

უსაფრთხოებაზე ორიენტირებული კონფიდენციალურობის არქიტექტურა ციფრული წვდომის კონტროლის სისტემებისთვის AI ასისტენტის აღსრულებით

გრიგოლ მიქაძე
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
grigol.mikadze976@ens.tsu.edu.ge

ანოტაცია — ციფრული წვდომის კონტროლის სისტემები წარმოადგენს უსაფრთხოების კრიტიკულ ფენას, რომელიც უზრუნველყოფს ფიზიკური და ციფრული აქტივების დაცვას იდენტობაზე დაფუძნებული წვდომის რეგულირებით. ამ სისტემების მზარდი დამოკიდებულება ცენტრალიზებულ რწმუნებათა სიგელების საცავებსა და დეტალურ ღონისძიებების ლოგირებაზე მათ აქცევს არასწორი გამოყენების, მონაცემთა გაჟონვისა და შიდა ბოროტად გამოყენების მიმზიდველ სამიზნედ. შესაბამისად, ძლიერი უსაფრთხოების გარანტიების უზრუნველყოფა წარმოადგენს კონფიდენციალურობის ეფექტური დაცვის წინაპირობას.

ნაშრომი სთავაზობს უსაფრთხოებაზე ორიენტირებულ არქიტექტურულ მოდელს, რომელიც კონფიდენციალურობის დაცვის მექანიზმებს უშუალოდ ციფრული წვდომის კონტროლის სისტემების ბირთვში აერთიანებს. შემოთავაზებული არქიტექტურა პრიორიტეტს ანიჭებს რწმუნებათა სიგელების უსაფრთხო მართვას, კონტროლირებულ მონაცემთა ნაკადებსა და გამძლე ლოგირების მექანიზმებს, ხოლო ხელოვნურ ინტელექტს იყენებს როგორც დამხმარე ფენას უსაფრთხოების მონიტორინგისა და პოლიტიკის აღსრულების გასაძლიერებლად. AI-ის მეთოდები გამოიყენება ანომალიების გამოვლენის, კონტექსტზე დაფუძნებული რისკის შეფასებისა და კონფიდენციალურობაზე ორიენტირებული უსაფრთხოების პოლიტიკების ადაპტიური აღსრულებისთვის.

ნაშრომში წარმოდგენილია ძირითადი არქიტექტურული პრინციპები, კონფიდენციალურობის გამაძლიერებელი ტექნოლოგიების (PETs) ინტეგრაციის გზები და შეფასების მეტრიკები, რომლებიც ერთობლივად უზრუნველყოფს უსაფრთხოების გამძლეობას, რეგულაციურ შესაბამისობასა და ოპერაციულ ეფექტიანობას. AI-ის დამხმარე უსაფრთხოების მექანიზმად პოზიციონირებით — და არა ძირითადი გადაწყვეტილების მიმღებად — შემოთავაზებული ჩარჩო უზრუნველყოფს მასშტაბირებად, ადაპტიურ და აუდიტირებად დაცვას როგორც წვდომის მთლიანობის, ისე პერსონალური მონაცემების მიმართ.

საკვანძო სიტყვები — წვდომის კონტროლის სისტემები, უსაფრთხო არქიტექტურა, მონაცემთა კონფიდენციალურობა, ხელოვნური ინტელექტი, Privacy-by-Design, ადაპტიური უსაფრთხოება, კონფიდენციალურობის გამაძლიერებელი ტექნოლოგიები, ანომალიების გამოვლენა