentiality (CC)	It measures the state of OS in ensuring that only those with sufficient privileges and demonstrated need access certain information.	0 to 1
	6. Integrity (CI)	It is the state of wholeness of OS.	0 to 1
	7. Availability (CA)	It measures the state of OS in ensuring uninterrupted user access.	0 to 1
Program Vulnerability Source	8. Integrity (II)	This is the measure of the condition of vulnerability source to produce the right output.	0 to 1
	9. Comprehension (IC)	This is the measure of the condition of vulnerability source to produce understandable outputs.	0 to 1
	10. Reliability (IR)	This is the measure of the condition of vulnerability source to always produce the right output.	0 to 1

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

Combination

The belief scores for the respective evidences of a request are factorized to obtain the realistic posterior probability (M_i).

We define trust, T, as the average of the posterior probabilities for request, r.

$$T = \frac{\sum_{i=1}^{10} M_i}{10} \quad (8)$$

since the indicators are 10.

Trust Rating

The obtained trust, T_r, for all the requests are rated according to access status in descending order such that the set of requests with the highest trust values have the highest rating, while the set of requests with the lowest trust values have the lowest rating.

CONTINUOUS BYOD ACCESS CONTROL MANAGEMENT

Use Cases

ABC is a telecom company with many agents, which registers new customers and attends to customer complaints using a public cloud-based telecom customer service app. The agent manager is responsible for receiving the daily report of agents and transmitting it to the management information system. In the experimental analysis, two use cases are simulated and evaluated.

i. **BYOD Node 1:** This has employee 1 with five years' experience as the customer service agent in the organization. He operates with personal Ubuntu Linux (device 1);

ii. **BYOD Node 2:** This has employee 3, with two years' experience as the customer service agent in the organization. He operates with Windows 2012 (device 2).

The services offered by cloud servers include:

i. **Open Portal:** The service is used to gain public user-level access to the cloud-based telecom customer service app. Apart from authentication by hypertext transfer protocol, a minimum trust value of 0.1 must be met to access the service; otherwise, transfer to zero trust scheme.

ii. **Login:** This service provides privilege access to cloud-based telecom customer service portal resources such as registration, submit update, edit and close portal. After being successful with open portal and meeting username/password authentication and authorization requirements, a minimum trust value of 0.5 must be met to access the service; otherwise, transfer to zero trust scheme.

iii. **Registration:** This service provides access to the employees to add information to the web temporarily. After being successful with previous services, a minimum trust of 0.6 is needed

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

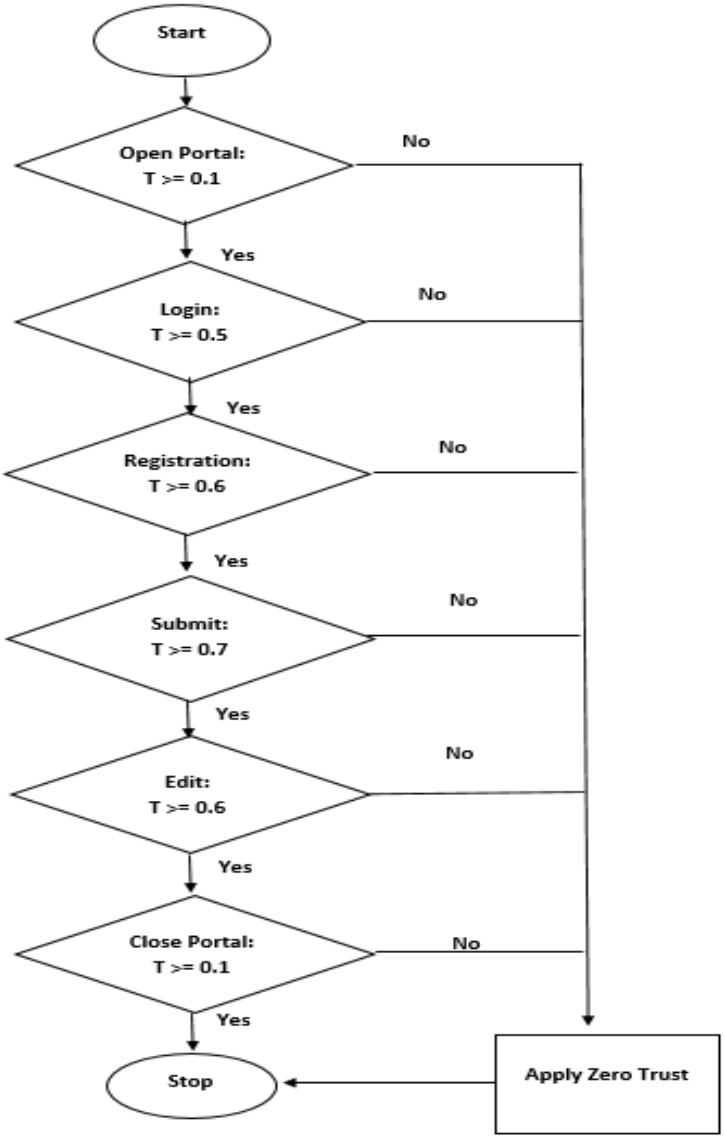
to accept new information and fetch information from other national databases; otherwise, transfer to zero trust scheme.

iv. **Submit:** The service provides privilege access to the employees to store registered information in the cloud database. After being successful with previous services, a minimum of 0.7 is needed to access the cloud database; otherwise, transfer to zero trust scheme.

v. **Edit:** The edit service is used to modify the records of customers in the database. The same requirements for registration are required; otherwise, transfer to zero trust scheme.

vi. **Close Portal:** The service is used to terminate the portal connection to the hypertext transfer protocol. The same requirements for open portal are required; otherwise, transfer to zero trust scheme.

The flowchart of the continuous BYOD access control management is presented in Figure 2.



Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

Figure 2: Flowchart of the continuous BYOD access control management

Analysis

Table 2 and Table 3 illustrate the probability (P) derived from information values (I) and session values (S) assigned by the Employer Agent and the CSP Agent for BYOD Node 1 and BYOD Node 2, respectively. The session values are directly proportional to duration of experience of the employees, while the information values are based on the level of information about nodes that is available to the agents. The information available to the CSP Agent about program vulnerability sources are slightly more than those available to the Employee Agent because the cloud service provider is more experienced and the servers run on public cloud.

Table 2: Trust Perspectives and Assigned Probability for BYOD Node 1

Perspective	Metric	Probability (Emp. Agent)			Probability (CSP Agent)		
		I	S	P	I	S	P
Employee	HI	0.1	0.5	0.6	0.2	0.5	0.7
	HA	0.2	0.5	0.7	0.2	0.5	0.7
	HB	0.0	0.5	0.5	0.2	0.5	0.7
	HP	0.2	0.5	0.7	0.2	0.5	0.7
Device	CC	0.0	0.5	0.5	0.0	0.5	0.5
	CI	0.0	0.5	0.5	0.0	0.5	0.5
	CA	0.0	0.5	0.5	0.0	0.5	0.5
Program Vulnerability Source	II	0.3	0.5	0.8	0.4	0.5	0.9
	IC	0.2	0.5	0.7	0.3	0.5	0.8
	IR	0.1	0.5	0.6	0.3	0.5	0.8

Table 3: Trust Perspectives and Assigned Probability for BYOD Node 2

Perspective	Metric	Probability (Emp. Agent)			Probability (CSP Agent)		
		I	S	P	I	S	P
Employee	HI	0.1	0.2	0.3	0.2	0.2	0.4
	HA	0.2	0.2	0.4	0.2	0.2	0.4
	HB	0.1	0.2	0.3	0.2	0.2	0.4
	HP	0.2	0.2	0.4	0.2	0.2	0.4
Device	CC	0.1	0.2	0.3	0.2	0.2	0.4
	CI	0.1	0.2	0.3	0.2	0.2	0.4
	CA	0.1	0.2	0.3	0.2	0.2	0.4
Program Vulnerability Source	II	0.3	0.2	0.5	0.4	0.2	0.6
	IC	0.2	0.2	0.4	0.3	0.2	0.5
	IR	0.1	0.2	0.3	0.3	0.2	0.5

In Table 4 and Table 5, the belief values for the various hypotheses and the posterior probability values are presented as obtained from Equation (6) - (7). In both tables, same outcomes result where the evidences presented by the Agents are same. Also, same outcomes result where the evidences are contradictory. The hypotheses with the highest belief scores are used to derive

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

the posterior probability. However, null posterior probability value is inferred where neither of the agents produces the highest belief scores.

Table 4: Results of Dempster-Shafer Belief Function for BYOD Node 1

Request	Evidence	Metric	Belief (Emp. Agent)	Belief (CSP Agent)	Belief (Neither)	Posterior Probability
Open Portal	Same	HI	0.6	0.7	0.12	0.88
		HA	0.7	0.7	0.09	0.91
		HB	0.5	0.7	0.15	0.85
		HP	0.7	0.7	0.09	0.91
		CC	0.5	0.5	0.25	0.75
		CI	0.5	0.5	0.25	0.75
		CA	0.5	0.5	0.25	0.75
		II	0.8	0.9	0.02	0.98
		IC	0.7	0.8	0.06	0.94
		IR	0.6	0.8	0.08	0.92
Login	Same	HI	0.6	0.7	0.12	0.88
		HA	0.7	0.7	0.09	0.91
		HB	0.5	0.7	0.15	0.85
		HP	0.7	0.7	0.09	0.91
		CC	0.5	0.5	0.25	0.75
		CI	0.5	0.5	0.25	0.75
		CA	0.5	0.5	0.25	0.75
		II	0.8	0.9	0.02	0.98
		IC	0.7	0.8	0.06	0.94
		IR	0.6	0.8	0.08	0.92
Registration	Contradict	HI	0.18	0.28	0.12	0.48
		HA	0.21	0.21	0.09	0.41
		HB	0.15	0.35	0.15	0.54
		HP	0.21	0.21	0.09	0.41
		CC	0.25	0.25	0.25	0.33
		CI	0.25	0.25	0.25	0.33
		CA	0.25	0.25	0.25	0.33
		II	0.08	0.18	0.02	0.64
		IC	0.14	0.24	0.06	0.55
		IR	0.12	0.32	0.08	0.62
Submit	Contradict	HI	0.18	0.28	0.12	0.48
		HA	0.21	0.21	0.09	0.41
		HB	0.15	0.35	0.15	0.54
		HP	0.21	0.21	0.09	0.41
		CC	0.25	0.25	0.25	0.33
		CI	0.25	0.25	0.25	0.33
		CA	0.25	0.25	0.25	0.33
		II	0.08	0.18	0.02	0.64
		IC	0.14	0.24	0.06	0.55

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

		IR	0.12	0.32	0.08	0.62
Edit	Same	HI	0.6	0.7	0.12	0.88
		HA	0.7	0.7	0.09	0.91
		HB	0.5	0.7	0.15	0.85
		HP	0.7	0.7	0.09	0.91
		CC	0.5	0.5	0.25	0.75
		CI	0.5	0.5	0.25	0.75
		CA	0.5	0.5	0.25	0.75
		II	0.8	0.9	0.02	0.98
		IC	0.7	0.8	0.06	0.94
		IR	0.6	0.8	0.08	0.92
Close Portal	Contradict	HI	0.18	0.28	0.12	0.48
		HA	0.21	0.21	0.09	0.41
		HB	0.15	0.35	0.15	0.54
		HP	0.21	0.21	0.09	0.41
		CC	0.25	0.25	0.25	0.33
		CI	0.25	0.25	0.25	0.33
		CA	0.25	0.25	0.25	0.33
		II	0.08	0.18	0.02	0.64
		IC	0.14	0.24	0.06	0.55
		IR	0.12	0.32	0.08	0.62

Table 5: Results of Dempster-Shafer Belief Function for BYOD Node 2

Request	**Evidence**	**Metrics**	**Belief (Emp. Agent)**	**Belief (CSP Agent)**	**Belief (Neither)**	**Posterior Probability**
Open Portal	Contradict	HI	0.18	0.28	0.42	0
		HA	0.24	0.24	0.36	0
		HB	0.18	0.28	0.42	0
		HP	0.24	0.24	0.36	0
		CC	0.18	0.28	0.42	0
		CI	0.18	0.28	0.42	0
		CA	0.18	0.28	0.42	0
		II	0.2	0.3	0.2	0.33
		IC	0.2	0.3	0.3	0.38
		IR	0.15	0.35	0.35	0.41
Login	Same	HI	0.3	0.4	0.42	0.58
		HA	0.4	0.4	0.36	0.64
		HB	0.3	0.4	0.42	0.58
		HP	0.4	0.4	0.36	0.64
		CC	0.3	0.4	0.42	0.58
		CI	0.3	0.4	0.42	0.58
		CA	0.3	0.4	0.42	0.58
		II	0.5	0.6	0.2	0.8
		IC	0.4	0.5	0.3	0.7

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

		IR	0.3	0.5	0.35	0.65
Registration	Contradict	HI	0.18	0.28	0.42	0
		HA	0.24	0.24	0.36	0
		HB	0.18	0.28	0.42	0
		HP	0.24	0.24	0.36	0
		CC	0.18	0.28	0.42	0
		CI	0.18	0.28	0.42	0
		CA	0.18	0.28	0.42	0
		II	0.2	0.3	0.2	0.33
		IC	0.2	0.3	0.3	0.38
		IR	0.15	0.35	0.35	0.41
Submit	Same	HI	0.3	0.4	0.42	0.58
		HA	0.4	0.4	0.36	0.64
		HB	0.3	0.4	0.42	0.58
		HP	0.4	0.4	0.36	0.64
		CC	0.3	0.4	0.42	0.58
		CI	0.3	0.4	0.42	0.58
		CA	0.3	0.4	0.42	0.58
		II	0.5	0.6	0.2	0.8
		IC	0.4	0.5	0.3	0.7
		IR	0.3	0.5	0.35	0.65
Edit	Same	HI	0.3	0.4	0.42	0.58
		HA	0.4	0.4	0.36	0.64
		HB	0.3	0.4	0.42	0.58
		HP	0.4	0.4	0.36	0.64
		CC	0.3	0.4	0.42	0.58
		CI	0.3	0.4	0.42	0.58
		CA	0.3	0.4	0.42	0.58
		II	0.5	0.6	0.2	0.8
		IC	0.4	0.5	0.3	0.7
		IR	0.3	0.5	0.35	0.65
Close Portal	Same	HI	0.3	0.4	0.42	0.58
		HA	0.4	0.4	0.36	0.64
		HB	0.3	0.4	0.42	0.58
		HP	0.4	0.4	0.36	0.64
		CC	0.3	0.4	0.42	0.58
		CI	0.3	0.4	0.42	0.58
		CA	0.3	0.4	0.42	0.58
		II	0.5	0.6	0.2	0.8
		IC	0.4	0.5	0.3	0.7
		IR	0.3	0.5	0.35	0.65

Table 6 indicates the trust values for BYOD Node 1 and BYOD Node 2 as computed using Equation (8) and their rating and status. The rating and the status are based on the access control management requirements. A request that meets up with the requirement is rated ‘trusted’;

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

otherwise, it is 'suspicious'. The 'trusted' requests are granted access to the respective cloud services, while the 'suspicious' requests are transferred to the zero trust scheme for further security check.

Table 6: Trust Values, Rating and Status for BYOD Node 1 and BYOD Node 2

Request	BYOD Node 1			BYOD Node 2		
	Trust	Rating	Status	Trust	Rating	Status
Open Portal	0.86	Trusted	Successful	0.11	Trusted	Successful
Login	0.86	Trusted	Successful	0.63	Trusted	Successful
Registration	0.46	Suspicious	Successful	0.11	Suspicious	Successful
Submit	0.46	Suspicious	Apply Zero Trust	0.63	Suspicious	Apply Zero Trust
Edit	0.86	Trusted	Apply Zero Trust	0.63	Trusted	Apply Zero Trust
Close Portal	0.46	Trusted	Successful	0.63	Trusted	Successful

Table 6 shows that only two (2) out of six (6) requests are transferred to the zero trust model for further authentications in BYOD Node 1 and BYOD Node 2, while the remaining four are granted permission to the service requested, needing no further validation. By assigning costs to zero trust steps, for instance, the reduction of requests requiring zero trust validation from six (6) to two (2) requests means that operational cost is reduced drastically, which would improve profit margin. Also, the usability of the cloud system also improves as additional authentication is skipped by the 'trusted' nodes.

CONCLUSION

This paper has presented a collaborative-based dynamic trust model for BYOD access control management. The model addressed the problem of hostility against trusted BYOD nodes and high operational cost inflicted by zero-trust models in BYOD access control management. The main contributions of the study are development of a collaborative-based dynamic trust model for BYOD access control management, and implementation of continuous BYOD access control management framework involving employee, device and program authentication.

The collaborative-based dynamic trust model involved both employer and cloud service provider agents, who assigned probability values and estimated belief scores to BYOD nodes' requests using Dempster-Shafer Belief Function. The trust values for the requests as derived from the belief scores are scaled to rate the requests. The outcomes revealed that the proposed model reduced operational cost and improved usability of the cloud.

In the future, the efficiency of the collaborative-based dynamic trust model and zero trust model will be compared. Also, the implication of the proposed model on security will be evaluated.

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ

REFERENCES

Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. (2018). A Proposed Framework for Access Control in the Cloud and BYOD Environment. *International Journal of Computer Science and Network Security*, *18*(2), 144–152. https://doi.org/10.14569/IJACSA.2018.091026

Almulla, S., & Yeun, C. Y. (2010). Cloud computing security management. *IEEE*, *May*.

Alshomrani, S., & Li, S. (2022). PUFDCA : A Zero-Trust-Based IoT Device Continuous Authentication Protocol. *Wireless Communications and Mobile Computing*, *2022*(November), 1–9.

Anderson, J., Huang, Q., Cheng, L., & Hu, H. (2022). BYOZ : Protecting BYOD Through Zero Trust Network Security. *IEEE*, 1–8.

Gökçe, K. G., & Dogerlioglu, O. (2019). " Bring your own device " policies : Perspectives of both employees and organizations Recommended citation : " Bring your own device " policies : Perspectives of both employees and organizations Kevser Gülnur Gökçe Ozgur Dogerlioglu *. *Knowledge Management and E-Learning*, *11*(2), 233–246.

IBM. (2016). Ten rules for Bring Your Own Device (BYOD). *IBM Corporation*.

Iqbal, U., Tandon, A., Gupta, S., Yadav, A. R., Neware, R., & Gelana, F. W. (2022). A Novel Secure Authentication Protocol for IoT and Cloud Servers. *Wireless Communications and Mobile Computing*, *2022*(March).

Makokha, F., Chepken, C. K., & Opiyo, E. T. (2021). End User Centric Quantitative Trust Model in Cloud Computing. *American Journal of Computer Science and Engineering*, *7*(1), 1–7.

Netskope. (2022). Cloud and Threat Report: 2022 Year In Review. *Netskope Threat Labs*, 1–11. https://www.prnewswire.com/news-releases/netskope-threat-research-malware-delivering-cloud-apps-nearly-tripled-in-2022-301717314.html

Nwebonyi, N. F., & Ani, U. P. D. (2014). BYOD NETWORK : Enhancing Security through Trust – Aided Access Control Mechanisms. *International Journal of Cybersecurity and Digital Forensics*, *4*(1), 272–289.

Oriola, O., Adeyemo, A. B., & Papadaki, M. (2020). *A collaborative approach for national cybersecurity incident management*. 457–484. https://doi.org/10.1108/ICS-02-2020-0027

Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in cloud computing. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010, September 2010*. https://doi.org/10.1109/ISSA.2010.5588290

SentryBay. (2022). Prioritise Security to Successfully Deliver BYOD in a Zero Trust Framework in a Zero Trust Framework. *SentryBay*.

SlashNext. (2022). *Mobile BYOD Security Report*. SlashNext. https://slashnext.com/report-the-mobile-byod-security-report/

Zhu, X., Ren, Z., He, J., Ren, B., Zhao, S., & Zhang, P. (2022). LAAP : Lightweight Anonymous Authentication Protocol for IoT Edge Devices Based on Elliptic Curve. *Wireless Communication and Mobile Computing*, *2022*(September).

Article DOI: 10.52589/BJCNIT-QAKC5NIJ
DOI URL: https://doi.org/10.52589/BJCNIT-QAKC5NIJ