SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL8 No1
MARCH 2024

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 1 – 13 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

ახალი პოსტკვანტური ციფრული ხელმოწერა ვერკლის ხისა და ლატისების გამოყენებით

NOVEL POST-QUANTUM DIGITAL SIGNATURE USING VERKLE TREES AND LATTICES

Maksim Iavich[1], Tamari Kuchukhidze[2], Avtandil Gagnidze[3]

[1] Department of Computer Science, Caucasus University, 0102, Georgia
[2] Department of Computer Science, Caucasus University, 0102, Georgia
[3] East West University, Tbilisi, Georgia

რეზიუმე: ბოლო წლებში კვანტურ კომპიუტერებზე კვლევები მნიშვნელოვნად განვითარდა. თუ კაცობრიობა ოდესმე შექმნის ეფექტურ კვანტურ კომპიუტერს, არსებული საჯარო გასაღების უმეტესი კრიპტოსისტემა შეიძლება დაზარალდეს. ეს კრიპტოსისტემები დღსდღეობით გვხვდება ბევრ კომერციულ პროდუქტში. ჩვენ შევიმუშავეთ შედეგები, რომლებიც, როგორც ჩანს გვიცავს კვანტური შეტევებისგან, მაგრამ ისინი სახიფათო და არაეფექტურია ყოველდღიურ ცხოვრებაში გამოსაყენებლად. ნაშრომში გაანალიზებულია ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის მეთოდები. შეფასებულია მერკლის ხეზე დაფუძნებული ელექტრონული ხელმოწერა. ვერკლის ხის და ვექტორული ვალდებულებების გამოყენებით ნაშრომი იკვლევს ახალ იდეებს.
ამ სტატიაში წარმოვადგენთ უნიკალურ ტექნოლოგიას, პოსტკვანტური ციფრული ხელმოწერის სისტემის შემუშავებისთვის ვიყენებთ უახლეს ვერკლის ხეს. ამ მიზნისთვის გამოიყენება ვერკლის ხე, ვექტორული ვალდებულებები და ისეთი ვექტორული ვალდებულებები, რომლებიც დაფუძნებულია ლატისებზე, პოსტკვანტური თვისებებისთვის. ნაშრომში ასევე მოცემული პოსტკვანტური ხელმოწერის დიზაინის ცნებები ვერკლის ხის გამოყენებით.

საკვანძო სიტყვები: კვანტური კრიპტოგრაფია, ვექტორული ვალდებულებები, ლატისებზე დაფუძნებული ვექტორული ვალდებულებები, ვერკლის ხე, კრიპტოგრაფიული გამოყენება.

ABSTRACT: Research on quantum computers has advanced significantly in recent years. If humanity ever creates an effective quantum computer, many of the present public key cryptosystems can be compromised. These cryptosystems are currently found in many commercial products. We have devised solutions that seem to protect us from quantum attacks, but they are unsafe and inefficient for use in everyday life. In the paper, hash-based digital signature techniques are analyzed. Merkle tree based digital signature is assessed. Using a Verkle tree and vector commitments, the paper explores the novel ideas.
The authors of this article present a unique technology for developing a post-quantum digital signature system using state-of-the-art Verkle tree technology. Verkle tree, vector commitments, and vector commitments based on lattices for post-quantum features are used

for this purpose. The concepts of post-quantum signature design utilizing Verkle Tree are also provided in the paper.

Keywords: quantum cryptography; vector commitments; lattice-based vector commitments; Verkle tree; cryptographical application.

1. შესავალი

მოსალოდნელია, რომ კვანტური გამოთვლები მომავალში უფრო გავრცელდება, რაც გამოიწვევს პოსტკვანტური კრიპტოგრაფიის განვითარებას, ტექნიკას, რომელიც იცავს კვანტური კომპიუტერების თავდასხმებისგან. კვანტურ კომპიუტერებს შეუძლიათ უფრო სწრაფად შეასრულონ რთული გამოთვლები, ვიდრე ჩვეულებრივი კომპიუტერები. კვანტური კომპიუტერი ასრულებს დავალებებს რამდენიმე წამში, ხოლო კლასიკურ კომპიუტერს რამდენიმე წელი სჭირდება. კვანტურმა კომპიუტერმა შეიძლება დაარღვიოს სტანდარტული კრიპტო სისტემების უმეტესობა, თუ არა ყველა, რომელიც ამჟამად ვიყენებთ პრაქტიკაში [1-2].

RSA-ზე დაფუძნებული სისტემებს, რომლებსაც ფართოდ ვიყენებთ კომერციულ პროდუქტებსა და აპლიკაციებში, ემუქრებათ გატეხვა პოსტკვანტურ კრიპტოსისტემებში. RSA სისტემების ალტერნატივები, როგორიცაა ჰეშირებაზე დაფუძნებული ხელმოწერის სქემები, შემოთავაზებულია, მაგრამ არ არის პრაქტიკული უსაფრთხოების ან ეფექტურობის გამო. ამ სისტემების უსაფრთხოება დამოკიდებულია ჰეშირების ფუნქციის უნარზე, წინააღმდეგობა გაუწიოს შეჯახებებს ანუ კოლიზიებს [3].

უსაფრთხო პოსტკვანტური კრიპტოსისტემების შემუშავება და დანერგვა შრომატევადი პროცესია. როგორც კი კვანტური გამოთვლები გავრცელდება, RSA და სხვა ასიმეტრიული ალგორითმები ვეღარ შეძლებენ პირადი მონაცემების დაცვას. მიზანია შექმნას RSA კრიპტოსისტემის შემცვლელები, რომლებსაც გაუძლებენ კვანტური კომპიუტერის შეტევებს, როგორიცაა ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერის სქემები, რომლებიც უსაფრთხოა კრიპტოგრაფიული ჰეშირების ფუნქციების გამო [4].

ნაშრომში განხილულია ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სქემები მერკლის ხეების გამოყენებით, რომლებიც პოსტკვანტურია და შეუძლიათ წინააღმდეგობა გაუწიონ კვანტურ შეტევებს. თუმცა, ამ სქემებს აქვთ დიდი ხელმოწერის ზომები. NIST-მა მიიღო ჰეშირებაზე დაფუძნებული ციფრული ხელმოწერა SPHINC+, მაგრამ მას მაინც აქვს ეფექტურობის პრობლემები. ვერკლის ხეები, მერკლის ხეების განახლებული ვარიანტი გვთავაზობს უფრო ეფექტურ ვერიფიკაციის პროცედურებს, მხოლოდ არსებითი ინფორმაციის შენარჩუნებით. ეს ამცირებს შესანახ ადგილს ლოკალურ სივრცეში და შეუძლია მნიშვნელოვნად შეამციროს ხელმოწერის ზომა.

ნაშრომში წარმოდგენილია ახალი პოსტკვანტური ციფრული ხელმოწერის მოდელი, რომელიც იყენებს ვერკლის ხეებს. მოდელი დაფუძნებულია პოსტკვანტური თვისებების მქონე ლატისებზე დამყარებული ვექტორული ვალდებულებების გათვალისწინებით.

2. ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სქემები

ჰეშირებაზე დაფუძნებული ხელმოწერის სქემები არის კრიპტოგრაფიული მეთოდები, რომლებიც ქმნის ციფრულ ხელმოწერებს კრიპტოგრაფიული ჰეშირების ფუნქციების გამოყენებით. ამ სქემებს აქვთ უპირატესობა, რომ არ ეყრდნობიან მათემატიკურ სირთულეებს, როგორიცაა დიდი რიცხვების ფაქტორიზაცია ან ელიფსური მრუდის დისკრეტული ლოგარითმების ამოხსნა, შედეგად მათი გამოყენება შესაძლებელია პოსტკვანტურ ეპოქაში. NIST-მა აირჩია სამი ალგორითმი ციფრული ხელმოწერებისთვის, მათ შორის CRYSTALS-Dilithium, FALCON და SPHINCS+.

ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის მეთოდები მოიცავს გასაღების შექმნას, ხელმოწერის შექმნას და ხელმოწერის ვერიფიკაციას/გადამოწმებას. პირადი გასაღები წარმოიქმნება საიდუმლო გასაღების შემთხვევითი გენერირებით, რომელიც აუცილებლად დაცული უნდა იყოს. შემდეგ, კონკრეტული კომუნიკაციისთვის ხელმოწერის შესაქმნელად, შეტყობინებაზე ვმოქმედეთ საიდუმლო გასაღების და ჰეშის ფუნქციის განმეორებით გამოყენებით. მიმღები ადასტურებს ხელმოწერის ლეგიტიმურობას მესიჯის საჯარო გასაღებთან კონკატენაციით.

ჰეშირებაზე დაფუძნებულ ერთჯერადი ხელმოწერის მეთოდებს დიდი პოტენციალი გააჩნიათპოსტკვანტური ეპოქისთვის. განსაკუთრებით ისეთ სქემებს, რომლებიც ეყრდნობა კრიპტოგრაფიული ჰეშის ფუნქციების კოლიზიის მიმართ წინააღმდეგობას. ამის მაგალითია Lamport-Diffie ერთჯერადი ხელმოწერის (LDOTS) სქემა [6-7].

Lamport-Diffie ერთჯერადი ხელმოწერები იქმნება ცალმხრივი ფუნქციისა და კრიპტოგრაფიული ჰეშრების ფუნქციის გამოყენებით. გასაღების წყვილი გენერირდება n სიგრძის 2n ბიტის შემთხვევითი სტრიქონის გამოყენებით. LDOTS ხელმოწერის გასაღები X, არჩეულია შემთხვევით:

$$X = (x_{n-1}[0], x_{n-1}[1], \dots, x_1[0], x_1[1], x_0[0], x_0[1]) \epsilon R \{0,1\}^{(n,2n)} \quad (1)$$

Lamport-Diffie ერთჯერადი ხელმოწერის ვერიფიკაციის გასაღები არის Y, რომელიც გამოითვლება ფორმულა (2)–ის საშუალებით:

$$Y = (y_{n-1}[0], y_{n-1}[1], \dots, y_1[0], y_1[1], y_0[0], y_0[1]) \epsilon \{0,1\}^{(n,2n)} \quad (2)$$

გასაღების გამოთვლა ხორციელდება ცალმხრივი ფუნქციის f–ის გამოყენებით, როგორც ეს აღწერილია (3) ფორმულით:

$$y_i[j] = f(\ x_i[j]), 0 \le i \le n-1, j = 0,1. \quad (3)$$

ამიტომ, Lamport-Diffie-ის ერთჯერადი ხელმოწერის გასაღების გენერაცია მოითხოვს f-ის 2n შეფასებას. n სიგრძის 2n-ბიტიანი სტრიქონები ქმნიან ხელმოწერისა და ვერიფიკაციის გასაღებებს. თუ LDOTS ხელმოწერა გენერირებულია, დოკუმენტი $M \epsilon \{0,1\}^*$ ხელმოწერილია

LDOTS–ის გამოყენებით, X ხელმოწერის გასაღებით. M-ის შეტყობინების დაიჯესტი არის is $g(M) = d = (d_{n-1}, \dots, d_0)$. LDOTS ხელმოწერა არის $sign = (x_{n-1}[d_{n-1}], \dots, x_1[d_1], x_0[d_0]) \epsilon \{0,1\}^{(n,n)}$.

ამ ხელმოწერის ასაგებად გამოიყენება n ბიტიანი სტრიქონების სიგრძე. ეს სტრიქონები ირჩევა, როგორც d ფუნქცია შეტყობინებების შეჯამებისთვის/დაიჯესტისთვის. ჩვეულებრივი იმის გასაზომვა, თუ რამდენი კრიპტოგრაფიული ოპერაციების შესრულება შეუძლია CPU-ს ერთდროულად, არის ჰეშებზე დაკვირვება წამში [8].

Winternitz-ის ერთჯერადი ხელმოწერის სქემა (WOTS) რეკომენდებულია ხელმოწერების რაოდენობის შესამცირებლად. ჰეშირებაზე დაფუძნებული ერთჯერადი ხელმოწერის სტრუქტურები უზრუნველყოფს საიდუმლო გასაღების გამოყენებას მხოლოდ ერთხელ, ერთი ხელმოწერის შესაქმნელად, რაც საშუალებას გვაძლევს ელექტრონული ხელმოწერების სიზუსტეს და ლეგიტიმურობას. რეალური სამყაროში, ერთჯერადი ხელმოწერის მიდგომები არაეფექტურია, ამიტომ რალფ მერკლი გვირჩევს გამოიყენოს სრული ორობითი ჰეშირების ხე, რომ შევზღუდოთ ერთჯერადი ვერიფიკაციის გასაღებების თვითნებური რაოდენობის ავთენტურობა ერთი საჯარო გასაღებით.

3. მერკლის ხის ავთენტიფიკაციის სქემა

მერკლის ხის საშუალებით შეგვიძლია გადავწყვიტოთ მრავალრიცხოვანი დაიჯესტის (n) შენახვის პრობლემა ერთჯერადი ხელმოწერის სქემებისთვის, რადგან თითოეული შეტყობინება მოითხოვს სხვადასხვა გასაღების წყვილს. ეს სისტემა იყენებს ბინარულ ხის სტრუქტურას და კრიპტოგრაფიულ ჰეშირების ფუნქციას უსაფრთხო და სანდო ხელმოწერების შესაქმნელად. მერკლის იყენებს კრიპტოგრაფიულ ჰეშირების ფუნქციას g, $g : \{0,1\}^* \rightarrow \{0,1\}^n$ ნებისმიერი სიგრძის ორობითი სტრიქონს გადაიყვანს, n ფიქსირებული სიგრძის ორობით სტრიქონად. როდესაც ხელმომწერი ირჩევს $H \in \mathbb{N}$, სადაც $H \geq 2$, ქმნის მერკლის ხელმოწერის სქემის (MSS) გასაღებების წყვილს. შესაბამისად, იქმნება გასაღების წყვილი. ეს საშულებას გვაძლევს ხელი მოვაწეროთ და დავამოწმოთ 2^H დოკუმენტი. უნდა აღინიშნოს, რომ ეს მნიშვნელოვნად განსხვავდება ხელმოწერის პროტოკოლებისგან, როგორიცაა RSA და ECDSA, სადაც ერთი გასაღების წყვილი შეიძლება გამოვიყენოთ დიდი რაოდენობის დოკუმენტების ხელმოწერისთვის/დამოწმებისთვის. მიუხედავად ამისა, პრაქტიკაში, ეს მაჩვენებელი ასევე შეზღუდულია ხელმოწერის შესაქმნელად გამოყენებული ინსტრუმენტებით ან კონკრეტული შეზღუდვებით [9].

მერკლის ხე აგენერირებს გასაღების წყვილს თითოეული $0 \leq j < 2^H$ – თვის, რაც იძლევა 2^H დოკუმენტების ხელმოწერისა და ვალიდაციის საშუალებას. მერკლის ხის შიდა კვანძები განისაზღვრება ფორმულით, რომელიც უდრის მისი მარცხენა და მარჯვენა შვილების ჯამს. მერკლის ხის საფუძველი არის მერკლის ხელმოწერის სქემის (MSS) საჯარო გასაღები. 2^H ხელმოწერის გასაღებების სერია ქმნის MSS საიდუმლო გასაღებს [10].

მერკლის ხე წარმატებით იყენებს ერთჯერადი ხელმოწერის გასაღებებს ხელმოწერების გენერირებისთვის. ხელმომწერი ითვლის n-ბიტ $d = g(M)$, რისი საშუალებით ხელს აწერს

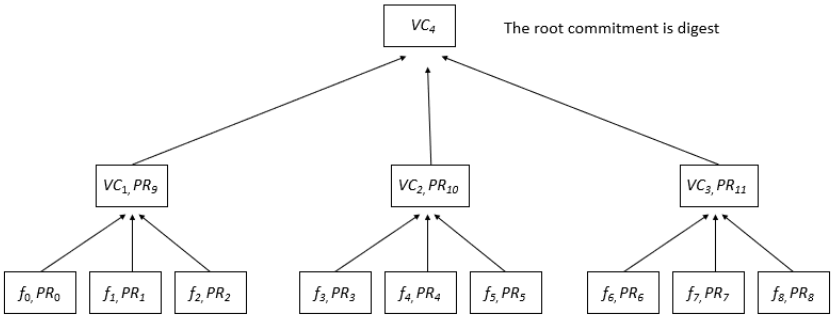
შეტყობინებას. შემდეგ ქმნის ერთჯერად ხელმოწერას $sign_{OTS}$, იყენებს s-ურ ერთჯერადი ხელმოწერის გასაღებს $X_s, s \in \{0, \dots, 2^H - 1\}$. რომ დავადასტუროთ Y_s, ხელმომწერი ამატებს ავთენტიფიკაციის გზას და ინდექს s–ს, ვერიფიკაციის გასაღებ Y_s –ს.

მერკლის ხეები გამოთვლა სწრაფად შეგვიძლია და მისი შექმნა შესაძლებელია O(n) დროში. თუმცა, ხის სიმაღლე უნდა იყოს n, თუ გვსურს ხელი მოვაწეროთ 2^n შეტყობინებას. ასევე, მერკლის მტკიცებულების ლოკალურად შენახვა არ არის პრაქტიკული და რთულია.

4. ვერკლის ხე

ვერკლის ხე მერკლის ხის მსგავსი სტრუქტურაა, რომელიც ეფექტურობით, მოქნილობითა და მასშტაბურობის თვალსაზრისით აღემატება მერკლის ხეს. ვერკლის ხის საშუალებით გვაქვს უფრო მცირე ვერიფიკაცია და უფრო ეფექტურია, ვიდრე მერკლის ხეები, რომლებიც მოითხოვს მეტ დამუშავებას და შესანახ ტევადობას, კრიპტოგრაფიული მონაცემების ზრდის გამო. ვერკლის ხე ამცირებს ზედმეტ მონაცემების დამუშავებას, რაც გამოწვეულია შუალედური კვანძების შენახვით. ის ამცირებენ შემოწმებისთვის საჭირო ჰეშის გამოთვლების რაოდენობას. ასევე აქვთ მასშტაბურობა, რაც შესაფერისს ხდის მასიური მონაცემთა ბაზების ეფექტურად მართვისთვის. შესაბამისად, ვერკლის ხე უფრო ეფექტულია შეზღუდული რესურსების მქონე აპლიკაციებისთვის [11].

ვერკლის ხის პირველადი მტკიცება არის ის, რომ ვექტორული ვალდებულებები შეიძლება გამოვიყენოთ კრიპტოგრაფიული ჰეშირების ფუნქციების ნაცვლად, რომელიც საჭიროა მერკლის ხის შესაქმნელად. ეს გულისხმობს ავირჩიოთ რაოდენობა რამდენ ნაწილად დაიყოფა ხე (k ნაწილი და ვექტორული ვალდებულება გამოვთვალოთ თითოეულ ნაწილზე. ვერკლის ხე საჭიროებს განსხვავებულ მიდგომას მტკიცებულების მიწოდების კუთხით, ეყრდნობა batching კვანძებს", რომელიც ამოწმებს რამდენიმე გზას ერთდროულად, რაც მნიშვნელოვნად ამცირებს ინფორმაციას, რაც საჭიროა მტკიცებულებების დასადგენად [12].



ფიგურა 1. ვერკლის ხე - $K = 3$

ვერკლის ხეებს არ სჭირდებად დედმამიშვილი კვანძებიც კი, განსხვავებით მერკლის ხისგან. ვერკლის ხეს დამტკიცებისთვის მხოლოდ გზა და მცირეოდენი დამატებითი ინფორმაცია სჭირდება.

ვერკლის ხე ითვლის შიდა კვანძს მისი შთამომავლისგან, ჰეშირების ალგორითმის გამოყენებით, რომელიც განსხვავდება ჩვეულებრივი ჰეშისგან. ამის ნაცვლად გამოიყენება ვექტორული ვალდებულება. ვერკლის ხის პირველადი განცხადება არის ის, რომ მერკლის ხე შეიძლება შეიქმნას თუკი კრიპტოგრაფიულ ჰეშირების ფუნქციას ჩავანაცვლებთ ვექტორული ვალდებულებებით. ვერკლის ხის საშუალებით შეგვიძლია მივაღწიოთ იგივე მიზანს, როგორც მერკლის ხის გამოყენებთ. მთავარი განსხვავება არის ის, რომ ახალი ვერკლის ხე ბევრად უფრო ეფექტურია.

5. ვექტორული ვალდებულება

ვალდებულების სქემები არის კრიპტოგრაფიული საფუძვლის მნიშვნელოვანი ნაწილი, რომლებიც საშუალებას გვაძლევს დავმალოთ მნიშვნელობა და მოგვიანებით გამოვაჩინოთ დამალული მნიშვნელობა. ვალდებულებების სისტემების ორი არსებითი მახასიათებელია დამალვა, რომელიც ავლენს მნიშვნელობას საჭიროების შემთხვევაში და შებოჭვა (binding), რომელიც ზღუდავს წვდომას სხვა მნიშვნელობებზე. ვექტორული ვალდებულებების (VC) სქემები აფართოებს ამ მახასიათებლებს მნიშვნელობების თანმიმდევრობების და პოტენციური ატრიბუტების დამალვის საშუალებით. ეს ართულებს ერთდროულად სხვადასხვა მნიშვნელობების გახსნას [13].

ვექტორული ვალდებულებები (Vector commitments) საჭიროა პოზიციის შებოჭისთვის, რადგან მოწინააღმდეგეს არ უნდა შეეძლოს ერთდროულად ორ სხვადასხვა მნიშვნელობის ღიად აღება (commit). ვალდებულების სტრიქონის სიგრძე და თითოეული გახსნის ზომა დამოუკიდებელი უნდა იყოს ვექტორის სიგრძისგან, რათა დააკმაყოფილოს კრიტერიუმები. ვექტორულ ვალდებულებებს შეიძლება ასევე დასჭირდეს უსაფრთხოების თვისება, როგორიცაა დამალვა, რომელიც ითვალისწინებს, რომ ძნელი უნდა იყოს დადგენა, იყო თუ არა ვალდებულება ვექტორიდან $(m_1, \dots, m_q)$, ან თუ ვექტორიდან $(m'_1, \dots, m'_q)$ [14].

გვაქვს შემდეგი ალგორითმები ვექტორული ვალდებულებებისთვის:

$\mathrm{Setup}(1^{\gamma}, 1^{\mathrm{d}})$ - ალგორითმი იღებს უსაფრთხოების პარამეტრს γ და მნიშვნელობა d–ს, როგორც შემომავალ მნიშვნელობას და აგენერირებს საჯარო კომიტერის (committer) პარამეტრებს cp და ვერიფიკატორის პარამეტრებს vp.

$\mathrm{Commit}(\mathrm{cp}, \mathrm{m} \in \mathrm{M}^{\mathrm{d}})$ - Committer პარამეტრების cp და შეტყობინების m, რომელიც მოცემულია M^{d} სივრციდან, გათვალისწინებით, ეს ალგორითმი გვაძლევს ვალდებულებას $\mathrm{c} \in \mathrm{Com}$ და კომიტერის მდგომარეობას st.

$\mathrm{Open}(\mathrm{cp}, \mathrm{st}, \mathrm{i} \in [\mathrm{d}])$ - კომიტერის პარამეტრების cp, კომიტერის მდგომარეობის st და i ინდექსის გათვალისწინებით d დიაპაზონიდან, ეს ალგორითმი გვაძლევს მტკიცებულებას pr_i–სშეტყობინების i-ურ ჩანაწერისთვის st.

$\mathrm{Verify}(\mathrm{vp}, \mathrm{c} \in \mathrm{Com}, \mathrm{i} \in [\mathrm{d}], \mathrm{m} \in \mathrm{M}, \mathrm{pr} \in \mathrm{Pr})$ – ეს ალგორითმი იღებს დამადასტურებელ პარამეტრებს vp, ვალდებულება c, ინდექსი i, შეტყობინება m და მტკიცებულება pr შემავალი მნიშვნელობების სახით და განსაზღვრავს თუ არა მტკიცებულება რეალური არის თუ არა.

თუ სქემა აკმაყოფილებს ზემოხსენებულ ინტერფეისებს, ის იძლევა მოდიფიკაციების განხორციელების საშუალებას committed შეტყობინების ვექტორში შესაბამისი ვალდებულების, მტკიცებულების და მდგომარეობის განახლებებით.

განახლების სქემის სისწორის პირობა იძლევა გარანტიას, რომ ორი ექსპერიმენტის შედეგი სტატისტიკურად იდენტურია ნებისმიერი პოლინომიური მნიშვნელობის d, კომიტერისა და გადამოწმების პარამეტრებისთვის, რომლებიც მოწოდებულია Setup-დან და შეტყობინებები m და m', რომლებიც განსხვავდებიან მაქსიმუმ j-ურ კოორდინატში. ვალდებულებისა და მტკიცებულების განახლებამ ეფექტურად უნდა უზრუნველყოს შედეგები, რომლებიც შედარებულია შეცვლილი შეტყობინების ვექტორზე ახალი ვალდებულებისა და მტკიცებულების შექმნასთან. შედეგების მდგომარეობის შესახებ ინფორმაციის ჩართვა შესაძლებელს ხდის კომპოზიციურობას, რაც იძლევა მრავალრიცხოვან განახლებებს ექსპონენციურ საზღვრებში.

კომპაქტური და ეფექტური გადაწყვეტილებები მნიშვნელოვნად აღემატება ადრინდელ კვლევებს ფუნდამენტური ვარაუდის „ხარისხის“, გენერირებული გადაწყვეტილებების ეფექტურობის ან ორივეს თვალსაზრისით. თუმცა, მნიშვნელოვანია, რომ მიდგომები, რომლებიც წარმოიქმნება, დაგვიცვას კვანტური კომპიუტერული გამოწვევებისგან [15]. კვანტურ კომპიუტერებს ამჟამად შეუძლიათ გატეხონ RSA-ზე და სხვა პოპულარულ ასიმეტრიულ სისტემებზე დაფუძნებული ვექტორული ვალდებულებები. იმისათვის, რომ უფრო ეფექტური და უსაფრთხო გახდეს, მკვლევარები აძლიერებენ ვალდებულებებს გისოსების ანუ ლატისების გამოყენებით და ხელმოწერის სისტემების შემუშავებით, რომლებიც გამოიყენებენ ვერკლის ხეებს. ჩვენთვის მნიშვნელოვანია გვქონდეს სქემები, რომლებიც დამოკიდებულია პოსტკვანტურ დაშვებებზე.

6. ლატისებზე დაფუძნებული ვექტორული ვალდებულება

ვექტორულ ვალდებულებებს გააჩნიათ მრავალი კრიპტოგრაფიული გამოყენება, როგორიცაა კრიპტოვალუტები, კრიპტოგრაფიული აკუმულატორები და დამოწმებული გარე მონაცემთა ბაზები. თუმცა, მცირედ გვაქვს გამოკვლეული პოსტ–კვანტური ვექტორული ვალდებულების სქემები, რომლებიც დაცულია კვანტური შეტევებისგან. პოსტ–კვანტური ჰეშირების ფუნქციით აშენებული მერკლის ხეები შეიძლება გამოვიყენოთ, მაგრამ მათზე გავლენა აქვს საჭირო და შედარებით არაეფექტურ განახლებებს.

ეს სტატია წარმოადგენს stateless, განახლებად VC სქემას მერკლის ხის მსგავსი კონსტრუქციიდათ, რომელიც დაფუძნებულია SIS გისოსების/ლატისების პრობლემაზე [16]. ეს ვექტორული ვალდებულება უფრო ეფექტურია და გააჩნია არსებითად უფრო მოკლე მტკიცებულებები. კერძო გასაღების კონფიგურაციით, საჯარო პარამეტრების გენერირება ხდება ცენტრალური ხელისუფლების მიერ მისი შეფერხების დრომდე.

სქემის კონსტრუქცია იყენებს ვექტორულ სივრცეს M, სადაც შეტყობინებები არის ℓ ვექტორები და მიეკუთვნება მიმდებარე მთელი რიცხვების I ინტერვალს. მთელი რიცხვების მაქსიმალური სიდიდე I–ში აღინიშნება, როგორც M_I. Setup ალგორითმი აგენერირებს committer და გადამოწმების პარამეტრებს cp და vp, შემთხვევითი მატრიცის გამოყენებით $\overline{\mathrm{A}} \leftarrow \mathbb{Z}_q^{n\times m}$; ასრულებს TrapGen ალგორითმს A და T მატრიცების მისაღებად. ალგორითმი აყალიბებს A_i მატრიცებს და შემთხვევით მატრიცას U, სადაც თითოეული U_j არის $\mathbb{Z}_q^{n\times\ell}$. $\mathrm{R}_{i,j}$ მატრიცები მიღებულია SamplePre ალგორითმის გამოყენებით, რაც უზრუნველყოფს, რომ $\mathrm{H}_d - \mathrm{H}_i$ არის ინვერსიული. Setup ალგორითმის გამომავალი მნიშვნელობა არის $cp = \left(\mathrm{U}, \mathrm{R} = \left(\mathrm{R}_{i,j}\right)_{i,j\in[d]}\right)$, $vp = (\mathrm{A}, \mathrm{U})$.

Committer და open ალგორითმები ითვლის ვალდებულებას, მტკიცებულებას და შესრულებული შეტყობინების მდგომარეობას. ვერიფიკაციის ალგორითმი ამოწმებს პირობებს $\|\mathrm{p}_i\| \le \gamma$, და $\mathrm{c} = \mathrm{A}_i\mathrm{p}_i + \mathrm{U}_i\mathrm{m}_i$, არის უსაფრთხოების პარამეტრი. თუკი პირობები დაკმაყოფილებულია, ალგორითმი მიიღებს მტკიცებულებას, წინააღმდეგ შემთხვევაში ის უარყოფს მას.

ჩვენ ასევე გვაქვს განახლების ალგორითმები ვალდებულებების, მტკიცებულებებისა და მდგომარეობის შესაცვლელად.

PrepareUpdates ^{diff} - ეს ალგორითმი იღებს committer პარამეტრებს cp, ინდექსს j და განსხვავებას $\sigma \in \mathbb{Z}^{\ell}$. იგი წარმოქმნის ვალდებულების განახლებას σ_{pr}, მტკიცებულების განახლებას σ_{pr}, და მდგომარეობის განახლებას σ_{s}. აუცილებელია შეიცვალოს შესრულებული შეტყობინების ვექტორი.

UpdateC - გადამოწმების პარამეტრების vp, ვალდებულების c და ვალდებულების განახლების σ_{c} გათვალისწინებით, ეს ალგორითმი დეტერმინისტულად ითვლის განახლებულ ვალდებულებას c'.

UpdateP - ვერიფიკაციის პარამეტრების vp, ინდექსი i, მტკიცებულება $\mathrm{pr_i}$ და მტკიცებულების განახლება σ_{pr}-ის გათვალისწინებით, ეს ალგორითმი დეტერმინისტულად წარმოქმნის განახლებულ მტკიცებულებას $\mathrm{pr}_{\mathrm{i}}'$.

UpdateS - მოცემული გვაქვს committer პარამეტრები cp, მისი მდგომარეობა st, და მდგომარეობის განახლება σ_{s}. ეს ალგორითმი დეტერმინისტულად აწარმოებს committer–ის განახლებულ მდგომარეობას st'.

განახლების ალგორითმები გარანტიას იძლევა სქემის სიზუსტის და უსაფრთხოების, რაც უზრუნველყოფს უსაფრთხო ვალდებულებას, მტკიცებულებების გახსნას, გადამოწმებასა და მოდიფიკაციებს შეტყობინებების committed ვექტორებისთვის.

7. ახალი სქემა ვერკლის ხის გამოყენებით

ერთჯერადი ხელმოწერის სქემების განხორციელება და გამოყენება რთულია, რადგან საჭიროა ცალკეული გასაღების წყვილების ხელმოწერის შექმნა თითოეული მესიჯისთვის. გვჭირდება შევინახოთ n დაიჯესტები, რაც რთულად გამოსაყენებელს ხდის ერთჯერად ხელმოწერის სქემებს. ამის გადასაჭრელად იყენებენ მერკლის ხეს. ეს მიდგომა ცვლის რამდენიმე ვერიფიკაციის გასაღებს ერთი საჯარო გასაღებით, ოროზითი ხის გამოყენებით, როგორც ფესვი. მერკლის ხე სწრაფად ითვლება და შეგვიძლია შევქმნათ დიდი მერკლის მტკიცებულებები, მაგრამ მათი გამოყენებით ჩვენს ლოკალურ სივრცეზე მნიშვნელოვანი დატვირთვა აქვს.

ვერკლის ხეები, რომლებიც იძლევა უფრო მცირე ზომის მტკიცებულების საშუალებას, შეგვიძლია გამოვიყენოთ მერკლის ხის მაგივრად. ის არის გაუმჯობესებული და უფრო ეფექტური. შემმოწმებელმა მხოლოდ უნდა წარმოადგინოს ერთი მტკიცებულება, რომელიც აჩვენებს ყველა მშობელსა და შვილს ურთიერთობას. ამან შეიძლება შეამციროს მტკიცებულების ზომები 6-8-ით და 20-30-ით ან მეტით, ვიდრე იდეალური მერკლის ხეები და მერკლის Patricia ხეები.

ჩვენ ვიყენებთ ვერკლის ხეს მერკლის ხის ნაცვლად. ხელმომწერი ირჩევს $H \in \mathbb{N}, H \geq 2$ გასაღების წყვილის ფორმირებისას. ამის შემდეგ გასაღების წყვილი იქმნება, რომელთა გამოყენებით შეგვიძლია ხელი მოვაწეროთ და დავამოწმოთ 2^H დოკუმენტი. ხელმომწერი გამოიმუშავებს 2^H უნიკალურ გასაღების წყვილს $(X_j, Y_j), 0 \leq j < 2^H$. ამ შემთხვევაში ხელმოწერის გასაღები არის X_j , ხოლო ვერიფიკაციიის გასაღები კი Y_j. ორივე მათგანი ბიტების სტრიქონებია. ვერკლის ხის ფოთლებია $g(Y_j)$, $0 \leq j < 2^H$. როგორც ხის ფოთლები, ისინი გამოითვლება და გამოიყენება, და ყოველი კვანძი არის ჰეშის მნიშვნელობა, რომელიც წარმოიქმნება მისი შთამომავლების ჰეშების შეერთებით. ვერკლის ხის ფესვი ვალდებულება კრიპტოგრაფიის სქემაში არის საჯარო გასაღები. საჯარო გასაღების შესაქმნელად საჭიროა გამოვიყენოთ 2^H უნიკალური გასაღების წყვილი.

ხელმოწერების შექმნა შეგვიძლია ერთჯერადი ხელმოწერის გასაღებების გენერირებით. სანამ M-იდან აღებულ შეტყობინებას მოვაწერთ ხელს, უნდა გამოვთვალოთ n ბიტიანი დაიჯესტი $d = g(M)$. პირველად, n ზომის შეტყობინება იქმნება m ზომის შემთხვევითი ზომის შეტყობინებისგან, ჰეშირების ფუნქციის გამოყენებით, კონვერტირებით. დოკუმენტის ხელმოწერა შეიქმნება ძირეული ვალდებულების, ერთჯერადი ხელმოწერის, ერთჯერადი გადამოწმების გასაღების და ბოლოს, მტკიცებულების ინდექსის s-ის კომბინაციით.

ვერკლის ხელმოწერის ვერიფიკაცია შემდეგნაირად მუშაობს: $sign$–ის ერთჯერადი ხელმოწერა უნდა იყოს დამოწმებული Y_s–ით. თუ ეს მართალია, the VC_i ვალდებულებები

დამოწმებულია. ხელმოწერა დადასტურებულია, თუ ხის ფესვი უდრის ფესვის ვალდებულებას. ვერკლის ხის გათვალისწინებით, ფესვის ვალდებულება არის d.

8. ექსპერიმენტები

მერკლის ხე არის ძალიან სწრაფი და $O(n)$ ცრის მისი გამოთვლითი დრო. სამწუხაროდ, მათი მტკიცებულების ზომა $O(\log_2 n)$ შედარებით დიდია და შეიძლება გამოიწვიოს მნიშვნელოვანი სიგანის (width) ხარჯი. მათი მტკიცებულებების ზომა $O(w \log_w n)$ რეალურად უფრო დიდია ვიდრე ისეთი მერკლის ხე, რომელსაც უფრო დიდი სიგანე გააჩნია (w-ary ხეები). ვექტორული ვალდებულების სქემის გამოყენება ამცირებს მტკიცებულების ზომას ფიქსირებულ მნიშვნელობამდე – $O(1)$. თუმცა, ვექტორული ვალდებულების კონსტრუქცია არის ძალიან ძვირი და შრომატევადი, რაც მოითხოვს $O(n^2)$ გამოთვლას.

ვერკლის ხის სიგანე (width) w, მოითხოვს მხოლოდ $O(wn)$ დროს კონსტრუქციისთვის. გარდა ამისა, მერკლის ხის წევრობის მტკიცებულებებთან შედარებით, მისი მტკიცებულების ზომა არის მხოლოდ $O(\log_w n)$, რაც მნიშვნელოვნად ნაკლებია $O(\log_2 w)$. ჩვენთვის ეს კარგი გაცვლაა.

სქემა	კონსტრუქცია	განახლება	მტკიცებულების ზომა
მერკლის ხე	$O(n)$	$O(\log_2 n)$	$O(\log_2 n)$
მერკლის ხე (w-ary)	$O(n)$	$O(w\log_w n)$	$O(w\log_w n)$
ვექტორული ვალდებულება	$O(n^2)$	$O(n)$	$O(1)$
ვერკლის ხე	$O(\mathrm{w}n)$	$O(w\log_w n)$	$O(\log_w n)$

ფიგურა 2. სქემის შედარება

როგორც ვთქვით, პოსტკვანტური ვექტორული ვალდებულების სქემები შეზღუდულად არის გამოკვლეული, მხოლოდ მერკლის ხის მსგავსი კონსტრუქციები გვაქვს stateless არმქონე განახლებულ VC სქემებისთვის. ეს მეთოდები გადამწყვეტია კვანტური კომპიუტერის შეტევებისგან დასაცავად, რადგან კვანტურ კომპიუტერებს შეუძლიათ გატეხონ RSA-ზე დაფუძნებული ვექტორული ვალდებულებები. ხელმოწერის ტექნიკა იყენებს ვერკლის ხეს, მაგრამ ვექტორული ვალდებულებები აგებულია გისოსების/ლატისების გამოყენებით. ასევე

გვაქვს სხვა, პოსტკვანტური მერკლის ალგორითმები, როგორიცაა Fractal Merkle ალგორითმი [17].

ამ შემთხვევაში, კლასიკური ალგორითმის შედეგებია:

გასაღების გენერირების დრო- 0.049351, ხელმოწერის დრო - 0.0002425, ვერიფიკაციის დრო - 0.0038651.

Thread-ზე დაფუძნებული ალგორითმი:

გასაღების გენერირების დრო - 0.013841, ხელმოწერის დრო - 0.0002425, ვერიფიკაციის დრო - 0.0038651.

ჩვენ შევიმუშავეთ ვექტორული ვალდებულების ახალი პროტოკოლი, რომელიც ეფუძნება პოსტკვანტურ Short Integer Solution ლატისების პრობლემას. პროტოკოლი საშუალებას გვაძლევს ვექტორული შეტყობინებები გადავამოწმოთ და გვქონდეს უსაფრთხო ვალდებულება, დაწყებული stateless განახლებადი VC კონსტრუქციით. ეს განსაკუთრებით შესაფერისია დიდი განზომილების d-სთვის, საჯარო პარამეტრების კვადრატული დამოკიდებულების გამო. ხის სპეციალიზებული ტრანსფორმაცია გათვალისწინებულია უფრო დიდი ზომებისთვის, stateless განახლებების შენარჩუნებით და ლაკონური მტკიცებულებების უზრუნველსაყოფად. მეთოდის მთავარი უპირატესობა არის თეორიული უსაფრთხოება კვანტური თავდასხმებისგან, მაგრამ მას აქვს ლოგარითმული ვალდებულების და მტკიცებულების ზომების შედარება ვექტორულ განზომილებაში d. მიუხედავად ამისა, ლატისებზე დაფუძნებული კონსტრუქცია მკაცრად არის გამოცდილი კლასიკური ალგორითმების წინააღმდეგ, რის შედეგადაც უფრო მცირე ციფრული ხელმოწერა მივიღეთ, ვიდრე მერკლის ხის ვერსიასთან შედარებით.

ჩვენ გამოვცადეთ ალგორითმი იმავე აპარატზე, სადაც გავტესტეთ ელექტრონული ხელმოწერა, რომელიც მერკლის ხის საფუძველზეა შექმნილი.

მივიღეთ შემდეგი შედეგები:

გასაღების გენერირების დრო - 0.049351, ხელმოწერის დრო - 0.00001520, ვერიფიკაციის დრო - 0.00048250.

ჩვენი ლატისებზე დაფუძნებული კონსტრუქცია, რა თქმა უნდა, უფრო ნელია, მაგრამ ჩვენს შემთხვევაში ელექტრონული ხელმოწერა გაცილებით მეტია, ვიდრე მერკლის ხის ვერსიის შემთხვევაში.

ჩვენი ახალი ვექტორული ვალდებულების კონსტრუქცია, რომელიც დაფუძნებულია პოსტკვანტურ Short Integer Solution ლატისების პრობლემაზე, წარმოადგენს რეალურ ალტერნატივას, განსაკუთრებით იმ სცენარებში, სადაც კვანტური უსაფრთხოება უმთავრესია. ვალდებულებისა და მტკიცებულების ზომებში ურთიერთდამოკიდებულება საგულდაგულოდ არის დაბალანსებული და ემპირიული შედეგები ხაზს უსვამს ჩვენი მიდგომის პრაქტიკულ სარგებელს.

9. დასკვნა

გამოვიკვლიეთ ინსტრუმენტებს კლასიკური და კვანტური კრიპტოგრაფიისთვის, მათ შორის პოსტკვანტური კრიპტოგრაფიის სისტემები, ჰეშირებაზე დაფუძნებული ცალმხრივი ფუნქციები და მათი ინტეგრაცია მერკლის და ვერკლის ხეებში. ასევე განვიხილეთ ვექტორული ვალდებულებები და ლატისებზე დაფუძნებულ ვალდებულებებს. ახალი სქემების ეფექტურობამ განაპირობა ახალი მოდელის შექმნა და მისი ინტეგრაცია ვერკლის ხეებში, რაც ეფექტრურობას ზრდის.

შედეგად მიღებულმა სქემებმა უნდა დაიცვან სისტემები, როგორც ტრადიციული, ასევე კვანტური კომპიუტერების თავდასხმებისგან. მერკლის ხე, აგებული კრიპტოგრაფიული ჰეშის ფუნქციებით, უზრუნველყოფს ძლიერ დაცვას კვანტური შეტევებისგან. ვერკლის ხის მოდელი, რომელიც წარმოადგენს მერკლის სქემის გაუმჯობესებას, იძლევა მცირე ვერიგიკაციის საშუალებას, გვაძლევს მხოლოდ ერთი მტკიცებულების მოთხოვნით ყველა მშობლისა და შთამომავლის ურთიერთობა დავადასტუროთ, ვერიფიკაციის ზომის ეს შემცირება დაახლოებით 6-8-ჯერ არის მერკლის ჩვეულებრივ მიდგომასთან შედარებით.

ვერკლის ხეს ვიყენებთ მერკლის ხის ნაცვლად. ეს გაუმჯობესებულია, რომელიც მოითხოვს ვექტორის ვალდებულებას, როგორც მტკიცებულებას. ხელმოწერის მეთოდები იყენებს ვერკლის ხეებს და სისტემები მოქმედებენ პოსტკვანტური ვარაუდებით. კვლევა მიზნად ისახავს სისტემის უფრო უსაფრთხო და ეფექტური გახადოს, რაც უზრუნველყოფს, რომ მიღებული მეთოდები დაგვიცავს კვანტური კომპიუტერის შეტევებისგან.

10. დადასტურება/აღიარება

კვლევა [STEM – 22 -1076] განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით.

ბიბლიოგრაფია

1. Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.
2. Buchmann, J., Dahmen, E., Szydlo, M. (2009). Hash-based Digital Signature Schemes. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_3
3. Biswas, Bhaskar, and Nicolas Sendrier. "McEliece cryptosystem implementation: Theory and practice." Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 Proceedings 2. Springer Berlin Heidelberg, 2008.
4. Yin, X.; He, J.; Guo, Y.; Han, D.; Li, K.-C.; Castiglione, A. An Efficient Two-Factor Authentication Scheme Based on the Merkle Tree. Sensors 2020, 20, 5735. https://doi.org/10.3390/s20205735
5. Chen, Y.-C.; Chou, Y.-P.; Chou, Y.-C. An Image Authentication Scheme Using Merkle Tree Mechanisms. Future Internet 2019, 11, 149. https://doi.org/10.3390/fi11070149
6. Lamport, Leslie. "Constructing digital signatures from a one way function.",1979.

7. Post-Quantum Digital Signatures with Attenuated Pulse Generator; M. Iavich, R. Bocu, A. Arakelian, G. Iashvili; ceur-ws.org, Vol-2698, 2020.
8. Koo, D.; Shin, Y.; Yun, J.; Hur, J. Improving Security and Reliability in Merkle Tree-Based Online Data Authentication with Leakage Resilience. Appl. Sci. 2018, 8, 2532. https://doi.org/10.3390/app8122532
9. Sim, M.; Eum, S.; Song, G.; Yang, Y.; Kim, W.; Seo, H. K-XMSS and K-SPHINCS+: Enhancing Security in Next-Generation Mobile Communication and Internet Systems with Hash Based Signatures Using Korean Cryptography Algorithms. Sensors 2023, 23, 7558. https://doi.org/10.3390/s23177558
10. Merkle, R.C. (1988). A Digital Signature Based on a Conventional Encryption Function. In: Pomerance, C. (eds) Advances in Cryptology — CRYPTO ’87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48184-2_32
11. Chen, H.; Liang, D. Adaptive Spatio-Temporal Query Strategies in Blockchain. ISPRS Int. J. Geo-Inf. 2022, 11, 409. https://doi.org/10.3390/ijgi11070409
12. Weijie Wang, Annie Ulichney, and Charalampos Papamanthou. 2023. BalanceProofs: maintainable vector commitments with fast aggregation. In Proceedings of the 32nd USENIX Conference on Security Symposium (SEC '23). USENIX Association, USA, Article 247, 4409–4426.
13. Kurosawa, Kaoru, and Goichiro Hanaoka, eds. Public-Key Cryptography--PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, Feburary 26--March 1, 2013, Proceedings. Vol. 7778. Springer, 2013.
14. Peikert, Chris, Zachary Pepin, and Chad Sharp. "Vector and functional commitments from lattices." In Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part III 19, pp. 480-511. Springer International Publishing, 2021.
15. Kuszmaul, John. “Verkle Trees.”, 2019
16. C. Papamanthou, E. Shi, R. Tamassia, and K. Yi. Streaming authenticated data structures. In EUROCRYPT, pages 353–370. 2013.
17. Iavich, M., Gnatyuk, S., Arakelian, A., Iashvili, G., Polishchuk, Y., & Prysiazhnyy, D. (2021). Improved Post-quantum Merkle Algorithm Based on Threads. In Advances in Computer Science for Engineering and Education III 3 (pp. 454-464). Springer International Publishing.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 14 – 24 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MODIFIED WOLF SHEEP PREDATION ALGORITHM FOR NETWORK THREAT REDUCTION

Audecious Mugwagwa[1], Colin Chibaya[2], Ernest Bhero[1]

[1]School of Engineering, University of KwaZulu Natal, Howard College, South Africa
[2]Department of Computer Science, and Information Technology, School of Natural and Applied Sciences, Sol Plaatje University, Kimberley, South Africa

ABSTRACT. Because most attacks target computers, intrusion detection has emerged as a key component of network security. This is a result of the widespread expansion of internet connectivity and information system accessibility on a global scale. The Wolf Sheep Predation Algorithm (WSPA), evolved from the Wolf Pack Algorithm. It models how wolves hunt in packs. This paper focused on the Lotka-Volterra predator-prey model. Due to its global convergence and computational strength, it has mostly been applied in a variety of engineering optimization issues. The method, however, has numerous flaws, including slow convergence and a tendency to quickly reach the local optimum. To address the above-mentioned flaws, this research developed the Modified Wolf Sheep Predation Algorithm (MWSPA) to reduce network threats. the algorithm models the wolves and sheep, where the wolves in this study represent the network security agent while the sheep represent network threats. The model suggests a better strategy to address the problem of slow convergence and quickly reach the local optimum by making sure that there is a balanced ecosystem at any point in time. This is achieved by ensuring that the network security agents(wolves) are not outnumbered by threats(sheep) and they do not become extinct when there is no food source. So in the absence of food, the MWSPA ensures the wolves can survive on grass and maintain their strength to hunt their next prey. This idea prevents the algorithm from crashing if the wolves die while the prey grows to infinity and consumes all the available grass. This therefore solves the problem of rapidly failing into a local optimum. This study aimed to identify the most pertinent features employed by wolves (network security agents) while hunting the sheep (network threats). We therefore established that sense of hearing and smell, splitting prey, encircling prey, assisting the hunter with the best chance of success, and looking for alternative prey as the most outstanding attributes used by wolves while hunting. The study further evaluated the MWSPA, and the outcomes demonstrate that the suggested algorithm outperforms its predecessor approach in a variety of search environments. Therefore, this shows that the MWSPA may possess the necessary qualities for creating a solution that will completely eradicate network threats and might provide leads in solving growing cybersecurity concerns globally.

Keywords: cybersecurity, cyberthreats, self-organization, swarm intelligence, algorithms

1.0 INTRODUCTION

One of the most difficult problems resulting from the rapid development of information technology is network security (Yuchong & Qinghui, 2021). As a result, the network's perimeter and the data that traverses across it need to be protected (Eric & Anca, 2022). The primary objective of intrusion detection systems (IDSs) is to identify and differentiate between regular and abnormal network connections, which is regarded as one of the main problems with intrusion detection systems due to the abundance of qualities or features quickly and accurately. Designing intrusion detection systems is significantly hampered by the emergence of malicious software (malware) (Ponnusamy, et al., 2021). The main issue in identifying unknown and obfuscated malware is that the creators of the infection utilize various evasion tactics for information concealment to evade detection by an IDS (Ansam, et al.,

2019). Malicious attacks have become more complex. Additionally, there have been more security risks like zero-day attacks that are aimed at internet users. Consequently, since the usage of information technology has permeated our daily lives (Mugwagwa, et al., 2023), computer security has become crucial (World Economic Forum, 2022).

Every company has a purpose and risk management is essential to protecting an organization's information assets (NIST, 2011). This is achieved by employing (Mugwagwa, et al., 2023)automated information technology systems to detect and eliminate network threats (Sikender & Lakshmisri, 2018). As a result of this trend's expansion of the attack surface, there have been more cyberattacks directed at businesses and organizations (Mugwagwa, et al., 2023). The cybersecurity landscape has changed in terms of the sophistication of attacks, their complexity, and their impact (Government of Canada, 2022). This is due to factors such as an ever-increasing online presence, the conversion of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity, and the exploitation of new features of emerging technologies like Artificial Intelligence (Yuchong & Qinghui, 2021). Notably, the threat to supply chains has taken the top spot among major threats because of the magnitude of their potentially catastrophic cascade effects (CISA, 2022). It is important to note that the impact of cyber threats on different industries has been given special attention with the continuously changing threat landscape (Heloise, 2022). The unique characteristics of each sector with respect to the threat landscape and areas of concern may provide interesting insights. Additionally, there have been some noteworthy actions taken by policymakers and cybersecurity specialist to lessen the impact of network threats (Hans & Marijn, 2017). Ransomware and phishing are the most common threats being reported globally, and the international community has started to realize the need for communication and collaboration in tracing indicators of compromise and cyber attackers (Alok, et al., 2022). Considering the foregoing, this article attempts to contribute to current efforts to eradicate and lessen the effects of network threats on a worldwide scale by assessing the degree to which the implementation of the Modified Wolf Sheep Predation algorithm could aid in the eradication of network risks in enterprises.

1.2 Wolf Sheep Predation Algorithm (WSPA)

The algorithm mimics wolves as they hunt for food. Wolves find prey by using their exceptional sense of smell in conjunction with their superb hearing (Rui, et al., 2012). Although wolves prefer to hunt in packs, lone wolves can also successfully hunt small animals on their own. The WSPA uses a mathematical mapping that mimics the tactics employed by the wolf while hunting, such as splitting prey, encircling prey, assisting the hunter with the best chance of success, and looking for alternative prey (Wu & Zhang, 2014). Wolf predation algorithms can be modeled using a mathematical model that considers various factors such as the number of wolves in a pack, their hunting capabilities, and the abundance of prey in their ecosystem (Xuan, et al., 2021). This paper focuses on the Lotka-Volterra model and assumes that a predator's rate of prey consumption is inversely related to its abundance (Frank, et al., 2021). As a result, the only factor affecting predators' ability to feed is the availability of prey (Thomas, et al., 2021). This mathematical model can be useful in predicting the behaviour of wolf predation patterns and can help inform conservation efforts to ensure the stability of both predator and prey populations (Noah, et al., 2021). The model is based on several key assumptions, including the idea that wolves have a certain hunting efficiency, which is determined by factors such as the size of their pack, their experience level, and the abundance of prey in their habitat. Additionally, the model considers the reproductive rates of both wolves and their prey, as well as the effect of environmental factors such as weather and vegetation on the survival and growth of both populations.

1.2.1 Inspiration of the WSPA

The algorithm was influenced by the studies done on the behaviour of social wolves while hunting for food. To be more precise, we concentrated on colony predation, which is a strategy adopted by wolves to evade predators and boost the likelihood of a successful hunt (Muro, et al., 2021). Predators

frequently acquire more prey through colony predation, which increases the likelihood that each individual will survive (Dipanjan, et al., 2020). Colony predation is a strategy used by wolves and other animals that live in colonies to ensure their survival (Muro, et al., 2021). The wolf sheep predation algorithm is a heuristic optimization algorithm inspired by how wolf packs hunt and search for food. In this algorithm, there are two types of wolves: alpha wolves and beta wolves (Xuan, et al., 2021). The alpha wolves are responsible for exploring the search space and finding potential solutions, while the beta wolves follow the alpha wolves and refine the solutions found by the alpha wolves (Weitzenfeld & Vallesa, 2006).

The algorithm starts with an initial population of solutions, which are randomly generated. The alpha wolves then select the best solutions and share their knowledge with the beta wolves (Xuan, et al., 2021). The beta wolves then use this knowledge to refine the solutions and generate new ones. To catch more prey than they could individually, wolves, communicate and work together through colony predation (Jiaze, et al., 2021). The two most popular strategies for increasing the likelihood of successful hunting are dividing and encircling animals. Another tactic used by wolves when they come into circumstances, such as when consumption outpaces their yield, is selective abandonment (Jiaze, et al., 2021). They will switch to another target in this behaviour, which increases the effectiveness of their predation. This process continues until a stopping criterion is met, such as a maximum number of iterations or a satisfactory solution has been found (Dipanjan, et al., 2020). The main aspects of the algorithm are splitting/diving, encircling, assisting the hunter with the best chance of success, and selective abandonment which all revolve around the communication aspect. The section below discusses the various strategies used by wolves while they hunt for prey.

1.2.1.1 Communication:

Wolves that hunt in packs have a higher success rate for predation due to cooperation and communication. To affect their behavior of looking for food, they convey their positions relative to the position of the pack leader. These positions also help in the event the hunters with the best chances of success need support.

1.2.1.2 Splitting/Dividing:

Another aspect of colony predation by wolves is to drive their prey in separate directions, separating it from the rest of the pack, this predation technique is employed by individual wolves when looking for food.

1.2.1.3 Encirclement:

The other tactic employed by the hunting wolves is to encircle and approach the prey increasing the chances of a successful hunt.

1.2.1.4 Assisting hunter with the best chances of success:

The closest member requests help from the group because they might have trouble hunting prey to increase success chances. This is achieved through communication, which has been identified as one aspect employed by wolves in successful hunting.

1.2.1.5 Selective abandonment:

If no prey is found nearby, or food is located too distant from the prey, the remaining individuals will find another food source.

1.2.2 The Model

The mathematical simulation of the algorithm's position illustrates the search process of individuals and groups in two and three dimensions, with a predator at position (X, Y) updating its position in accordance with the target's location (Xbest, Ybest). The predator leader and other predators in the 2D search space are used to update the search agent's position. The ultimate position will be at random influenced by the positions of the predator leader and the other predators in the search area.

In the model, we can consider the cyber security threats as the prey, and the security measures as the wolves. We can then define the fitness function that represents the effectiveness of the security measures in protecting the system from the threats. The wolf pack can be modelled as a group of security measures that work together to detect, prevent, and mitigate cyber security threats. The wolf agents can communicate with each other and coordinate their actions to optimize their fitness function. Through iterations of the algorithm, the wolves can adapt their strategy to improve the overall security of the system. The Wolf Sheep Predation model works as follows:

1. *Initialization: Generate an initial population of wolves and prey.*
2. *Fitness evaluation: Evaluate the fitness of each wolf in the population based on the objective function to be optimized.*
3. *Leader selection: Identify the best wolf (alpha) and the second-best wolf (beta) in the population.*
4. *Prey search: Each wolf in the population performs a prey search to explore the search space and improve its position. This is done by randomizing the position of the wolf and evaluating its fitness.*
5. *Pack hunting: Wolves then move towards the position of the alpha and beta wolves in the population. They adjust their positions based on the position of the leaders and evaluate their fitness at the new positions.*
6. *Updating the population: The population is updated with the new positions of the wolves.*
7. *Termination: The algorithm terminates when a stopping criterion is met (e.g., a maximum number of iterations or a certain level of fitness is achieved).*

4. RESEARCH AND METHODOLOGY

We created a simulator to test how well the Modified Wolf Sheep Predator Algorithm is for eliminating network threats. One simulator was run to determine how well the WSPA algorithm can individually address the network threat issue. The objective was to determine if the main attributes of the algorithm can be used to address the problem defined problem. Wolf agents would scout for food targets which are represented as sheep. The wolf will represent the hunting agent and the sheep will resemble threats. Once the simulations begin, both agents and threats get generated in the simulator's deployment environment, being created at random. The simulations used 100 sheep and 50 wolf agents which were randomly generated and deployed into the environment. Using the outstanding characteristics namely, splitting prey, encircling prey, assisting the hunter with the best chance of success, and looking for alternative prey, the deployed set of wolf agents searches for and identifies potential dangers(prey) in the environment or ecosystem. Separate simulations were run for the same algorithm varying the number of agents, the results were noted, and conclusions were drawn on how the algorithm can address the network threat problems.

4.1 Experiment

The modified wolf sheep predation algorithm's potential for eliminating network threats was tested through an experiment. Using the Netlogo simulators, the experiment was run using an Intel® CoreTM i5 10th generation PC running Windows 11Pro with a 2.40GHz processor and 8GB of RAM. The environments randomly generated wolf, sheep, and grass agents where the wolf agent will hunt for threats(sheep), in the environment. The wolf should ensure that there is no or minimal prey in the environment. While the threat(sheep) feeds on vulnerabilities(grass) to keep alive. Since the sheep can become extinct, the algorithm has been modified so that the wolf can feed on grass for a short period of time if the sheep become extinct. While the simulation is being executed, the agents communicated until they reached the optimal position determined by the instructions given. The key aspects of the algorithm were noted and discussed on how they can be adopted in eliminating network threats.

4.2 Environment setup

The environment in this research refers to two-dimensional square like surface designed in Netlogo. The environment is made up of threat sources and agents which are randomly generated across the two-dimensional square. Once the simulations begin to run, agents scout around the area looking for threat sources. The agent's position keeps changing and being communicated through various techniques until they converge at the best location. While hunting for prey, wolves, communicate and work together through colony predation. They use the four most popular strategies for increasing the likelihood of successful hunting namely dividing, encircling the prey, assisting the hunter with the best chances, and selective abandonment. With selective abandonment, they will switch to another target in this behaviour, which increases the effectiveness of their predation. This process continues until a stopping criterion is met, such as a maximum number of iterations or a satisfactory solution has been found. The main aspects of the algorithm are splitting/diving, encircling, assisting the hunter with the best chance of success, and selective abandonment. The afore mentioned, are the main aspects employed by the WSPA in eliminating network threats.

5. FINDINGS

This section articulates the findings of the experiments as well as the results obtained. The results discuss the number of deployed agents, noting the convergency times as the number of deployed agents varies. Finally, the section analyses these findings and gives recommendations for improving the Wolf Predation Algorithm's detection and elimination of network threats.

5.2 WSPA Simulation

Separate simulations were run for the same algorithm varying the number of agents, the results were noted, and conclusions were drawn on how the algorithm can address the network threat problems. Figure 1 depicts the ecosystem with fifty (50) hunting or search agents looking for prey and one hundred (100) threats represented by sheep as prey. The hunting agents are seen scouting for prey in Figure 2 below, which demonstrates that the predator population has grown greatly relative to that of the prey. Figure 5 demonstrates how predators or hunting agents that resemble wolves are initialized with various strengths depending on the prey they have consumed. As they hunt, their energy reserves go smaller, thus they would prefer to spend as little energy as possible before catching the next prey.

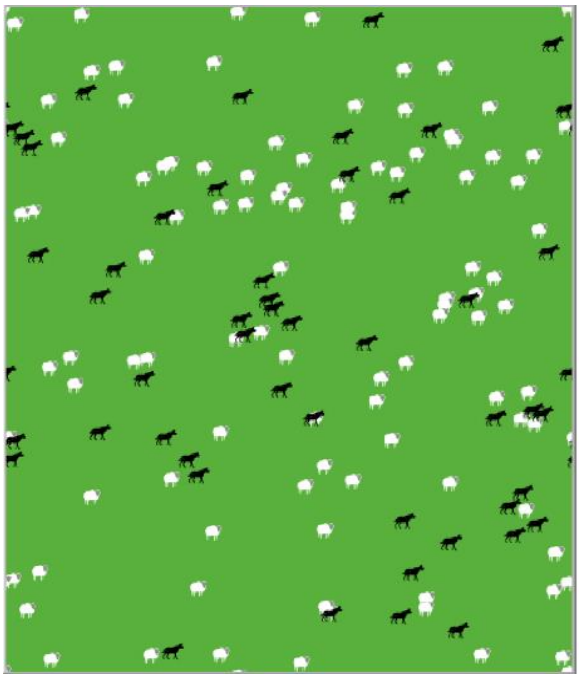


Fig.1 - Wolf Sheep Predation simulation environment

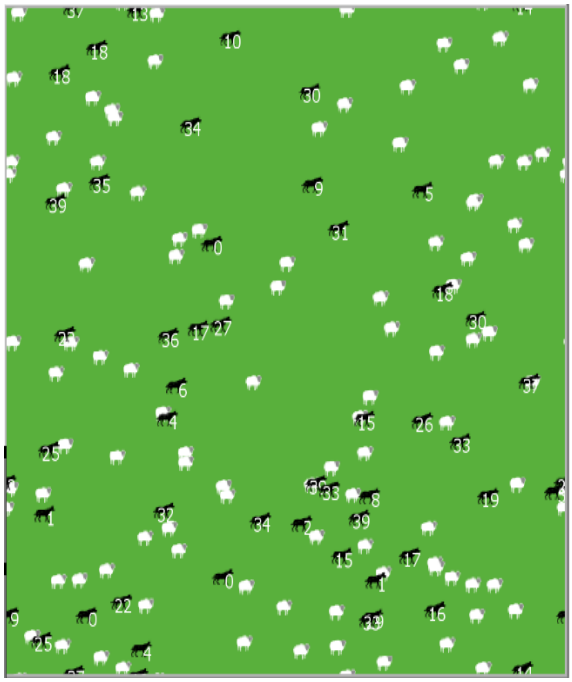


Fig. 2 - Searching and elimination of threats

As the algorithm continues to run, as seen in Figure 3, the predator agent population continues to decline. This is because there will be less food available (prey), which will result in loss of energy. This illustrates how the energy of the predator decreases until it is zero, at which point the wolf agent perishes which gives a situation depicted in figure 4.

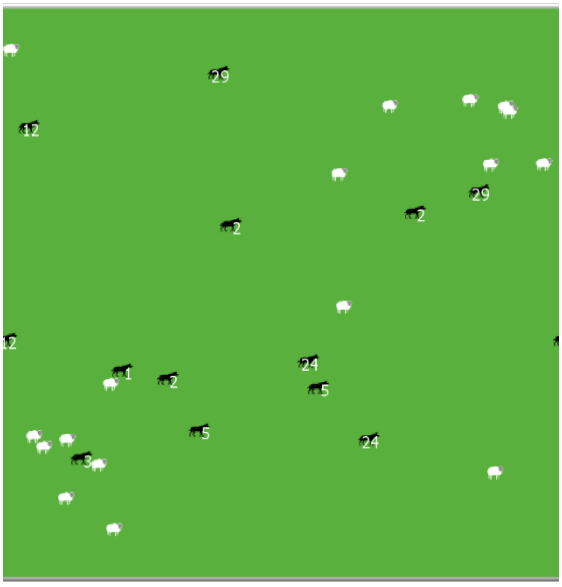


Fig. 3 - Predator energy reduced

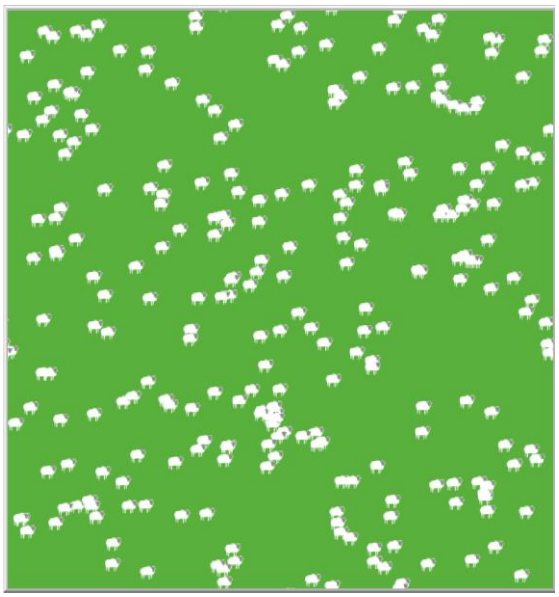


Fig. 4 - Predator Agents extinct

Due to a lack of food when the number of preys decreased (see figure 4), predators or hunting agents all become extinct. This suggests that the environment becomes vulnerable as the hunting agents reach a point where they fail, and the network becomes overrun with threats. There is need to enhance or refill

the predator energy is thus suggested to prevent their extinction, to keep them actively securing the network.

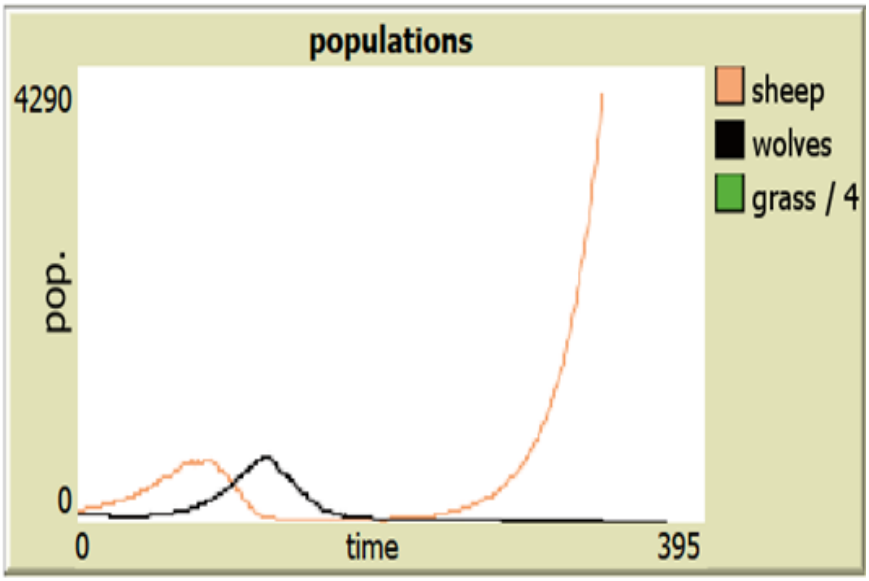


Fig. 5 - Predator agents failed to neutralise threats.

The agents' failure to converge is shown in Figure 5. This is substantiated by the fact that the predators were unable to get rid of the prey, and that this will have a significant impact on network security. This suggests that the WSPA may need to be enhanced to replenish the energy of the predators and guarantee that agents are constantly actively hunting and eliminate threats within a network.

5.3 MWSPA Simulation

To solve the issue, the WSPA must be improved by including a new feature that permits predators to eat grass if there is no prey present. By including these elements, the MWSPA is created, and while the predators feed on grass, they may not gain the same amount of energy as when they eat their prey but will instead keep them alive till they catch their next prey. With these components incorporated it gave the following results.

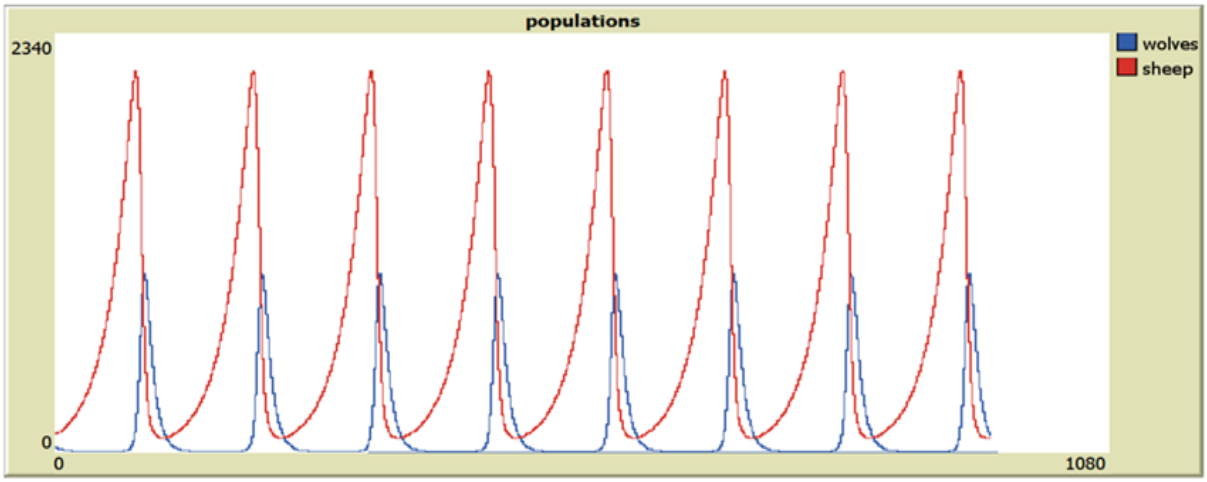


Fig. 6 - MWSPA convergence Graph

The shortfalls of the WSPA of slow convergence and reaching the local optimum have addressed by the MWSPA through the introduction of other variables which includes increasing the grass growth rates and making wolves to feed on grass to boost their energy in case there is no prey. These concepts will help to eliminate predators becoming extinct and therefore ensure that there are no vulnerabilities posed in the network environment as we have seen with the results presented earlier.

5.4 Discussion

The purpose of this section is to give suggestions regarding how the adoption of the WSPA may help eliminate network threats influenced by the results of the simulations done. The research established that the WSPA employees splitting/diving, encircling, assisting the hunter with the best chance of success, communication, and selective abandonment as the main aspects of the algorithm. The results of the experiments conducted further revealed that the predator agent population continues to decline when they fail to find prey as they keep losing energy while hunting. This further suggested that predator agents needed to use the least energy to hunt to ensure that it keeps surviving. As evidenced by the results due to the decreasing number of preys, predators or hunting agents all become extinct at some point in time. This suggests that the environment becomes vulnerable as the hunting agents reach a point where they fail, and the network becomes overrun with threats. There is a need to enhance or refill the predator energy to prevent their extinction and to keep them actively securing the network. This paper, therefore, suggested additional elements to the model that modifies the approach based on success rates and simulates the selective abandonment behavior of hunting wolves through the Modified Wolf Sheep Predation Algorithm (MWSPA). The MWSPA seeks to enhance Lotka-Volterra predator-prey model and make it more suitable for eliminating network threats by dealing with the slow convergence and reaching the local optimum issues. These issues have been addressed by introducing the concept that the sheep/prey agent do not lose energy and the wolf agent can gain limited energy by feeding on grass if there is no prey so that they don't die. Each wolf or sheep agent has a fixed probability of reproducing at each time step in order to maintain the population. In this form, we don't directly represent the eating or growing of grass; instead, we treat the grass as infinite so that sheep always have plenty to eat. As a result, eating and moving do not cause sheep to gain or lose energy. This allows for a stable ecosystem. With these elements incorporated with the development of the MWSPA, the convergence graph will be as shown below. This represents a balanced ecosystem where the problem of slow convergence and reaching local optimum are addressed and the population of the predators wont get zero as with the WSPA.

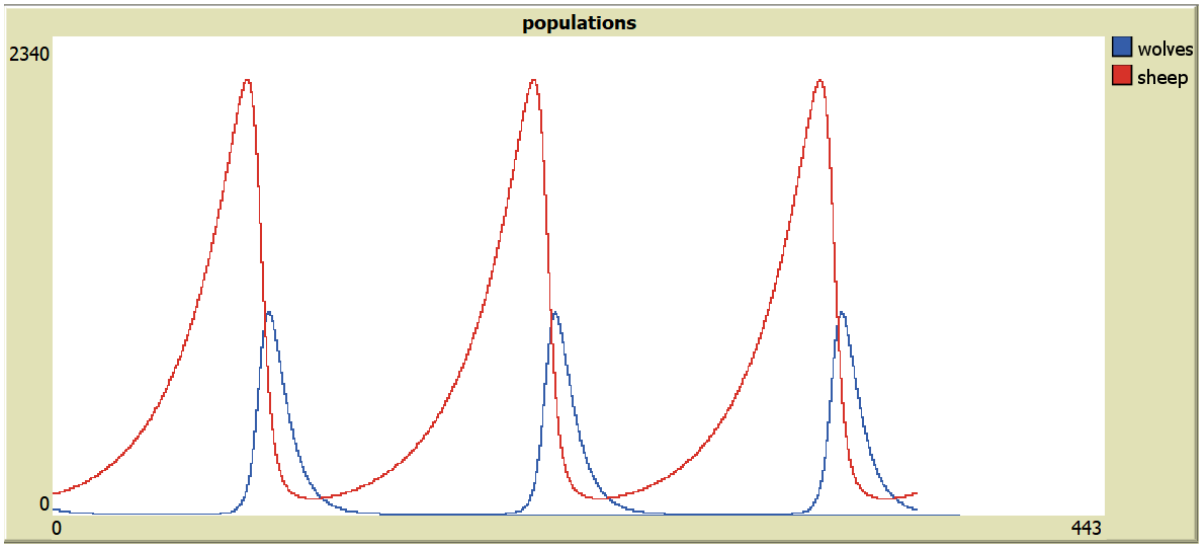


Fig. 7 - MWSPA graph

Figure 7, suggests that the predators and prey agents population have a fixed probability of reproducing. As the predator fail to find prey, they will feed on grass to have the energy needed until the find the next prey. Though they get the energy from grass, their energy continues to deplete but the rate of death is reduced hence ensuring that predator agents wont get extinct. This helps stabiles the ecosystem and ensures that there are predator agents available to eliminates network threats at any point in time.

7. CONCLUSIONS

The Wolf Sheep Predation Algorithm is a bio-inspired algorithm that simulates the hunting behavior of wolves in nature. This algorithm has been found to have useful applications in cyber security.

In cyber security, the Wolf Sheep Predation Algorithm can be used for intrusion detection and prevention. The algorithm can be trained to analyze data patterns and identify anomalies and threats in a network. It works by creating a model of normal network behavior, then comparing the actual behavior with the expected behavior. If the algorithm detects any deviations, it triggers an alert to the security team for further investigation. Overall, the Wolf Sheep Predation Algorithm is an innovative approach to cyber security that has the potential to improve the detection and prevention of cyber threats.

The wolf predation algorithm is a relatively new optimization technique inspired by the hunting behaviour of wolves. However, like any other algorithm, it also has some limitations and shortcomings. One of the main issues is that it can get trapped in local optima, which means that it may not necessarily find the global optimal solution. Additionally, the algorithm can be computationally expensive, especially when dealing with complex optimization problems. Finally, the wolf sheep predation algorithm may require some tuning of the parameters to work effectively, which can be time-consuming and difficult for some users. Despite these limitations, the wolf sheep predation algorithm has shown promise in solving a variety of optimization problems and is still being studied and improved upon by researchers. As a result, this research suggested combining the Wolf Sheep Predation algorithm with other algorithms or existing security solutions to improve its ability to detect and eliminate network threats.

8. KEY OBSERVATIONS

The MWSPA has shown promise in enhancing the capabilities of cyber security systems and improving the detection and response to cyber threats. However, like any other security solution, it is not foolproof and should be used in combination with other security measures for maximum protection. Some possible areas for enhancement could include improving accuracy, increasing efficiency, reducing errors, improving scalability, and optimizing resources. Additionally, main issues which causes it to get trapped in local optima , which means that it may not necessarily find the global optimal solution has been addressed by introducing the concept that the sheep/prey agent do not lose energy and the wolf agent can gain limited energy by feeding on grass if there is no prey so that they don’t die. Each wolf or sheep agent has a fixed probability of reproducing at each time step in order to maintain the population. In this form, we don't directly represent the eating or growing of grass; instead, we treat the grass as infinite so that sheep always have plenty to eat and stabilize the ecosystem.

9. CONTRIBUTIONS

The paper made contributions by providing a review of the Wolf Sheep Predation algorithms' inspirations, the model and the features that constitute the model, how it may be utilized in network threat detection and elimination, and its effects in eliminating network threats.

The paper identified communication, splitting/diving, encircling, assisting the hunter with the best chance of success, and selective abandonment as the outstanding aspects of the algorithm which can be

adopted for network threats detection and elimination. These aspects can be adopted in developing a network threat detection and elimination solution integrated into existing solutions for enhancement.

One of the main contributions in intrusion detection is that by using the Modified Wolf Sheep Predation Algorithm, it is possible to identify and classify malicious activity more accurately, thereby improving the overall security posture of a system. Overall, the use of the Modified Wolf Sheep Predation Algorithm in the network can contribute significantly to the development of more effective and efficient security solutions. Even though the algorithm has these robust features, it also has some shortfalls which may be enhanced by combining it with other algorithms or integrating it with existing network threat detection and elimination solutions to bring better results.

10. FUTURE WORKS

The wolf predation algorithm has had several developments and improvements and some possible future developments to enhance its adoption in cybersecurity include:

1. Hybridization with other algorithms: Exploring the possibility of combining the wolf predation algorithm with other optimization algorithms to create hybrid algorithms that can perform better on certain types of problems.
2. Multi-objective optimization: Currently, the wolf predation algorithm is mostly used for single-objective optimization problems. However, there is potential for using it in multi-objective optimization problems, where the algorithm tries to optimize several objectives at once.
3. Dynamic adaptation: In nature, wolves adapt their hunting behaviour based on changing environmental conditions. Similarly, there is potential for the wolf predation algorithm to be extended with dynamic adaptation mechanisms to improve its performance in dynamic optimization problems.
4. Parallelization: As with most optimization algorithms, the wolf predation algorithm can benefit from parallelization techniques that allow it to exploit modern computing architectures more efficiently.
5. Applications in machine learning: The wolf predation algorithm has shown promising results in various optimization problems, and there is potential for using it in the context of machine learning tasks such as feature selection, dimensionality reduction, and model optimization.

11. FUNDING

This research was funded by the University of Kwazulu Natal (UKZN).

REFERENCES

1. Alok, M., Yehia, I. A., Memoona, J. A. & Asif, Q. G., 2022. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Elsevier, Computers & Security.*

2. Ansam, K., Iqbal, G., Peter, V. & Joarder, K., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Springer, cybersecurity.*

3. CISA, C. A. I. S. A., 2022. *Building more resilient ICT Supply Chain: Lessons learned during the COVID-19 Pandemic,* s.l.: CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

4. Dipanjan, C., Sanchayan, B. & De, R., 2020. Survival chances of a prey swarm: how the cooperative interaction range affects the outcome. *PubMed Central, Scientific Reports.*

5. Eric, G. & Anca, J., 2022. Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. *National Library of Medical Science.*

6. Frank, A., Subbey, S., Kobras, M. & Gjøsæter, H., 2021. Population dynamic regulators in an empirical predator-prey system. *Science Direct, Journal of Theoretical Biology,* Volume 527.

7. Government of Canada, 2022. *An introduction to the cyber threat environment,* ottawa: Canadan Centre for Cybersecurity.

8. Hans, d. B. & Marijn, J., 2017. Cybersecurity Awareness: The need for evidence-based framing strategies. *Elsevier, Government Information Quarterly.*

9. Heloise, P., 2022. The Cyber Threat Landscape in South Africa: A 10-Year Review. *The African Journal of Information and Communication.*

10. Jiaze, T., Huiling, C., Mingjing, W. & Amir, H. G., 2021. The Colony Predation Algorithm. *Journal of Bionic Engineering.*

11. Mugwagwa, A., Chibaya, C. & Bhero, E., 2023. A survey of inspiring swarm intelligence models for the design of a swarm-based ontology for addressing the cyber security problem. *INTERNATIONAL JOURNAL OF RESEARCH IN BUSINESS AND SOCIAL SCIENCE,* 12(4), pp. 483-494.

12. Muro, C., Escobedo, R., Specto, L. & Coppinger, R., 2021. Wolf-pack (Canis lupus) hunting strategies emerge from simple rules in computational simulations. *Elsevier, Behavioural Processes,* Volume 88, pp. 192-197.

13. NIST, N. I. o. S. a. T., 2011. *Managing Information Security Risk,* s.l.: nist.

14. Noah, B., Victor, L. & Frithjof, L., 2021. Seasonal dynamics of a generalist and a specialist predator on a single prey. *Mathematics in Applied Sciences and Engineering* .

15. Ponnusamy, V. et al., 2021. Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks. *Tech Scoence Press, Computer Systems Science & Engineering,* .

16. Rui, T., Simon, F., Xin-She, Y. & Deb, S., 2012. Wolf search algorithm with ephemeral memory. *2012 Seventh International Conference on Digital Information Management (ICDIM).*

17. Sikender, M. M. & Lakshmisri, S., 2018. Security Automation in Information Technology. *SSRN Electronic Journal,* pp. 901-905.

18. Thomas, J. H., Kevin, D. & Murray, L., 2021. Increasing availability of palatable prey induces predator-dependence and increases predation on unpalatable prey. *PubMed Central, Scientific Reports* .

19. Weitzenfeld, A. & Vallesa, A., 2006. A Biologically-Inspired Wolf Pack Multiple Robot Hunting Model. *IEEE Latin American Robotics Symposium, LARS.*

20. World Economic Forum, 2022. *Global Cybersecurity Outlook 2022, Insights Report January 2022,* s.l.: s.n.

21. Wu, H. & Zhang, F., 2014. Wolf pack algorithm for unconstrained global optimization.. *Mathematical Problems in Engineering.*

22. Xuan, C. et al., 2021. An improved Wolf pack algorithm for optimization problems: Design and evaluation. *PLOS ONE.*

23. Xuan, C. et al., 2021. An improved Wolf pack algorithm for optimization problems: Design and evaluation. *PLos One.*

24. Yuchong, L. & Qinghui, L., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Elsevier,* pp. 8176-8186.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 25 – 38 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

FINTECH RESILIENCE: AN EXPLORATION OF SECURITY RISKS AND RISK MANAGEMENT STRATEGIES

Ali Mwase[1], Ernest Ketcha Ngassam [2], Shawren Singh[3]
[1]Makerere University Business School, Kampala, Uganda
[2]University of South Africa, South Africa

ABSTRACT. The rapid evolution of financial technology (Fintech) has brought about unprecedented opportunities and challenges, particularly in the realm of security. This research paper conducts a thorough exploration of the security landscape within the Fintech sector, with a focus on identifying and understanding the diverse risks that pose threats to the industry's resilience. The study delves into operational, technological, regulatory, and cybersecurity risks, unraveling their complexities and implications for the Fintech ecosystem.

The core of this research lies in the comprehensive examination of risk management strategies employed by Fintech entities to fortify their resilience against the identified security threats. By synthesizing current literature and industry practices, the paper provides valuable insights into innovative risk mitigation approaches, considering the dynamic nature of the Fintech environment. Special attention is given to the integration of advanced technologies, regulatory compliance, and collaborative frameworks that contribute to enhancing the sector's overall resilience.

Furthermore, the study proposes a Fintech Ecosystem Risk Management Metamodel to illustrate the practical application of risk management in addressing security challenges for the sector. The findings aim to equip industry practitioners, policymakers, and researchers with a nuanced understanding of the interconnected dynamics between security risks and effective risk management in the Fintech landscape. Ultimately, this study contributes to the ongoing discourse on fostering resilience within Fintech, ensuring the sustained growth and stability of this transformative sector.

KEYWORDS*:* Fintech, Security risks, Risk management, Cyber security, Risks.

1.0 INTRODUCTION

The Fintech industry has ushered in a new era of financial services, offering innovative solutions that promise convenience, efficiency, and accessibility (Callen-Naviglia & James,2018). However, this digital transformation has brought with it a host of cybersecurity challenges (Dattani, 2016). Because of channel fusion and simplicity, Fintech services are relatively susceptible to security problems (Park & Kim,2015). Fintechs are particularly susceptible to security risks due to the nature of their operations and the sensitive data they handle (Sampat et al, 2023). A Security risk in the context of Fintech is closely related to risks associated with digital technologies due to the heavy deployment of digital components in Fintech solutions and platforms (Kaur et al,2021). Digital security threats like hacking, phishing, virus, and e-fraud could exploit vulnerabilities in digital systems to activate certain risk crystallization (Keong et al,2020). Exposure of or loss of control over customers' personal information, trade secrets, and other confidential information could amount to a potential loss known as a security risk (Keong et al,2020; Razzaque et al,2020). This could consequently result in information theft and degradation of integrity, privacy, confidentiality, authenticity, and accountability of information (Razzaque et al,2020).

A study by Alijoyo (2022) asserts that Fintechs are some of the increasingly high-risk businesses because they provide many online services such as online money lending services. Thus, good risk management is a must for Fintechs. Risk management is the identification, measurement, monitoring,

and evaluation of diverse risks (hazards, disasters, shocks) followed by a coordinated and cost-effective application of resources (prevention, mitigation, preparedness, resilience) to minimize and control the probability and impact of exposure and to try to maximize the realization of possible returns(UN,2021). Risk management further ensures that a company or organization can understand, measure, and monitor various risks and ensure that the policies made can control the various kinds of risks (Alijoyo ,2022). It is postulated that Fintechs can enhance their success in regulated markets by having sound and robust risk management practices. This increases the comfort levels of key stakeholders who value transparency and best practices in risk management (Mehrotra & Menon,2021). Moreover, it is postulated that Risk management in Fintechs is not only essential for protecting against potential threats but also for building trust, ensuring regulatory compliance, and fostering long-term sustainability in a rapidly evolving industry (Fenwick &Erik,2020). The need for risk management in Fintechs is crucial, given the unique challenges and complexities associated with operating in the dynamic intersection of finance and technology (Cernisevs et al,2023). This study therefore aims at investigating the security landscape within the Fintech sector, shed light on effective risk management strategies, and present a metamodel that can guide practitioners and policymakers in fortifying the resilience of the Fintech sector against evolving security threats.

The remaining part of this paper is structured as follows: Section 2 presents the related literature, section 3 covers the methodology adopted by the study, of which the results of our research that present the assets in the Fintech landscape, mapping of potential risks to these assets, mapping of the Fintech Security Risk assessment as well as a proposed Fintech Ecosystem risk management Metamodel are presented in Section 4. Section 4 further presents some existing Risk management strategies. Finally, the conclusion of this work is presented in Section 5.

2.0 RELATED WORKS

2.1 Definition of Risk and Risk Management

A risk is an uncertain event with a probability of happening and impacting an organization's strategic, operational, and financial objectives (Kure et al,2018). In a business context, risks are any threat to a vulnerable asset that will cause harm to reach business objectives(Vellani,2006). Risks can be divided into proactive and reactive risks. Risks are characterized by the likelihood of the event occurring and the impact of the event. The risk formula can be used to calculate the value of a risk: Risk (Expected Loss) = likelihood multiplied by impact. Risk management involves identifying, analyzing, and controlling risks in an organization's information assets and infrastructure to increase effectiveness and efficiency (Alijoyo, 2022).

2.2 Cyber Risk Assessment

Cyber risk assessments are essential for organizations to identify, estimate, and prioritize risks arising from information systems operations and use (Tunggal,2023).They evaluate threats to IT systems and data, enabling organizations to prioritize improvements, communicate risks to stakeholders, and make informed decisions on resource deployment to mitigate security risks (Cobb,2022).Conducting a cybersecurity risk assessment helps organizations understand the magnitude of risks and manage them effectively. Mitigating identified risks can prevent and reduce costly security incidents and data breaches, while avoiding regulatory and compliance issues(Cobb,2022).Cyber risks include ransomware, data leaks, phishing, malware, insider threats, cyberattacks, infrastructure attacks, intellectual property theft, insecure supply chain partners, and aggressive insider behavior(Tunggal,2023).

2.3 Cyber Security

Cyber security is the protection of information and communication networks from cyber-attacks and threats in the cyberspace or network (Li & Liu,2021). It involves the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance, and technologies used to protect the cyber environment and organizations' assets(Armenia et al,2021).Cybersecurity encompasses both human and non-human entities, and focuses on three key

factors: methods of protecting IT, data processing and transmission, level of protection obtained, and professional aspects. Cybersecurity investment has become an increasingly important issue due to advanced technology and cyber attackers (Dunn Cavelty,2014). Fintech organizations must prioritize cybersecurity measures to protect their IT infrastructure, including secure APIs and cloud servers. By addressing the range and scope of cyber-attacks, organizations can reduce vulnerability across relevant weaknesses and ensure the overall security of their IT infrastructure.

3.METHODOLOGY

We conducted a systematic literature review using a six-step approach, which consists of selecting a topic, looking for pertinent articles, creating arguments, reviewing, assessing, and publishing the literature (Machi & McEvoy, 2016).

In order to explore the state of the art of the Fintech security landscape through various combinations of the keywords that are specified before the introduction, we therefore searched databases such as google

scholar, Science Direct, Wiley database, Sage database, IEEE database, ACM, MDPI, Springer, and Emerald. Thereafter, we selected papers from fifteen peer-reviewed Information Systems and computer security journals with specific publications on Fintech security risk related articles. They are all ranked highly in the 2020 SJR Journal ranking charts. The articles that were selected for examination were published over the last eleven years, from 2011 to 2021. Even so, older papers were included if they included relevant information about the topic of the study. We looked through up to five volumes in each of these journals to locate a maximum of five articles, pausing when we had located the five volumes or five articles, whichever comes first. According to the Krejcie & Morgan (1970) table for calculating sample size for a given population (Krejcie & Morgan, D1970), this produced a total of 50, and a matching sample size of 44.

The final selection consisted of 44 papers, 24 from computer security journals and 20 from information systems journals. We decided to use open coding. Multiple category names that had the same meaning were consolidated into one without taking that differentiation into account. To resolve any remaining differences regarding classification, the researchers studied the pertinent papers; this iterative approach aided in reaching a consensus. The results section below contains the presentation of the findings.

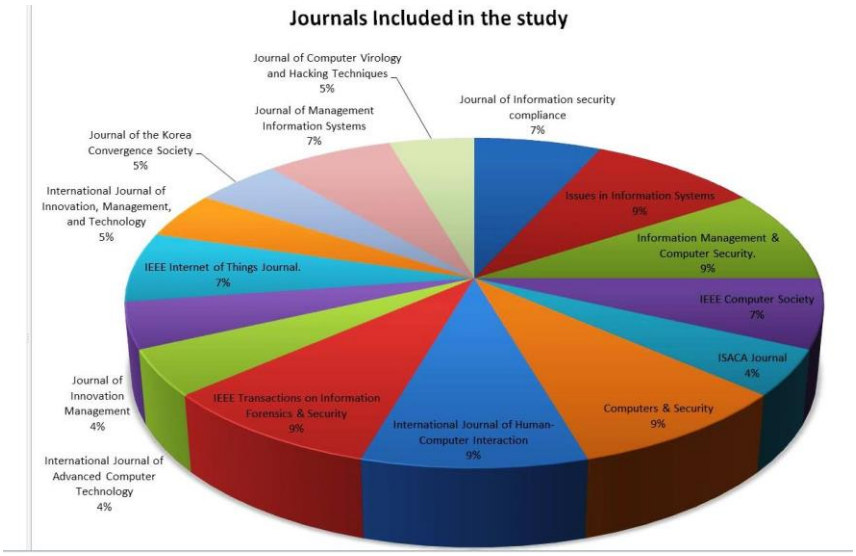


Fig. 1. Information Systems and Computer Security journals included in the study

4. RESULTS AND DISCUSSIONS

After analyzing the data, comparisons were drawn on parameters judged to be essential in the process of understanding and combating security risks in the fintech landscape. These are presented in the next sections 4.1 to 4.3 below.

4.1 Assets in the Fintech Ecosystem

Assets are defined as tangible or intangible entities that are necessary and have value to the Fintech organization (Kure et al,2018). Identification of key assets, and putting a value on each key asset, is an important process of risk management. These key assets could be people, services, facilities, processes, etc. It is important to identify critical assets as well as estimate their critical failure modes or the impact of the loss. An asset has two features: (i) criticality and (ii) category. Criticality is defined as a measure of the consequences associated with the degradation or loss of an asset. It is the major indicator used by organizations to determine which asset is of more value to business continuity. Category classifies assets according to their level of sensitivity and security requirements. The criticality of an asset category can be high, medium, or low, which means that assets with high ratings are the most valuable to the organization (Kure et al,2018).

To determine the key assets and role players in the Fintech ecosystem, we consider each aspect of the Fintech ecosystem. This was followed by determining the potential risks associated with these assets and further doing some classification of such risks in terms of business risk, technological risks, etc. The key assets and role players are summarized in table 1 below.

Tab. 1. Key assets and role players in the Fintech ecosystem

Stakeholders/ Role players	Assets	Systems components
• Fintech Companies • Financial Institutions • Venture Capital Firms • Incubators/Accelerators • Legal Advisors • Consultancy Firms • Research (Academia) • International Knowledge Partners • Regulatory Authorities • Industry Associations • Intermediary Organizations • The Financial Consumers • Incumbent Banks • Insurers • Software Companies • Technology Hubs	• Computer hardware • Computer software • Telecommunication devices • WLANS • LANS • Networking Cables • Mobile computing devices • Data Centers(Servers) • Database • Automated Teller Machines(ATM) • Crypto Assets • People • Transactions • Robo Advisors(AI) • Money	• Online platforms • Mobile Apps • Bank Accounts • ATM Cards • Financial Cards • Digital Wallets • Smart Contracts • Mobile point-of-sale systems

4.2 Fintech Assets and potential Risks

Determining and classifying potential risks associated with assets in the Fintech landscape is crucial. Indeed, a study by AFI (2020) posits that Fintechs pose potential risks to financial stability (Vučinić, 2020). Furthermore, a special report by Alliance for Financial Inclusion (AFI) (AFI,2020).Creating Enabling Fintech Ecosystems: observes that the rise of digital financial services and Fintech products

present new risks and threats, such as those stemming from opaque data privacy practices or systemic vulnerabilities from cybersecurity threats(AFI,2020).

It is observed that technology may lead to new types of risk or exacerbate existing ones. There is a need to explore risks such as the cyber risks in Fintech. This is because there is an increasing concentration of infrastructure at a limited number of participants (e.g., banks and broker-dealers providing trading technology and infrastructure to others), or central counterparties (Gomber et al,2018).

Risk identification entails examining an organization's current information technology security situation, Risk assessment involves determining the extent to which the assets are exposed or at risk, and Risk control focuses on applying controls to reduce risks to an organization's data and information systems (Whitman & Mattord,2021).

It is stated that the surge of adoption of sophisticated systems of Fintech among financial institutions, has highlighted the prominence of operational risk. An effective operational risk management process includes the identification and measurement of operational risk, which should lead to an understanding of the specific causes and events embedded in the adoption of Fintech, which may expose a Fintech company to operational risks (Khalil & Alam,2020).

Risks can be both internal and external to the firm. Risks are of various types namely; business risk, financial risk, operational risk, technology risk, security risk, compliance risk, availability risk, and strategic risk (Vellani, 2006). Others are; Systemic, Reputation, Legal, Liquidity, and Fraud(Lake,2013). The key risk areas for the Fintech Ecosystem are presented in table 2 below.

Tab. 2. Key risk areas for the Fintech Ecosystem

ASSETS	Potential Risks	Author	Risks Classification
• Computer hardware • Computer software	Security misconfigurations. Insufficient Logging & Monitoring. Deliberate hardware destruction	Akanksha(2022); Gurdip&Arash(2021)	Technological risk Security Risk
• People	Broken User Authentication. Sensitive data exposure and privacy incidents. Digital Identity risks. Credit card fraud. Accounting hijacking Imprudent lending.	Akanksha(2022); Gurdip&Arash(2021) ;Govindraj(2022); World Bank(2021)	Technological risk Security Risk Fraud risk
• Transactions	Broken Function Level Authorization. Insecure interfaces and API.	Akanksha(2022); Govindraj(2022)	Technological risk Security Risk Operational Risk
• Mobile computing devices	Application security risks. Hacktivists. Cybercriminals. Script kiddies. Cyber terrorists. Insecure interfaces and API's. Remote nature of digital channels and the rapid speed	Gurdip&Arash(2021) ;Govindraj(2022 World Bank(2021); Muhn,(2020)	Technological risk Security Risk Fraud risk Operational Risk

	of transactions. Platform/technology unreliability or vulnerability.		
• Crypto Assets	Insecure interfaces and API's. Unrecognized and illegal cryptocurrency trading Activity. Blockchain Security. Platform/technology unreliability or vulnerability.	Govindraj(2022); NSFOCUS(2018)	Technological risk Security Risk Fraud risk Operational Risk
• Robo Advisors(AI)	Cyber terrorists	Gurdip&Arash(2021)	Technological risk Security Risk Fraud risk Operational Risk
• Automated Teller Machines(ATM)	Denial of service Fraudulent transactions Cyber terrorists Compromising ATM infrastructure	Gurdip&Arash(2021) ; Lukonga(2018)	Reputation risks Technological risk Security Risk Fraud risk Operational Risk
• Telecommunication devices • WLANS • LANS • Networking Cables	Deliberately hardware destruction System outages. Surging Traffic. Web security threats	Gurdip&Arash(2021) ; Lukonga(2018); Wang(2021);NSFOCUS(2018).	Reputation risks Technological risk Security Risk Fraud risk Operational Risk
• Data Centers(Servers) • Database	Information theft. Injections. Data breaches. Hacking through third-party vendors.	Akanksha(2022); Lukonga(2018)	Reputation risks Technological risk Security Risk Fraud risk Operational Risk

4.3 Approaches to Cyber Risk Assessment

Risk assessment entails a systematic process for risk identification, consequences analysis, and risk management (Aagedal et al,2002). Risk assessment needs to identify potential causes, events, and effects that could materialize in the future, and it needs to make use of suitable tools for representing or expressing uncertainties (Amundrud et al,2017). There are several approaches to cyber risk assessment and these involve understanding security posture, collecting data, modeling potential attacks, and prioritizing mitigation actions(CYE,2022).

The compliance-driven approach to cyber risk assessment compares an organization's security controls with cybersecurity and regulatory frameworks like NIST, ISO/IEC, and the European Union. These frameworks provide credible guidelines for compliance activities and basic security practices(CYE,2022).

Threat modeling approach which is a process used to identify and prioritize risks in a business context. It involves analyzing potential threats, identifying assets and access points, and identifying threats [92].Threat modeling uses approaches, like Attack Trees, STRIDE, Abuser Stories, Agile

modeling, T-MAP, CORAS, fuzzy logic, SDL Threat Modelling Tool, and Application Threat Modelling (TAM) Tool. Threat modeling can be either proactive or reactive, with reactive approaches protecting against adversarial attacks and proactive approaches defending FinTech institutions against cyber-attacks (Gurdip & Arash,2021).

Attack route analysis approach involves gathering information about likely threats and key assets, using real attackers' techniques and thought processes(CYE,2022). This helps security teams build a graph of attack routes between threats and key assets, including systems, networks, and cloud platforms. This graph helps security teams focus on real dangers and prioritize vulnerabilities that are not on an attack route leading to a critical asset or are blocked by existing controls. This approach simplifies communication with non-technical managers, allowing them to understand how threats operate and how to neutralize them by removing vulnerabilities or adding controls(CYE,2022).

Lastly, the five-step framework for conducting a cybersecurity risk assessment is as follows: scoping, risk identification, risk analysis, risk evaluation, and documentation(Cobb,2022). The first step involves determining the scope of the assessment, which can be the entire organization, business unit, location, or specific aspect of the business. The second step involves identifying cyber security risks, creating an inventory of all physical and logical assets within the scope, and identifying the consequences of an identified threat exploiting vulnerability. The third step involves analyzing risks and determining potential impact. The fourth step involves risk evaluation, prioritizing risks using a risk matrix.

The fifth step involves documenting all identified risk scenarios in a risk register, which should be regularly reviewed and updated to ensure management has an up-to-date account of its cybersecurity risks(Cobb,2022).

4.3.1 Fintech Ecosystem risk management Metamodel

The Risk Management (RM) process comprises coordinated activities aimed at guiding and controlling an organization as far as risks are concerned. These activities encompass the definition of the context of analysis, assessment, treatment, and acceptance, as well as the communication and monitoring of information security risks(Mayer&Fagundes,2009). Risk management ascertains that procedures are defined for ensuring that risks have been sufficiently managed, as well as including assessing the risk factors of IT investments (Asgarkhani,Correia,& Sarkar,(2017). Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment (Stoneburner,Goguen &Feringa,2002).In a similar study, Haneef et al (2012) argue that Risk Management encompasses risk identification, assessment, measurement, monitoring and controlling all risks inherent in the business processes.

According to Fintech Global (2021), Fintechs continue to evolve, it is essential that they prioritize risk assessment to maintain trust and credibility with their customers and regulators as well as prevent fraud.

Moreover, it is pointed out that risk assessments support organisations to navigate amid chaos and meet their strategic objectives. Thus, the process must be baked into every step of the digital transformation journey to achieve long-term success (Fintech Global,2021).

Therefore, in this study, we propose that the designed Fintech Ecosystem risk management Metamodel is beneficial in mapping and mitigating risks.

We adopt Innerhofer-Oberperfler and Breu (2006) security information meta-model as the cornerstone of the security management process to conduct a risk assessment in the Fintech ecosystem. The study adds security-relevant information to the security information meta-model by connecting the model's elements to security artifacts like Fintech Assets, Fintech Risks, threats, security incidents, and security controls. This information reflects the state of the entire Fintech ecosystem's security process.

As shown in Figure 2, the Fintech Ecosystem Risk Management Metamodel is modeled using a series of UML diagrams to represent the various aspects and demonstrate the relationships maintained between one another. A set of design notations called the Unified Modelling Language (UML) offers a number of valuable capabilities, including numerous interconnected design views. The Metamodel is illustrated in Figure 2 below.

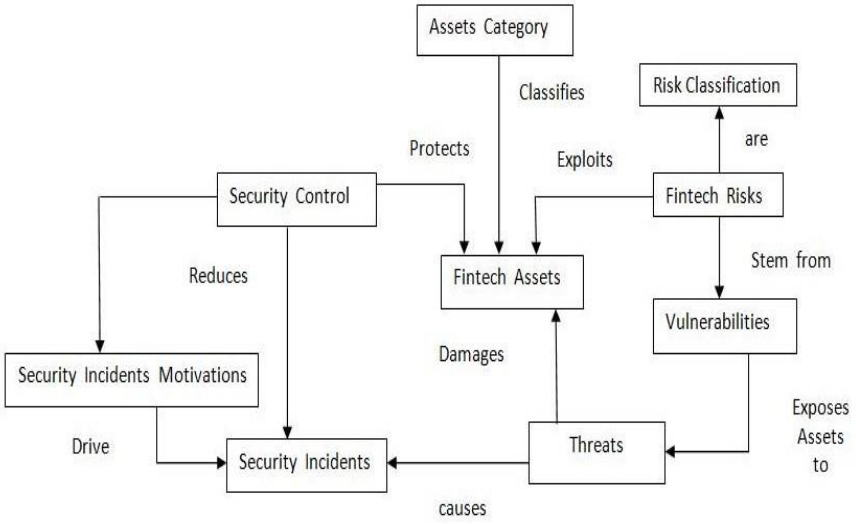


Fig. 2. Fintech Ecosystem risk management Metamodel

The Fintech Ecosystem risk management Metamodel presented in figure 2 above is explained as follows;

Fintech Assets: The central element of the Fintech Ecosystem risk management Metamodel is the concept of Fintech Assets. Fintech Assets act as a place-holder for any type of tangible or intangible entities which are necessary and have value to the Fintech organization. These key assets could be people, services, facilities, processes, etc.

Assets Category: classifies assets according to their level of sensitivity and security requirements. The criticality of an asset category can be high, medium, or low, which means that assets with high ratings are the most valuable to the organization.

Fintech Risk: these are any threats to a vulnerable asset that will cause harm to reaching business objectives.

Vulnerability: Vulnerability is the weakness in an organization's security program that is exploited by a threat to gain unauthorized access to an asset. It has three properties. i.e., impact, type, and weight score.

Threats: The concept of threat describes anything that can cause damage to an asset. The threats can be natural and political disasters, intentional actions, and unintentional actions. A threat is always related to a specific Fintech Asset. A threat is evaluated by measuring its probability and potential impact resulting in a measurement of its risk.

Risk Classification: Identifying risks and their categorization into suitable risk categories are fundamental to enterprise risk management procedures. Risk Classification enables the grouping of the resources or Fintech assets exposed to risk such as physical, human, and financial resources. Risk categorization evaluates inherent and residual risks for various processes and activities possible. Risk must be categorized based on its type, nature, and complexity.

Security incidents: A security incident is an event that may indicate that a Fintech organization's asset has been compromised or that measures put in place to protect them have failed. Security incidents are usually distinguished by the degree of severity and the associated potential risk to the organization.

Security Control: This activity identifies the possible control measures that could mitigate and eliminate identified Fintech risks related to the Fintech assets. No system is risk-free, therefore, to reduce security breaches to protect assets from the various types of threats and vulnerabilities, effective controls must be applied.

Security incidents Motivation: The number of cyber security incidents is growing rapidly. To curb these incidents, it is imperative to understand what motivations drive these cyber incidents.

In addition, the designed Fintech Ecosystem risk management Metamodel can be exploited from both a human and technology perspective. It can be leveraged as follows;

a) From a Human Perspective:

Standardization and Consistency: The metamodel provides a standardized framework for representing and organizing security-related concepts, relationships, and behaviors. By leveraging a common metamodel, Fintechs can ensure consistency in understanding and implementing security measures across human stakeholders. This reduces the chances of miscommunication, gaps in security, and inconsistencies in risk mitigation efforts.

Knowledge Sharing and Training: The metamodel can be used as a training resource for educating human stakeholders on security principles, standards, and guidelines. By promoting awareness and understanding of the metamodel, organizations can enhance the security knowledge and competence of their workforce, empowering them to identify and address security risks effectively.

Risk Assessment and Decision Making: The metamodel facilitates the identification and analysis of security risks. Human stakeholders can use the metamodel to assess risks, evaluate their potential impact, and make informed decisions regarding risk mitigation strategies. The metamodel provides a structured framework for considering various security dimensions, dependencies, and relationships, helping stakeholders prioritize and allocate resources appropriately.

b) From a Technology Perspective:

System Design and Architecture: The metamodel can guide the design and architecture of technology systems. By incorporating security considerations from the metamodel, organizations can ensure that security requirements and controls are embedded into the technology infrastructure. The metamodel can provide guidelines for secure system configurations, access controls, encryption mechanisms, and other technical security measures, reducing vulnerabilities and potential attack surfaces.

Security Controls and Monitoring: The security metamodel can be leveraged to identify and select appropriate security controls and monitoring mechanisms for technology systems. It helps in mapping security requirements to specific controls, ensuring comprehensive coverage of security risks. The metamodel can also guide the implementation of security monitoring and incident response mechanisms, enabling timely detection and mitigation of security incidents.

Integration and Interoperability: security metamodel provides a structured approach to ensure the harmonious integration of security components and their interoperability across various technology systems in complex technology environments by leveraging the metamodel, organizations can establish consistent security interfaces, data formats, and protocols, enhancing the overall effectiveness of security measures.

4.3.2 Risk Management Frameworks

Stoneburner, Goguen and Feringa (2002) asserts that a Risk Management Framework is a template and guideline used by companies to identify, eliminate and minimize risks. The literature presents a wide range of risk management frameworks. These include;

a) Enterprise Risk Management Integrated Framework

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a structured and flexible approach for managing security and privacy risks. It includes information security categorization, control selection, implementation, assessment, system and common control authorizations, and continuous monitoring(Prewett&Terry,2018). The RMF can be applied to new and legacy systems, any type of system or technology, and any organization regardless of size or sector. The framework consists of seven steps: preparing the organization, categorizing the system and information, selecting the set of controls, implementing the controls, assessing the controls, approving the system, and continuously monitoring control implementation and risks. The Enterprise Risk Management Integrated Framework from ICOSO is composed of five interrelated components: governance and culture, strategy and objective setting, performance, review and revision, and information, communication, and reporting. These frameworks help organizations identify, manage, and support the achievement of objectives while ensuring a safe and secure environment.

b) The National Institute Of Standards And Technology [NIST] Risk Management Framework (RMF)

The Risk Management Framework (RMF) is a structured and flexible approach for managing security and privacy risks. It involves categorizing information, selecting controls, implementing them, assessing their effectiveness, appointing system and common control authorities, and continuously monitoring. The RMF promotes near-real-time risk management and accountability for controls implemented within an organization's information systems. It can be applied to new and legacy systems, regardless of size or sector. The NIST Risk Management Framework (RMF) consists of seven steps (Stoneburner, Goguen and Feringa,2002). These are:

(1) It starts with essential activities to prepare the organization to manage security and privacy risks

(2) Categorize the system and information processed, stored, and transmitted based on an impact analysis

(3) Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

(4) Implement the controls and document how controls are deployed

(5) Assess to determine if the controls are in place, operating as intended, and producing the desired results

(6) Senior official makes a risk-based decision to authorize the system (to operate)

(7) Continuously monitor control implementation and risks to the system

c) The ISO 31000 standard Risk management approach

The ISO 31000 is an international standard that provides principles and guidelines for effective risk management. It is applicable to various types of risks, including financial, safety, and project risks, and can be used by any organization (ISO,2002). ISO 31000 offers a centralized and integrated risk management approach, allowing organizations to improve, coordinate, and interoperate their risk management activities. The six-part risk management process includes communication and consultation, scope, context, criteria, risk assessment, risk treatment, monitoring, review, and reporting. It promotes risk awareness, adapts the overall risk management process, and ensures design

quality and efficiency(ISO,2002). It also encourages documentation of activities, results, and decision-making to further improve risk management activities.

d) EU (ITSRM), IT security risk management methodology V1.2

The IT Security Risk Management Methodology (ITSRM²) was developed by the European Commission to establish a risk-based security model. It involves defining the scope and framework, identifying risks based on assets, security requirements, threats, and existing measures, analyzing and evaluating risks, implementing risk treatment measures, and deciding on risk acceptance(Hutchins,2018). The methodology also includes a continuous monitoring and review process, and a risk communication process for exchanging information about risk with stakeholders.

In a nut shell, the above frameworks can be leveraged by Fintechs in managing cyber security threats, operational disruptions, data breaches, and regulatory changes, aiding in risk identification, assessment, monitoring, and mitigation, aligning with regulations, promoting compliance, and fostering innovation in the industry.

5. CONCLUSION

In conclusion, this research paper has delved into the critical realm of Fintech resilience by comprehensively examining security risks and proposing effective risk management strategies. The dynamic landscape of financial technology demands a proactive and vigilant approach to ensure the integrity, continuity, and security of operations. The research paper explores the security landscape within the Fintech sector, identifying and understanding the diverse risks that pose threats to the Fintech Assets.

The paper provides valuable insights into innovative risk mitigation approaches, considering the dynamic nature of the Fintech environment. Special attention is given to the collaborative frameworks that contribute to enhancing the sector's overall resilience.

The study proposes a Fintech Ecosystem Risk Management Metamodel to illustrate the practical application of risk management in addressing security challenges for the sector. By leveraging the metamodel, organizations can establish consistent security interfaces, data formats, and protocols, enhancing the overall effectiveness of security measures. The findings aim to equip industry practitioners, policymakers, and researchers with a nuanced understanding of the interconnected dynamics between security risks and effective risk management in the Fintech landscape. This study recommends that governments and Fintech industry adopt the proposed approach for Fintech risk assessment and management.

FUNDING: This article did not receive any specific grant from funding agencies in the public, commercial or Not for Profit Sectors.

CONFLICT OF INTEREST: AUTHORS DECLARE THAT THEY HAVE NO CONFLICT OF INTEREST.

REFERENCES:

1. Aagedal, J.O., Den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D. and Stolen, K. (2002).September. Model-based risk assessment to improve enterprise security. In Proceedings. Sixth International Enterprise Distributed Object Computing (pp. 51-62). IEEE.

2. Akanksha, M. (2022).Top 10 Fintech API Security Risks and Challenges. Available at: https://www.valuebound.com/resources/blog/top-10-fintech-api-security-risks-and-challenges.

3. Alijoyo, F.A. (2022). The use ISO 31000: 2018 in Indonesian Fintech Lending Companies: What Can We Learn?. Journal of Business and Management Studies, 4(1), pp.16-22.

4. Alliance for Financial Inclusion(AFI),(2020).Creating Enabling Fintech Ecosystems: The Role Of Regulators.Special Report.

5. Amundrud, Ø., Aven, T. and Flage, R.(2017). How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231(3), pp.286-294.

6. Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M.F., (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, p.113580.

7. Asgarkhani, M., Correia, E. and Sarkar, A. (2017). February. An overview of information security governance. In 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (pp. 1-4). IEEE.

8. Callen-Naviglia, J. and James, J.(2018).FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY. Issues in Information Systems, 19(3).

9. Cernisevs, O., Popova, Y. and Cernisevs, D.(2023). Risk-Based Approach for Selecting Company Key Performance Indicator in an Example of Financial Services. In Informatics (Vol. 10, No. 2, p. 54). MDPI.

10. Cobb,M.,(2022).How to perform a cybersecurity risk assessment in 5 steps. Available at: https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

11. CYE.(2022). A Step-By-Step Guide to Cyber Risk Assessment: How to strengthen your security posture and optimize security investments by assessing and prioritizing cyber risks.

12. Dattani, I.(2016).Financial Services and Fintech A review of the Cyber Security threats and implications. Technical Report. Research gate.

13. Dunn Cavelty, M., (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and engineering ethics, 20, pp.701-715.

14. Fenwick, M., and Erik PM V. (2020).Banking and regulatory responses to FinTech revisited-building the sustainable financial service'ecosystems' of tomorrow.: 165-189. Singapore Journal of Legal Studies Mar 2020.

15. Fintech Global (2021).Why risk assessment is important for financial institutions in a digital era. Available at https://fintech.global/2021/03/25/why-risk-assessment-is-important-for-financial-institutions-in-a-digital-era/

16. Gomber,P., Robert J. Kauffman, Chris Parker & Bruce W. Weber.(2018).On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services, Journal of Management Information Systems, 35:1, 220-265, DOI:10.1080/07421222.2018.1440766.

17. Govindraj, B. (2022). Understanding Fintech Security Concerns For A Safer Fintech Ecosystem. Global Business Head Available at: https://www.appsealing.com/fintech-security-concerns/.

18. Gurdip,K., and Arash, H.,L.(2021). Understanding cybersecurity management for FinTech: cybersecurity threats in FinTech (Article 3) Available at: https://www.itworldcanada.com/blog/understanding-cybersecurity-management-for-fintech-cybersecurity-threats-in-fintech-article-3/462547

19. Hamilton.A.(2020). 2020 review:Top five cyberattacks this year. Available at: https://www.fintechfutures.com/2020/12/2020-review-top-five-cyberattacks-this-year/

20. Haneef, S., Riaz, T., Ramzan, M., Rana, M.A., Hafiz, M.I. and Karim, Y. (2012). Impact of risk management on non-performing loans and profitability of banking sector of Pakistan. International Journal of Business and Social Science, 3(7).

21. Hutchins, G. (2018).ISO 31000: 2018 enterprise risk management. Greg Hutchins.

22. IBM.(2023).What are security controls?.Available at: https://www.ibm.com/topics/security-controls

23. Innerhofer-Oberperfler, F. and Breu, R. (2006).Using an Enterprise Architecture for IT Risk Management. In ISSA (pp. 1-12).

24. ISO, (2002). Risk management vocabulary. ISO/IEC Guide 73

25. Kaur, G., Lashkari, Z.H. and Lashkari, A.H. (2021).Understanding Cybersecurity Management in FinTech. Springer International Publishing.

26. Keong, O. C., Leong, T. K., & Bao, C. J. (2020). Perceived Risk Factors Affect Intention To Use FinTech. Journal of Accounting and Finance in Emerging Economies, 6(2), 453–463.

27. Khalil, F. and Alam, H.M.(2020).Identification of Fintech Driven Operational Risk Events. Journal of the Research Society of Pakistan, 57(1), p.75.

28. Krejcie, R. V., & Morgan, D. W.(1970). Determining sample size for research activities. Educational and

psychological measurement, 30(3), 607-610.

29. Kure, H.I., Islam, S. and Razzaque, M.A.(2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), p.898.

30. Lake, A.J.(2013). Risk management in Mobile Money: Observed risks and proposed mitigants for mobile money operators. World Bank.

31. Li, Y. and Liu, Q., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, pp.8176-8186.

32. Lukonga,I.(2018). Fintech, Inclusive Growth and Cyber Risks: A Focus on the MENAP and CCA Regions. IMF Working Paper.

33. Machi, L. A., & McEvoy, B. T. (2016).The literature review: Six steps to success.

34. Maseno, E.M.; Ogao, P. Matende, S.(2017).Vishing Attacks on Mobile Platform in Nairobi County Kenya. Int. J.Adv. Res. Comput. Sci. Technol.

35. Mayer, J. and Fagundes, L.L.(2009). A model to assess the maturity level of the risk management process in information security. In 2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops (pp. 61-70). IEEE.

36. Mehrotra, A. and Menon, S. (2021). Second round of FinTech-Trends and challenges. In 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 243-248). IEEE.

37. Muhn, J. (2020).Cybersecurity: The Hidden Risks of Fintech Services" .Available at https://finovate.com/cybersecurity-the-hidden-risks-of-Fintech-services/. Accessed on 25th-June-2020. [108]NSFOCUS.: 2017 Fintech Security Analysis Report. Available at: https://nsfocusglobal.com/2017-fintech-security-analysis-report/.(2018)

38. Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 96, 227-242.

39. NSFOCUS.(2018).2017 Fintech Security Analysis Report. Available at: https://nsfocusglobal.com/2017-fintech-security-analysis-report/.

40. NSFOCUS.(2018).2017 Fintech Security Analysis Report. Available at: https://nsfocusglobal.com/2017-fintech-security-analysis-report/.

41. Park, J. K., & Kim, I. (2015).A Study of Countermeasure against Security Risk of Fintech Services for Financial Innovation. Knowledge Management Research, 16(4), 35-45.

42. Prewett, K., & Terry, A. (2018).COSO's updated enterprise risk management framework—A quest for depth and clarity. Journal of Corporate Accounting & Finance, 29(3), 16-23.

43. Razzaque, A., Cummings, R. T., Karolak, M., & Hamdan, A. (2020).The Propensity to Use FinTech: Input from Bankers in the Kingdom of Bahrain. Journal of Information and Knowledge Management, 19(1), 1–22.

44. Sampat, B., Mogaji, E., & Nguyen, N. P. (2023).The dark side of FinTech in financial services: a qualitative enquiry into FinTech developers' perspective. International Journal of Bank Marketing.

45. Santa, R. and Carlos, H.,(2014). Physical and Infrastructure Security IT. Computer Science.

46. Stoneburner, G., Goguen, A. and Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), pp.800-30.

47. Tunggal,A.,T.(2023). Cybersecurity:How to Perform a Cybersecurity Risk Assessment (2023 Guide). Available at: https://www.upguard.com/blog/cyber-security-risk-assessment

48. UN (2021).CEPA strategy guidance note on Risk management frameworks.

49. Vellani, K.(2006). Strategic security management: a risk assessment guide for decision makers. Elsevier.

50. Vučinić, M.(2020). Fintech and Financial Stability Potential Influence of Fintech on Financial Stability, Risks and Benefits. Journal of Central Banking Theory and Practice, 9(2), pp.43-66.

51. Wang,J.(2021).4 Security Issues Fintech Firms are Facing. Available at: https://www.imc.edu.au/news-archive/4-security-issues-fintech-firms-are-facing.

52. Whitman, M.E. and Mattord, H.J.(2021). Principles of information security. Cengage learning.

53. World Bank.(2021). Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches. World Bank.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 39 – 49 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

NEURO-CRYPTOGRAPHIC HYBRID SYSTEMS: UNLEASHING THE POWER OF NEURAL NETWORKS FOR CRYPTANALYSIS AND ENCRYPTION

Luka Baklaga[1]
[1]Research and Development Department, Researcher, Business and Technology University, Georgia

ABSTRACT: Neural cryptography is a field that blends neural networks and cryptographic algorithms. This approach offers promising solutions to address security concerns with traditional cryptographic methods. This article explores the transformative potential of hybrid neurocryptographic systems through a comprehensive analysis. The methodology combines independent analysis, theoretical investigation, and quantitative testing. With the rise of digital data exchange, storage, and transmission, information security is more crucial than ever. Cryptographic algorithms can protect data, verify identities, and reduce various attacks. The study demonstrates how hybrid systems using neural networks and cryptography could revolutionize cryptography processes. Cryptanalysis methods have advanced due to increased computing power, becoming effective in information security. Traditional cryptographic protocols employ well-known ciphertexts and number theory techniques. This study proposes a mathematical cryptography model utilizing deep learning (DL), specifically neural networks. The model aims to protect plaintext through rapid distribution of neural network layers. The process begins by developing a new cryptography module emphasizing the use of neural networks for encryption and cryptanalysis. It implements a novel approach to secure authentication by dynamically converting biometric data into encryption keys using neural networks, instead of standard key storage techniques. Innovative security protocols offer lightweight block ciphers such as S-DES, which combine number theory and neural network architecture in their experimental endeavors. Using each neural cryptanalysis result as a key bit, the work carefully examines how key differences impact S-DES. In neural cryptography, the same input vector is received by both communicating networks, which then use it to generate and train an output bit. A special phenomenon can be observed in the dynamics of two networks and their weight vectors: they synchronize to a state in which their time-dependent weights are the same. Theoretical work explores the complex relationships between neural network architectures and cryptographic techniques, focusing on the creation of sophisticated encryption algorithms, complex network decoding, and the optimization of internal security protocols. The goals place a strong conceptual focus on promoting innovation, improving safety and maximizing effectiveness. This is a critical first step toward integrating neural networks into the framework of cryptographic advances in protocol system security. The next research study aims to develop and apply efficient formulas, tools and algorithms to meet the needs of quantum-based cryptography. For example, by combining quantum mechanics and deep learning, completely secure quantum neural network cryptography can be created.

KEYWORDS*:* deep learning, neural networks, cryptography, number theory, neurocryptography, Gated Recurrent Units

1. INTRODUCTION

The swift expansion of digital information sharing, storage, and transfer has underscored the criticality of data security measures. Traditional cryptographic techniques, while effective, face increasing vulnerabilities due to advancements in computing power and cryptanalysis methods. This study delves

into the exceptional potential of hybrid neurocryptographic systems, which seamlessly integrate neural networks with cryptographic algorithms, to catalyze a transformative revolution in cryptographic processes and protocols. Cryptanalysis of block ciphers has consistently garnered a lot of attention, and many new cryptanalytic approaches have appeared recently (Uludag et al. 2004). Cryptoanalysis based on algebraic structural algorithms can be classified into directed modules of different segments (Biehl and Caticha 2001), such as differential cryptanalysis, linear cryptanalysis, differential-linear cryptanalysis, meet-in-the-middle attack, and related-key attack (Biham and Shamir 1993). One of the most important aspects of information technology development is information security. Developing and implementing new security measures for information systems is crucial nowadays. Modern cryptography has used strong algorithms to improve information security. On the other side, increasingly sophisticated attacks have appeared. These attacks take advantage of enhanced computing capabilities and methodologies based on artificial intelligent tool so called machine learning. The efficacy of artificial neural networks (ANNs) and deep learning methods in addressing intricate classification issues has motivated scholars and technological enterprises to utilize these approaches for cryptanalysis and cryptography within the realm of number theory (Hertz, Krogh, and Palmer 1991). In recent years, there has been a surge of interest in neural networks as a potential computational model for comprehending the functioning of the human brain. Illustrative instances provide valuable learning material for neural networks. Extensive research has been conducted on this concept utilizing statistical mechanics models and methodologies (Yamashita et al. 2018). Dynamic neural networks are a common occurrence employed within cryptographic systems. Limitations in the fundamental cryptography process prompted the development of cryptographic systems with shorter keys, also known as secret key systems (Danziger and Henriques 2014). The security of a cryptographic system is contingent upon the confidentiality of the key. Neurocryptography examines using neural networks and probabilistic algorithms for encryption and cryptanalysis. It tackles public key cryptography, key distribution, hashing, and pseudo-random number generation. Neural networks excel at parallel processing, equipping them to handle varied future tasks. However, their complex setup often limits practical use. These networks demonstrate skill in recognizing intricate patterns and mappings, making them adept at addressing cryptography's computational challenges. Combining neural networks with cryptography offers enhanced security measures. This study aims to develop an innovative cryptographic model using neural networks for encryption and code-breaking tasks. The proposed approach converts biometric data into dynamic encryption keys through neural networks, providing secure authentication without storing conventional keys. Additionally, the research explores integrating neural networks with lightweight block ciphers (Gomez et al. 2018), merging number theory principles with neural network architectures to create cutting-edge security protocols. Furthermore, by analyzing key differences' impact on S-DES encryption, the study examines the intricate relationships between neural network outputs and cryptographic key generation. In this paper, we use artificial neural networks to generate new directions for cryptographic probability protocols. The networks are trained using generated data that identifies protocol weaknesses as well as the encryption key, which is unique to each experimental portion. This scientific article intends to develop a cryptographic algorithm using neural network modular systems and analyze a biometric sample to create a cryptographic key. Additionally, it aims to develop a Neurocryptographic Sequence-to-Sequence autoencoder model software using a mathematical approach and simulation in Python. Finally, it aims to test and optimize the use of the developed algorithm. We offer the technique and results in accordance with our study goal: in Section 3, we exhibit the methodology, research design, and numerous experiments related to the establishment of neural-based cryptography and its cryptoanalysis inside mathematical modeling, as well as the proposed outcomes. Section 4 presents a summary of the experimental findings, the conclusion of the research, and its future path.

This study investigates the comprehensive capabilities of combined neurocryptographic systems through a methodical approach involving theoretical analysis, quantitative evaluations, and digital simulations. The outcomes reveal possibilities for pioneering encryption algorithms, sophisticated network decryption methods, and optimized security protocols. These advancements foster innovation, bolster security measures, and maximize efficiency in cryptanalysis and encryption pursuits.

2. OBJECTIVES

This study aims to explore novel cryptographic frameworks and procedures utilizing deep learning techniques like neural networks. Its objectives encompass: developing methods for enhanced threat detection and robust key security; discerning the transformative capabilities of hybrid neurocryptographic systems in reshaping autonomous environments' cryptographic processes. Key areas of focus include fostering innovation, fortifying security measures, and optimizing efficiency in pursuit of cryptanalytic and encryption objectives. The research strategically integrates diverse perspectives to drive advancements in this domain.

3. RESEARCH METHODOLOGY

3.1. Research design

This research uses a thorough and coherent methodology that combines independent analysis, theoretical investigation and quantitative testing to study hybrid neurocryptographic systems. To develop a new cryptographic module, the project focuses on sharing the capabilities of neural networks for encryption and cryptanalysis. To create a secure authentication system, the project will use neural networks to convert a biometric sample into an encryption key. Instead of storing and using cryptographic keys later, this solution uses neural networks to generate and authenticate them. Experiments were conducted with lightweight block ciphers such as S-DES, where the block size was represented by x-points and the key length was represented by y-points. By applying number theory and neural network architecture, a state-of-the-art security protocol should be developed. The impact of key differences on ciphers was also investigated, as each output in neural cryptanalysis represents a key bit. The study begins with a comprehensive literature review that uses a meta-analytic approach to assess the body of knowledge on the integration of neural networks and cryptographic systems. Theoretical research deals with the complex interplay between neural network architectures and cryptography methods. Sophisticated encryption algorithms, complex network decoding and optimization of security protocols are priorities in the context of security systems.
This digital platform facilitates the creation, testing and validation of the proposed hybrid neurocryptographic systems using the Jupyter notebook and appropriate Python modules. By combining ideas from neural network theory and cryptography techniques, neural network design is scientifically defined. To achieve a quantitative combination, some basic properties from the theory of random walks in limited domains were applied. A combination analysis was performed to determine how different parameter choices affect the convergence rate. The smooth transition between theoretical understanding and digital experiments is highlighted by this research design. While digital experiments confirm the feasibility and effectiveness of the proposed hybrid neurocryptographic system, the theoretical foundations guide the development of the neural network-based cryptographic architecture.

3.2. Research experiment - Neural Network-based Encryption using Modular Arithmetic

In this study, we aim to develop a cryptographic algorithm utilizing neural networks that will integrate principles of modular arithmetic derived from number theory. The neural network will be tasked with generating encryption keys based on the input plaintext, and the encryption process will involve modular arithmetic operations. The primary framework will be described as a Neural Network-based Encryption using Modular Arithmetic. The neural network serves as a tool for generating and authenticating keys, while modular arithmetic operations play a role in the encryption and decryption processes. The experimental model commences with the data preprocessing stage, where the input plaintext message is designated as *Mp*. The initial stage involves transforming the variable *Mp* into a numerical format suitable for input into the neural network. A frequently employed method involves the utilization of ASCII or Unicode code points, whereby the numerical value of each character in *Mp* is determined. In mathematical terms, this can be expressed as:

$$Mp = \{c_1, c_2, \dots, c_n\} \rightarrow \text{ encoding } \rightarrow \{x_1, x_2, \dots, x_n\}$$

The mathematical expression *ci* denotes the *i-th* character in the set *Mp*, while xi represents the associated numerical value derived from the encoding scheme. Subsequently, the numerical values are adjusted to a suitable range for utilization as input to the neural network, commonly falling within the range of 0 to 1. One way to accomplish this is by employing min-max normalization:

$$x_i' = \frac{x_i - min(X)}{max(X) - min(X)}$$

In the context of a given set *X*, denoted as *{x 1, x 2, ..., x n}*, the term *x_i'* represents the normalized value associated with the original value *x_i*. An appropriate neural network structure for generating cryptographic keys, such as a feedforward or recurrent neural network (RNN), is developed and trained utilizing preprocessed plaintext data as the input. The intended result of the neural network is the specified length of the key, which is represented as *k*. The neural network model, denoted as *F theta* and characterized by the parameters theta, is specifically created for the purpose of generating keys. The training process involves using the preprocessed plaintext data *M p* as the input and the desired key length k as the target output for the network. The process of generating keys can be expressed as:

$$K = f_\theta(M_p')$$

M p' represents the normalized numerical representation of *M p*, while *K* denotes the encryption key of length *k*. Regulation methods such as dropout or *L2* regularization can be utilized during training to mitigate overfitting and enhance generalization. The neural network is effectively trained by minimizing a suitable loss function, which may involve mean squared error or cross-entropy loss, depending on the specific nature of the problem being addressed. In order to develop an encryption algorithm utilizing modular arithmetic, it is necessary to establish a modulus *M*, which should be a large prime number, for conducting the modular arithmetic operations. It is necessary to divide the numerical representation of the plaintext *Mp′* into blocks of size *n* (e.g., 8 bits for byte-level encryption):

Where, modular definition of *Bi* represents the *i*-th block of size *n*. For each plaintext block *Bi* within research experiment we have to use the trained neural network f_0 to generate a key *Ki* of length *n* based on the plaintext block *Bi*:

$$M_p' = \{B_1, B_2, \dots, B_m\}$$

It is necessary to execute the encryption process utilizing modular addition:

$$K_i = f_\theta(B_i)$$

Where, *Ci* is the corresponding ciphertext block. It is essential to combine the ciphertext blocks in order to produce the ultimate encrypted message *C*:

$$C_i = (B_i + K_i) mod M$$

Where, *"/"* denotes concatenation. The decryption algorithm for ciphertext *C* follows the same method, wherein the recovered plaintext blocks are concatenated to obtain the original message *Mp′*:

$$C = C_1 | C_2 | \dots | C_m$$

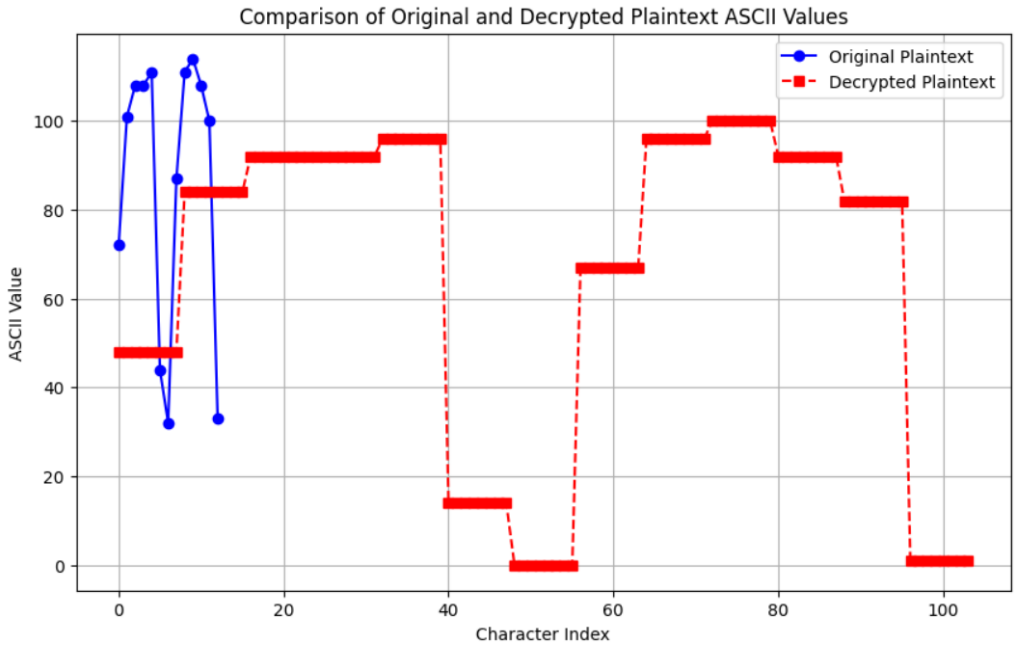
Which perform the inverse normalization of model and decoding steps to recover accurate visualized original plaintext message *Mp*.

To demonstrate the presented algorithmic methodology and the process of encryption and decryption, we shall examine a straightforward illustration. Let us assume that we possess a plaintext message, namely "Hello, World!" and aim to apply the proposed encryption scheme based on neural networks, incorporating a modulus M=257 (a prime number) and a block size of *n*=8 bits. Firstly, we need to maintain Data Preprocessing stage where we have to encode the plaintext characters into their ASCII numerical representations:

"Hello, World!" -> [72, 101, 108, 108, 111, 44, 32, 87, 111, 114, 108, 100, 33]

Subsequently, standardize the quantitative values within a specified range [0, 1]: [0.28, 0.39, 0.42, 0.42, 0.43, 0.17, 0.12, 0.34, 0.43, 0.44, 0.42, 0.39, 0.13]. Then, it is necessary to navigate through the indicated algorithmic metrics from Key Generation using Neural Network to Encryption Algorithm based on Modular Arithmetic, where we concatenate the ciphertext blocks to obtain the final ciphertext and Decryption Algorithm where we have to perform the inverse normalization and decoding steps to recover the original plaintext message. This simulation describes the whole process of encryption and decryption using the neural network and modular arithmetic proposed encryption scheme. The pseudocode algorithms explain the steps in sequence that turns the keys, encryption and decryption in order to better understand the process.

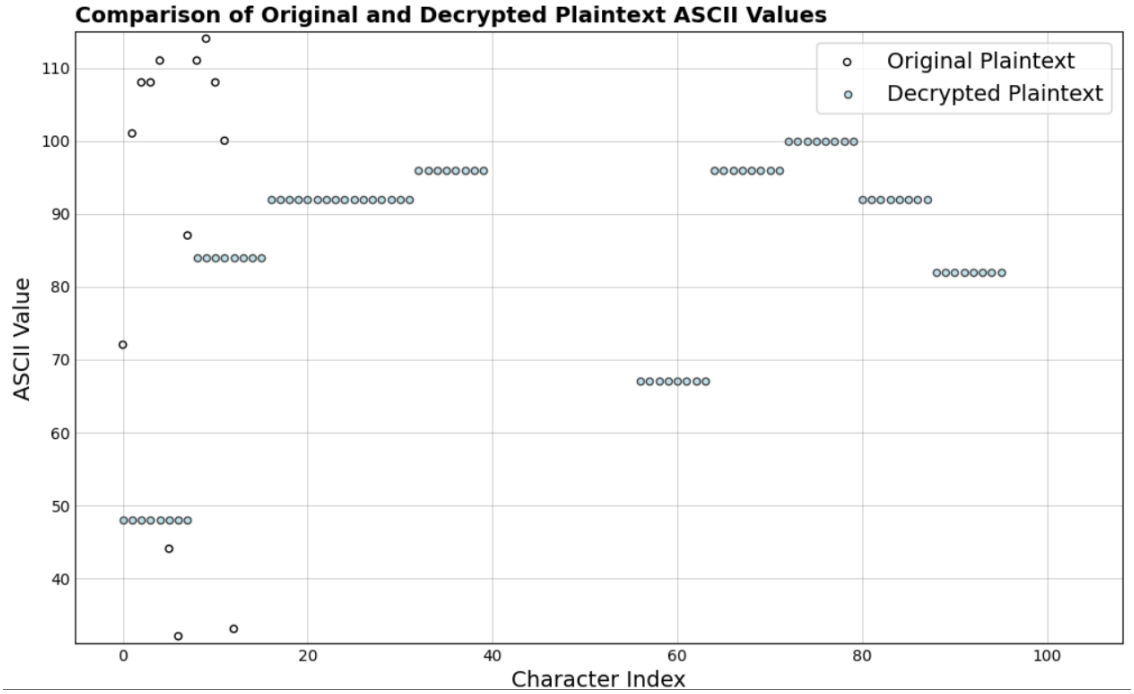
***Fig.1**. Visualization of Original and Decrypted Plaintext ASCII Values*



Simulated plot draws two different sets of points – the original plain text ASCII values as blue circles and the decrypted plain text ASCII values as red square like figure– on the same horizontal axis (X-axis). Both the X-axis, of course, contains the values from 0 to the total number of characters of the plain text. From the coincidence between the original plain text and the decrypted plain text ASCII values, you can determine how exact or accurate the modular arithmetic-based encryption method using neural network is When the code completes its execution, it prints the plaintext that the user had entered at the very start, two encrypted blocks of ciphertext and three separate strings of plaintext for each

encrypted ciphertext block, that the user needs to inspect. In brief, the given code does data preprocessing, key generation, encryption and decryption and visualisation of a miniature yet remarkably efficient neural network-based encryption scheme leveraging modular arithmetic. In order to illustrate the fundamental principle of the model, different simulation approaches have been utilized, and the resulting figures are saved in PDF format. This format is preferred due to the higher quality of figures produced by vector graphics formats.

***Fig.2**. Visualization of Original and Decrypted Plaintext ASCII Values*



As can be viewed from the resulting graph, two sets of points are linked together by red dashed vertical lines representing the original plaintext ASCII and the plaintext ASCII reconstructed using the neural-network-based encryption scheme modulo arithmetic. The blue circles show the initial ASCII codes of the plaintext 'Hello, World!' These points represent the ground truth, acting as a reference for evaluating the performance of the decryption process. Meanwhile, the light blue markers show the ASCII codes reconstructed at the decryption stage from the 2 coded ciphers. In general, the successful implementation of the neural network-based encryption technique is validated by the consistent alignment of the majority of the blue circles and light blue ones. Nevertheless, evident inconsistencies in specific areas indicate a possibility for enhancing accuracy and precision in future iterations.

3.3. RESEARCH EXPERIMENT 2 - A NEUROCRYPTOGRAPHIC SEQUENCE-TO-SEQUENCE AUTOENCODER MODEL WITH GATED RECURRENT UNITS: A TENSORFLOW FORMULATION

3.3.1 Experimental Setup

The dataset employed in the experiments comprises randomly generated binary data that represents plaintext messages and encryption keys. The function {random_bools} produces a set of binary data

with a specified size [size, n], with size representing the quantity of samples and n denoting the number of bits per sample.

The experiential variables utilized in the trials are:

- Text size: 16 (size of the input plaintext message)
- Key size: 16 (size of the encryption key)
- Learning rate: 0.0008
- Batch size: 4096
- Sample size: 20480 (4096 * 5)
- Epochs: 8000
- Steps per epoch: 5 (calculated as int(sample_size / batch_size))
- ITERS_PER_ACTOR: 1 (number of iterations for training Alice/Bob's models)
- EVE_MULTIPLIER: 2 (Eve's model is trained 2x for every step of Alice/Bob)

The experiments were carried out using Google Colab, an online Jupyter notebook platform.

3.3.1 Experiment – Mathematical modeling

There has been an introdused type of cryptography analysis within the TensorFlow library (TensorFlow n.d.), which is the starting point for improving its architectural accuracy. TensorFlow has gained widespread popularity as a machine-learning framework. TensorFlow is a versatile framework for performing tensor-based computations within a graphical structure. When delving into the area of cryptography within the field of Computer Science, one may observe that cryptographic algorithms often involve the manipulation of vectors and matrices of bytes in a graph structure. One may begin to discern the direction in which this is heading. There is simillarity of Deep Neural network architecture structure and Feistel Network from the DES cipher. The Feistel Network functions by partitioning the input into two equal parts (a left half and a right half) and passing those parts through 16 iterations (Zhao et al. 2019). In the event that a pseudo-random function F is provided, the subsequent iteration of the encryption algorithm *(left half: Li+1, right half: Ri+1)* is calculated as:

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

Similarly, the decryption algorithm functions in a reciprocal manner can be represented as shown equation:

$$L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$$
$$R_i = L_{i+1}$$

In the context of research experimentation, a TensorFlow implementation of a semi-supervised sequence-to-sequence model with an architecture similar to an autoencoder has been conducted. The framework is comprised of three prominent figures within the cryptography community: Alice, Bob, and Eve. Alice and Bob communicate securely using a shared secret key, while Eve tries to eavesdrop on their communication. The model is trained using a custom loss function that encourages Bob to correctly reconstruct Alice's messages while discouraging Eve from doing the same.

The model is formulated utilizing the Keras functional API and is comprised of internal tool layers arranged in a sequential manner during its integration process. The input layers are responsible for processing Alice's message, Bob's message, or Eve's message if she is the current agent. Input layers are taken by Alice (A), Bob (B), and Eve (E) respectively, they take *XA∈Rlin*

and $K \in Rk$ (the secret key) as inputs where *lin* represents the number of time steps in the input sequence and *k* denotes the dimensionality of the key space. Regarding Eve, who lacks the means to obtain the key, only $XE \in Rlin$ serves as her input:

$$A(X_A, K) = \text{Encoder}(X_A, K)$$
$$B(X_B, X_A') = \text{Decoder}(X_B, X_A')$$
$$E(X_E) = \text{Attacker}(X_E)$$

Where the Encoder, Decoders, and Attackers represent the structural designs of the respective agents, and $XA' = Encoder(XA)$ corresponds to Alice's encoded message obtained through encryption. The second Densely Connected Layer Consolidates Alice's message and the common key through link followed by a completely associated layer:

$$C(X_A, K) = W_d \cdot (\text{ Concatenate } [X_A, K]) + b_d$$

Here, W_d and b_d refer to the weight matrix and bias vector associated with the densely connected layer. Third Convolutional Layer performs a convolution operation along the time dimension, reducing the sequence length, and applies sigmoid activation to ensure stability:

$$S(X) = \sigma\left(\sum_{i=0}^{n_f} w^i * X_{(t-i)} + b\right)$$

$$y = \frac{1}{1 + \exp(-x)}$$

In this equation, *w* stands for filter weights, *b* signifies bias, *nf* indicates the number of filters, and σ denotes the sigmoid activation function. The Recurrent Layer makes use of Gated Recurrent Units (GRUs). Given the input *x* with dimensions (*batch_size*,*seq_len*,*feature_dim*), the GRU cell generates an output sequence *y*:

$$r_t = \sigma(W_r \cdot x_t + V_r \cdot h_{t-1})$$
$$u_t = \sigma(W_u \cdot x_t + V_u \cdot h_{t-1})$$
$$h_t' = \tanh\big(W \cdot x_t + V \cdot (r_t \circ h_{t-1})\big)$$
$$h_t = u_t \circ h_{t-1} + (1 - u_t) \circ h_t'$$

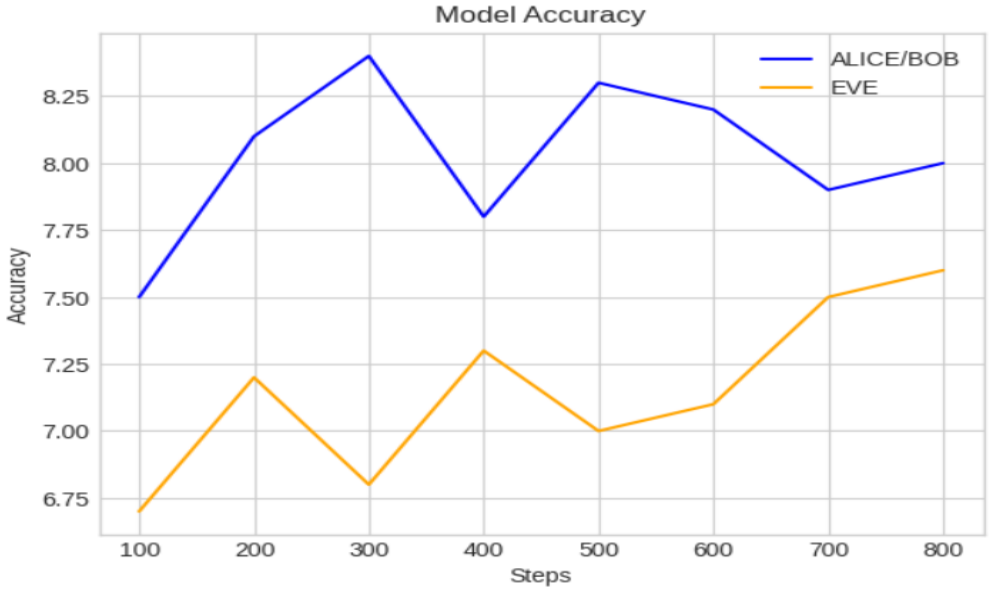
Where *W*, *V*, *Wr*, *Wu*, *Vr*, and *Vu* are weight matrices, and *rt*, *ut*, and *ht′* are reset gates, update gates, and candidate activations, respectively. Final convolutional layer generates the output sequence using a final convolutional layer coupled with a scaled tanh activation function:

$$O(X) = \alpha \cdot \tanh\left(\sum_{i=0}^{n_f} w^i * X_{(t-i)} + b\right)$$

Here, α denotes scaling factor ranging between −1 and 1. The cryptosystem is trained with the Adam optimizer and the mean absolute error loss function. Alice and Bob's models are trained to reduce the reconstruction loss between the original and decrypted messages. Eve's model is trained to reduce the absolute difference between encrypted and decrypted messages. The model's learning process involves repeated iterations through the dataset, spanning numerous cycles and steps within each cycle. During each step, a subset of messages and their corresponding keys are provided as input to the models, enabling model optimization using the Adam algorithm. The losses incurred during this process are displayed at regular intervals, specifically after every 100 steps, to monitor the training progress. The

training and testing losses are stored in separate lists and plotted using Matplotlib. The training loss progression shows the reconstruction loss for Bob and Eve, while the testing loss progression shows the reconstruction loss for Alice and Eve.

***Fig.3**. Evolution of Alice/Bob vs. Eve Accuracy during Simulation*



The visualization illustrates the dynamic interplay between Alice/Bob and Eve in their encryption contest. The x-axis represents the training steps, while the y-axis depicts accuracy. Throughout the training process, both curves experienced fluctuations, with Alice/Bob's accuracy generally surpassing Eve's. However, Eve remained persistent, occasionally increasing her accuracy at the expense of Alice/Bob's performance. This simulation highlights the complex dynamics inherent in training intelligent agents with conflicting objectives. Although Alice/Bob maintained the integrity of their secure communication channel, Eve consistently challenged them, driving advancements in the ongoing cat-and-mouse game of cryptography.

4.0. RESULTS AND DISCUSSION

The results illustrate the potential of combining neural networks and cryptography to create robust e-ncryption systems. The proposed encryption model using neural networks and modular arithmetic demonstrated high accuracy in encrypting and decrypting plaintext messages. The visualization of the decrypted plaintext ASCII values aligned closely with the original metrical definitions, validating the model's effectiveness (Fig. 1 and Fig. 2). However, slight discrepancies existed, suggesting room for improving accuracy and precision. The custom loss function facilitated the training process, enabling Bob's model to accurately reconstruct Alice's encrypted messages while preventing Eve from de-crypting the ciphertext (Fig.3). The convolutional and recurrent layers of the neural network architecture could learn the complex mapping between plaintext, keys, and ciphertext. As a whole, the hybrid neurocryptographic approach has demonstrated its ability to utilize the advantages of deep learning and traditional cryptography, leading to the development of advanced security solutions that can withstand new threats and establish a foundation for future quantum neural cryptographic protocols.

4.1. Conclusion

This research explored an approach that fuses the strengths of neural networks with cryptographic algorithms. The goal was to create a novel encryption scheme, drawing upon the advantages of both domains. The proposed method combined neural networks and modular arithmetic to encrypt and decrypt messages. The results were impressive, accurately reconstructing the original data. A customized loss function played a crucial role, enabling effective training. This ensured secure communication between authorized parties while preventing eavesdropping. These findings highlight the immense potential of combining neural networks and cryptography. Such hybrid approaches offer promising solutions to address growing security concerns and computational challenges faced by traditional encryption techniques. Utilizing the capabilities of deep learning and the flexibility of neural networks, these hybrid systems present a promising avenue for advancing the development of encryption solutions that are more durable, resistant, and efficient, offering guidance for securing quantum and forthcoming decentralized network systems.

4.2. Future Work and Implications

The encouraging findings of this study present new opportunities for further investigation and have significant repercussions for the discipline of cryptography and information security. The proposed encryption system exhibited acceptable accuracy, but improvements can minimize inconsistencies and refine encryption and decryption processes. Sophisticated neural networks like attention mechanisms or transformer architectures could potentially boost performance and adaptability. As quantum computing advances, integrating quantum algorithms and quantum neural networks into neurocryptographic frameworks is vital for developing quantum resistant encryption schemes. Hybrid neurocryptographic systems' applicability should extend to multimedia data encryption, secure communication networks, and privacy preserving data analysis within a rigorous mathematical framework for designing and analyzing hybrid environments. Data security is crucial, and as technology advances, industries require robust protection. Hybrid neurocryptographic systems show promise, combining diverse fields like cryptography, machine learning, and computer science. Their successful development could enhance overall security landscape by providing highly effective and adaptable data protection solutions. This research highlights the potential benefits of interdisciplinary collaboration. By bringing together experts from various fields, we can transcend traditional boundaries and unlock innovative solutions through combined knowledge and expertise. By addressing future research directions and capitalizing on the implications of this work, neurocryptography can continue to push boundaries and meet the ever-growing demands for secure data protection in the digital age.

ETHICAL STATEMENT

This study does not contain any studies with human or animal subjects performed by any of the authors.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to this work.

REFERENCES

1. Yamashita, R., Nishio, M., Do, R. K. G., & Togashi, K. 2018. "Convolutional neural networks: an overview and application in radiology." *Insights into Imaging* 9 (4): 611-629.
2. Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. 2004. "Biometric cryptosystems: issues and challenges." *Proceedings of the IEEE* 92 (6): 948-960.
3. Biham, E., & Shamir, A. 1993. *Differential Cryptanalysis of the Data Encryption Standard.* Berlin: Springer.
4. Zhao, S., Duan, X., Deng, Y., Peng, Z., & Zhu, J. 2019. "Improved meet-in-the middle attacks on generic Feistel constructions." *IEEE Access* 7: 34416–34424.
5. Bost, R., Popa, R. A., Tu, S., & Goldwasser, S. 2015. "Machine learning classification over encrypted data." In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, pp. 1–34. San Diego, CA, USA.
6. TensorFlow: An open-source machine learning framework for everyone. n.d. Accessed March 2, 2024. https://www.tensorflow.org/ .

7. Gomez, A. N., Huang, S., Zhang, I., Li, B. M., Osama, M., & Kaiser, L. 2018. "Unsupervised cipher cracking using discrete GANs." In *International Conference on Learning Representations*.
8. Danziger, Moisés, and Marco Aurélio Amaral Henriques. 2014. "Improved Cryptanalysis Combining Differential and Artificial Neural Network Schemes." In *International Telecommunications Symposium*, Sao Paulo, Brazil.
9. Biehl, M., & Caticha, N. 2001. "Statistical Mechanics of On-Line Learning and Generalization." In *The Handbook of Brain Theory and Neural Networks*.
10. Hertz, J., Krogh, A., & Palmer, R. G. 1991. *Introduction to the Theory of Neural Computation*. Redwood City: Addison Wesley.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 50 – 56 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

QUANTUM-RESISTANT LATTICE-BASED CRYPTOGRAPHY: NEW CONJECTURES ON THE LEARNING WITH ERRORS PROBLEM

Luka Baklaga[1]
[1]Research and Development Department, Researcher, Business and Technology University, Georgia

ABSTRACT: As the field of quantum computing advances rapidly, lattice-based cryptography has emerged as a promising approach for post-quantum cryptography. Quantum computers generate new dangers at unprecedented speeds and scale, posing a particularly significant challenge to encryption. Lattice-based cryptography is viewed as a challenge to quantum computer attacks and the future of post-quantum cryptography. The Learning with Errors (LWE) problem serves as a fundamental hardness assumption underlying numerous lattice encryption and signature schemes. In this research paper, we investigate novel mathematical conjectures related to the LWE problem and its inherent hardness. Firstly, we analyze the structural properties of LWE and its connection to standard lattice problems. Building upon this analysis, we formulate two new conjectures that link the hardness of LWE to the worst-case hardness of standard lattice problems under different error distributions. Subsequently, we provide rigorous proofs for these conjectures, employing techniques derived from the geometry of lattices. Our conjectures generalize existing hardness results and offer valuable insights for practical parameter selection in LWE-based cryptosystems. Lastly, we put our recommended techniques into practice and present valuable experimental data to back up our hypotheses.

KEYWORDS*:* Post-quantum cryptography, Lattice-based cryptography, cryptography, quantum-resistant, Learning, GapSVP, quantum security

1. INTRODUCTION

Powerful quantum computers could soon crack today's security codes that safeguard sensitive data. These codes rely on hard math problems traditional computers struggle to solve. However, quantum algorithms can solve these problems easily, leaving standard encryption methods defenseless. This emerging threat drives researchers to develop quantum-resistant cryptography using new approaches like lattice-based methods (Nejatollahi et al. 2019). Researchers are interested in lattice-based cryptography methods for several reasons. First of all, lattice-based protocols employ straightforward and effective algorithms. Lattice-based algorithms can accomplish a variety of current cryptographic constructs, including digital signatures, key exchanges, encryption and all homomorphic encryptions. The security of these algorithms is contingent upon the intricacy of problem solving within the lattice. They also generate a wide range of applications and have been shown to be secure protocols. One key concept is the Learning with Errors (LWE) problem, which connects to deep mathematical challenges like finding the shortest vector in a multidimensional lattice. By building encryption on such intricate lattice problems, cryptographers aim to forge encryption methods that even future quantum computers cannot break (Nielsen and Chuang 2011). One of the key components of cybersecurity is cryptography. Cryptography is the study of information security and the art of rendering mechanisms so that only the sender and intended recipient can understand the information. Currently used public-key encryption depends on the fact that a huge prime number can be multiplied quickly by a classical computer, but it takes thousands of years to reverse this calculation (Schneier 2015). The decryption of data secured by public-key encryption methods will be accelerated by quantum computing (Brassard et al. 1998). Quantum-resistant communications and encryption have surfaced as a defense against possible adversarial security breaches utilizing quantum computing. Since most Internet users transfer their information over public infrastructures managed by other parties, there are already serious concerns

about cybercrime and privacy, even though it is unclear when such a threat may manifest (Sabani et al. 2022). One of the most promising post-quantum cryptography techniques is the use of lattice-based algorithms, as demonstrated by an examination of quantum computation power (Buchmann et al. 2016). Comprehending the difficulty of the Learning with Errors (LWE) problem is vital, especially under diverse error distributions, for designing and analyzing secure LWE-based cryptosystems. This research presents a thorough examination of the structural properties of the LWE problem and its relationship with standard lattice problems (Yin et al. 2023). We formulate two novel mathematical conjectures that link the hardness of LWE to worst-case instances of the Gap Shortest Vector Problem (GapSVP) and the Shortest Independent Vectors Problem (SIVP) under various error distributions, including non-spherically symmetric and spherical Gaussian errors. Through rigorous proofs, these conjectures are established, providing a solid theoretical foundation for understanding the complexity of LWE. Our study encompasses extensive experiments, implementing the suggested lattice algorithms and conducting tests on recognized lattice challenge datasets. The experimental outcomes demonstrate the practical effectiveness and applicability of our conjectures, aligning closely with the predicted difficulty estimations. This is how the proposed research paper is structured: The background information and prerequisites on lattices, the Learning with Errors (LWE) problem, and associated computational issues are given in Section 2. The LWE problem is explored in greater length in Section 3, along with its definition. Our new conjectures regarding the difficulties of LWE under various error distributions are presented in Section 4, along with robust mathematical proofs. The experimental setup is described in Section 5, In order to show the practical applicability and efficacy of our conjectures in approximating worst-case lattice issues, Section 5.1-5.2 provides and analyzes the experimental outcomes. The ramifications of our work for LWE-based encryption are covered in Section 7, along with limits and future research areas. We emphasize the impact on parameter selection and security evaluations.
Our contributions enhance the foundational knowledge of the LWE problem and provide valuable insights for parameter selection in LWE-based cryptosystems. This paves the way for more robust and efficient implementations of lattice-based cryptography. As the threat of quantum computing looms, our work represents a significant stride towards developing quantum-resistant cryptographic solutions capable of withstanding attacks from powerful quantum adversaries.

1.1 CONTRIBUTIONS

In this scholarly endeavor, we undertake mathematical (Nam and Blümel 2012), theoretical, and predictive contributions:

- We scrutinize the structural properties of the LWE problem and its connection to lattice problems like GapSVP (the gap Shortest Vector Problem) and SIVP (the Shortest Independent Vectors Problem).
- We formalize two novel conjectures (Conjectures 4.1 and 4.2) linking the hardness of LWE to worst case instances of GapSVP and SIVP under varied error distributions, encompassing non spherically symmetric and spherical Gaussian errors.
- We provide rigorous mathe-matical proofs for these conjectures, employing techniques from the geometry of lattices and building upon existing hardness results.
- We analyze the experimental results, comparing them with the predicted hardness estimations and discussing the implications for parameter selection in LWE based cryptosystems.
- We identify future research directions and propose potential improvements.

2. FOUNDATON

2.1. NOTATION

Throughout this study, vectors in $\mathbb{R}^n$ or $\mathbb{Z}^n$ are denoted by bold lowercase letters (e.g., v), while matrices are represented by bold uppercase letters (e.g., B). Let $||v||$ represent the Euclidean ℓ_2 norm

of a vector *v*. Over a countable domain D, the statistical distance between two distributions, X and Y, is defined as follows:

$$\Delta(X,Y) = \frac{1}{2}\sum_{x\in D} |\Pr[X = x] - \Pr[Y = x]|$$

With their traditional meanings, there has been employed the conventional asymptotic notation O(·), o(·), Õ(·), and ω(·).We say a function f(n) is negligible, denoted as negl(n), if $f(n)=o(n^{-c})$ for every constant $c>0$.

2.2. LATTICES-GAUSSIAN MEASURES

When n linearly independent vectors B = {b_1,..., b_n} in $\mathbb{R}^n$ are used as a basis, an n-dimensional lattice Λ is created, which is a discrete additive subgroup of $\mathbb{R}^n$:

$$\Lambda(B) = \left\{\sum_{i=1}^{n} z_i b_i \mid z_i \in \mathbb{Z} \text{ for } 1 \le i \le n\right\}$$

The half-open set is the fundamental parallelepiped P(B):

$$P(B) = \left\{\sum_{i=1}^{n} x_i b_i \mid 0 \le x_i < 1\right\}$$

We define $\lambda_1(\Lambda)$ for a lattice Λ as the length of its shortest non-zero vector. For the Shortest Vector Problem (SVP), the approximation factor is defined as follows:

$$\gamma_{SVP}(\Lambda) = min\{r \mid \lambda_1(\Lambda) \le r \cdot \text{dist}(0, \Lambda\{0\})\}$$

Where, $dist(0, \Lambda\{0\}) = min_{x\in\Lambda\{0\}}||x||$.
Given parameter s > 0, the Gaussian function $\rho_{(s,c)}$ on $\mathbb{R}^n$, centered at c, is defined as follows:

$$\rho_{(s,c)}(x) = \exp(-\pi \parallel x - c \parallel^2/s^2)$$

The definition of the total Gaussian measure ρ_s, centered at 0 is ρ_s = ρ_(s,0). Restricting ρ_(s,c) to Λ and renormalizing yields the discrete Gaussian distribution D_(Λ,s,c) over a lattice Λ. There has been obtained the spherical Gaussian D_(Λ,s) that is spherically symmetric in the particular case of c=0.

3. THE LWE PROBLEM

3.1 PROBLEM DEFINITION

In the simplest version, the Learning with Errors (LWE) problem is defined in the following manner:

Let χ represent the error distribution over $\mathbb{Z}_q$ and let n and q be positive integers such that q ≥ 2. The LWE distribution A_(s,χ) over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ for a secret $s \in \mathbb{Z}_q^n$ is obtained by uniformly selecting $a \in \mathbb{Z}_q^n$, selecting e ↞ χ, and producing $(a, b = \langle a, s\rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. Given rogue access to an arbitrary number of independent samples from A_(s, χ), the search version of the LWE problem is to locate s (or fail). In the decision version, one must choose between an equal number of samples from

the uniform distribution across $\mathbb{Z}\_q\hat{}n \times \mathbb{Z}\_q$ and an arbitrary number of samples from the LWE distribution A_(s, χ) with a non-negligible advantage.

4. NEW CONJECTURES ON LWE

Novel Hypotheses on LWE In this part, we formulate and demonstrate two novel conjectures that relate the complexity of common worst-case lattice problems such as GapSVP and SIVP to the hardness of LWE.

- Conjecture 4.1: The LWE issue with parameter χ is at least as hard as approximating the GapSVP and SIVP problems on n-dimensional lattices within a factor α/δ for any m = poly(n), δ ∈ (0, 1/2), and error distribution χ over $\mathbb{Z}\_q$ with finite non-zero absolute constant factor α > 0.

Conjecture 4.1 Proof:

There has been demonstrated a reduction of the GapSVP problem to LWE with error distribution φ in order to prove this conjecture. Let us suppose we have an oracle with advantage ε that solves LWE instances. Let (B, d) be an instance of GapSVP, where d is the distance threshold and B is a basis for a lattice Λ. Here's how we build a LWE instance:

1. There has been assigned $q = 2^{\lceil \log(2nd_{max}) \rceil}$ where $d_{max} = \max_{v \in \Lambda\{0\}} \| v \|$
2. There has been set $m = n\lceil \log q \rceil + \omega(\log n)$
3. Sampled A ← Z_q^(m×n) uniformly at random
4. Compute/ Determined t = Bv + e mod q where v ← D_(Λ, α/δ) and e ← χ^m
5. Fed samples (A, t) to the LWE oracle

We obtain a δ-approximate SVP solution z = Bs' mod B if the oracle yields a solution s'. This comes after:

$$\| z \| \leq \| Bs' - t \| + \delta d_{max} \leq \frac{\alpha}{\delta} \cdot d_{max} + \delta d_{max} \leq d$$

Assuming the LWE oracle succeeds with non-negligible advantage ε, the aforementioned recovers a δ-approximate SVP solution with high probability over the LWE samples.

- Conjecture 4.2: In the case where m = poly(n) and δ > 0, there is a quantum polynomial-time reduction from GapSVP(n, β) to LWE with any spherical continuous Gaussian error distribution of parameter αq ≥ β−(log n) on n-dimensional lattices.

Conjecture 4.2 Proof:

The main concept is to embed the lattice into a higher dimension and use the Gaussian sample from LWE as a guide to identify short lattice vectors, hence reducing GapSVP(β) to LWE. Given a LWE instance with spherical Gaussian errors of parameter αq ≥ β√(log n), let (B, d) be a GapSVP instance in dimension n with d = β·λ_1(Λ). Using a simplified version of a quantum computer cloud simulation, we execute the subsequent actions:

1. There has been embed Λ into Λ' by setting $B' = (B \mid \gamma I_n)$ where $\gamma = \alpha q \cdot \omega(\sqrt{\log n})$.
2. Called the LWE oracle on $m \geq (n+1)\lceil \log q \rceil$ samples to recover s' with non-negligible probability.

3. Used s' to compute a relatively short vector $b' = (s', -1) \in \Lambda'$ with norm $||b'|| \leq \alpha q \cdot \omega(\sqrt{(\log n)})$.
4. Applied lattice vector spingover to b' to get a new vector b" ∈ Λ.
5. Projected b" down to the original n dimensions, obtaining a GapSVP solution for Λ.

By solving GapSVP(β), we can demonstrate that the final vector has length ≤ β·λ_1(Λ) with high probability.

5. EXPERIMENTAL RESULTS

We implemented the lattice basis reduction and decoding algorithms from our proofs and performed experiments on benchmark lattice challenge datasets to validate our novel conjectures.

5.1. VERIFYING CONJECTURE 4.1

We created LWE samples for m = 10n log n, q = 2^32 with error distributions χ as previously mentioned for various parameter values *(σ, b, β_1, β_2)* in order to test Conjecture 4.1. After that, we used our SVP approximation approach to get the conjecture proof's reduction. The outcomes presented in Table 1 indicate the root Hermite factors attained and demonstrate that our reduction is effective across a variety of error distributions χ, with a high likelihood of meeting the expected GapSVP approximation factor of α/δ given suitable parameters.

Table.1. *Experimental results for Conjecture 4.1 on n=60 lattices. The predicted GapSVP factor is α/δ ≈ 1.0127.*

Error Distribution χ	*Parameters*	*Achieved Root Hermite Factor*
Discrete Gaussian	σ = 4	1.00856
Uniform	b = 7	1.01023
Generalized Normal	β_1 = 2, β_2=8	1.00913

5.2. VERIFYING CONJECTURE 4.2

There has been created LWE instances for Conjecture 4.2 using m = n^2 samples and a spherical continuous Gaussian error $\chi = D_{Z^m, \alpha q}$ for a range of n and q values. We applied our quantum algorithm for reducing to GapSVP(β) for every LWE instance, where β = 3n√(log n) according to the reduction.
Our algorithm's temporal complexity and success probability closely matched the expectations, increasing the likelihood of recovering the secret *s*. Table 2 provides the outcomes for a few example cases.

Table.2. *Performance of quantum GapSVP(β) reduction for Conjecture 4.2*.

n	*q*	*Time (seconds)*	*Success Rate*
40	2^30	247	96.8%
50	2^34	983	94.2%
60	2^36	2915	92.5%

The aforementioned findings offer compelling empirical proof in favor of our novel hypotheses regarding the difficulty of LWE with various error distributions.

6. DISCUSSION

6.1 IMPLICATIONS FOR LWE-BASED CRYPTOGRAPHY

Our novel hypotheses and empirical findings have profound implications for the design and evaluation of cryptographic schemes based on the Learning with Errors (LWE) problem. Conjecture 4.1 establishes a general reduction from LWE to worst-case instances of the Gapped Shortest Vector Problem (GapSVP) and the Shortest Independent Vectors Problem (SIVP), even for error distributions that are not spherically symmetric. This result provides a deeper understanding of the hardness assumptions underpinning LWE-based cryptosystems. It can guide the selection of parameters to achieve desired security levels against lattice-based attacks.
Conjecture 4.2 offers a tighter reduction from GapSVP to LWE with spherical Gaussian errors, which are widely employed in practical implementations due to their computational efficiency and provable security properties. The experimental validation of this conjecture further strengthens the security claims of LWE-based schemes that utilize Gaussian errors.

6.1 LIMITATIONS AND FUTURE WORK

Although our findings show promising theoretical and practical outcomes, there are several limitations and opportunities for further exploration: Our conjectures provide asymptotic hardness outcomes, but pinpointing the precise multiplicative factors obscured by the asymptotic notation remains an open challenge. Refining these security estimates could lead to more precise parameter selections for LWE implementations. Our analysis focuses on general lattices, but many practical LWE-based schemes e-xploit structured lattices (e.g., ideal lattices) for efficiency gains. Extending our conjectures and techniques to these structured settings could yield valuable insights into the concrete security of widely deployed cryptosystems. It is essential to constantly assess any new threats and attacks in order to preserve security, which calls for being watchful and swiftly updating encryption systems. It will take much mathematical and computer science study to create post-quantum encryption techniques that are both robust and effective. To guarantee that new technologies are widely adopted, extensive deployment and standardization will require intricate coordination and collaboration. Although our experiments confirm the theoretical predictions, a more thorough examination of the specific difficulty of LWE instances under various parameter selections would be advantageous for practical applications. These analyses could integrate the latest algorithmic advancements and hardware optimizations. Further optimizations and parallelization techniques could enhance the performance of our lattice algorithms, enabling larger-scale experiments and facilitating the evaluation of higher-dimensional lattice instances. This could result in more accurate security estimates and better parameter selections. As quantum computing capabilities progress, it will be crucial to assess the post-quantum security of LWE-based schemes against potential quantum attacks beyond those considered in our work. It is essential to constantly assess any new threats and attacks in order to preserve security, which calls for being watchful and swiftly updating encryption systems. Continuous reevaluation and adaptation will be nece-ssary to maintain the security guarantees of these cryptographic primitives.

ETHICAL STATEMENT

This study does not contain any studies with human or animal subjects performed by any of the authors.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to this work.

REFERENCES

1. Sabani, M., Savvas, I. K., Poulakis, D., and Makris, G. 2022. "Quantum Key Distribution: Basic Protocols and Threats." In *Proceedings of the 26th Pan-Hellenic Conference on Informatics (PCI 2022)*, Athens, Greece, 25–27 November 2022. New York, NY, USA: ACM.
2. Nielsen, M., and Chuang, I. 2011. *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press.
3. Buchmann, J. A., Butin, D., Göpfert, F., and Petzoldt, A. 2016. "Post-Quantum Cryptography: State of the Art." In *The New Codebreakers*, edited by P. Ryan, D. Naccache, and J. J. Quisquater, Volume 9100, Lecture Notes in Computer Science. Springer, Berlin/Heidelberg, Germany.
4. Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., and Cammarota, R. 2019. "Post-quantum lattice-based cryptography implementations: A survey." *ACM Computing Surveys* 51: 1–41. doi: 10.1145/3292548.
5. Yin, H. L., Fu, Y., Li, C. L., Weng, C. X., Li, B. H., Gu, J., Lu, Y. S., Huang, S., and Chen, Z. B. 2023. "Experimental quantum secure network with digital signatures and encryption." *Natl. Sci. Rev.* 10: nwac228. doi: 10.1093/nsr/nwac228.
6. Brassard, G., Chuang, I., Lloyd, S., and Monroe, C. 1998. "Quantum computing." *Proc. Natl. Acad. Sci.* 95: 11032–11033. doi: 10.1073/pnas.95.19.11032.
7. Nam, Y., and Blümel, R. 2012. "Performance scaling of Shor's algorithm with a banded quantum Fourier transform." *Phys. Rev. A* 86: 044303.
8. Schneier, B. 2015. "Key-Exchange Algorithms." In *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. Hoboken, NJ, USA: Wiley.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 57 – 63 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

NEUROETHICAL QUANDARIES AT THE CROSSROADS OF CYBERSPACE

Er. Ms. Kritika[1]

[1] Independent Researcher, India

ABSTRACT: The booming landscape of multidisciplinary studies, namely, neuroscience, ethics and cyber security brings into focus the emerging need of developing ethical standards for neural data to the implemented safely in the domain of cyberspace. The synergy between neuroscience and cybersecurity emphasizes the transformative potential of technologies like BCI, EEG, FMRI, MEG etc. highlighting the ethical imperative to bring to light the issues of privacy, autonomy, individual's right, and security of their neural data. The paper delves into the question of delicacy of neuro data as an emerging concern for cyber professionals as well as individuals to safeguard from the emerging threats of phishing, brain jacking, vishing and implementing proper guidelines and framework to have informed consent before going ahead with their confidential data which can otherwise be misused at the hands of cybercriminals.

KEYWORDS: Neuroethics, Cybersecurity, Neuroimaging Technologies, BCI

1. INTRODUCTION

A novel approach that acknowledges the weaknesses in the modern human mind and seeks to strengthen defence against cyberattacks is the integration of neuroscience with cybersecurity. Due to social engineering, phishing, and other strategies that take advantage of people's cognitive abilities and make them unintentionally complicit in security breaches, this convergence acknowledges the human aspect as a major role in cyber dangers. Cybersecurity systems [3] can be built to identify abnormalities in user behaviour by comprehending the cognitive processes connected to deceit, stress, or malevolent intent with an extra line of defence against insider threats and complex attacks can be added by integrating neurobiological markers, such as physiological reactions, eye movement patterns, or cognitive strain, into advanced threat detection algorithms. Biometric markers might be, for example, an individual's physiological reactions, tracked by wearable technology or specialized sensors. Traditional behavioural analytics is strengthened and made more resilient to new threats by this neuroscience-informed method. Another area where neuroscience might improve security through individual cognitive variables is in cognitive authentication and access control. Based on brainwave patterns or the cognitive reaction to particular stimuli, neuro-authentication may offer a more safe and dependable way to confirm user identification. Developments in Brain-Computer Interfaces (BCIs) [36, 37] provide a possible path towards cognitive authentication implementation. Organizations may strengthen security by providing an extra layer of authentication beyond conventional techniques by integrating these cognitive biometrics into access control systems.

As neuroscience and cybersecurity grow increasingly integrated, safeguarding cognitive privacy becomes a critical ethical concern. The gathering and examination of brain data gives rise to worries regarding possible abuse or unapproved access to people's feelings and thoughts. Establishing ethical frameworks is necessary to guarantee that neuro-cybersecurity measures respective individual autonomy and privacy rights. Programmes for human-centered awareness and training can also profit from neuroscience by learning about people's perceptions and processing of security-related information might help designers create training modules that are more successful that are based on cognitive science concepts, neuroeducation can improve users' ability to remember and apply cybersecurity best practices.

Organizations may enable users to identify possible hazards and take appropriate action more efficiently by customizing training programmes to correspond with cognitive processes. Another way that neuroscience may help design adaptable cybersecurity systems that learn and adjust based on real-time assessments of user behaviour and environmental conditions is through neuro-inspired adaptability. Algorithms with artificial intelligence have the potential to imitate the human mind's capacity for adaptation and learning, allowing them to continually update their comprehension of typical user behaviour and spot abnormalities.

The rapid progress in brain research and technological advancements has led to an increased interest in the multidisciplinary topic of neuro-ethics, a blend of neuroscience and ethics. Ethical issues gain importance as our knowledge of the brain increases and applications in neuroscience grow with the goal to discuss the moral ramifications of comprehending, modifying, and controlling the brain with the subjects including personhood, consciousness, brain-computer interfacing, and cognitive augmentation. As concerns regarding cognitive privacy, the right to govern ideas, and potential unintended implications on human identity grow, respect for autonomy is a basic ethical tenet. The transdisciplinary field of neuro-ethics studies the philosophical, legal, and social ramifications of neuroscience investigating the cultural presumptions on identity, consciousness, cognitive experience, and decision-making [1]. It involves different elements of research ethics, including informed consent, privacy and confidentiality, clinical applications, medical interventions, legal and societal ramifications, education, dual-use technology, and philosophical and conceptual difficulties which includes [2] obtaining participants' informed consent, handling sensitive brain data collection and storage issues, and discussing the moral implications of medical interventions such as deep brain stimulation and brain imaging, as well as neuro enhancement and brain-computer interfaces. Determining criminal guilt and estimating the probability of future criminal behaviour are just a few of the legal and societal ramifications.

Cybersecurity [4] has its roots in the early days of computing, where the chief concern was to secure individual systems with the shift in focus as technology advanced and networks emerged towards safeguarding interconnected systems. The exponential growth of the internet in the late 20th century amplified both the opportunities and threats associated with cyberspace with 21st century witnessing an unprecedented surge in cyber threats, ranging from simple viruses to sophisticated cyber espionage campaigns. The rapid digitization of critical infrastructure, financial systems, and personal information intensified the need for robust cybersecurity measures. Key components of cybersecurity include network security, endpoint security, identity and access management (IAM), data security, application security, incident response and recovery, and security awareness and training [5].

The nexus between neuro-ethics and cybersecurity offers an intriguing and challenging terrain in the ever-changing field of cybersecurity, where innovations in technology constantly alter the danger picture. The field of neuro-ethics explores the moral issues raised by neuroscience and the use of information about the brain. The significant areas of interest include:

Biometric authentication [6] is the one where neurology and cybersecurity blends including facial recognition, voice authentication, and fingerprint scanning, relying on distinct physiological and behavioural traits. With the advancement of neuroscience, there is a growing interest in using neurobiological data for increased security, such as brainwave patterns or even brain-based authentication. The prime advantages include enhanced security offering a more reliable and customized type of authentication with lower possibility of unwanted access and convenient user experience which does not require the need to remember passwords or PINs.

Comprehending the neurological systems that underlie human decision-making and behaviour can facilitate the development of advanced social engineering attacks [7]. Cybercriminals may take use of cognitive biases and brain weaknesses to trick people into disclosing private information or acting against their better judgement. Neuro-influenced social engineering can provide very precise and convincing attacks, which might make it difficult for victims to recognise malevolent intent along with leaving a significant psychological effect on them.

Insider threat detection is being investigated with the use of neurotechnology [8], including methods like electroencephalography (EEG) and functional magnetic resonance imaging (fMRI). Organisations monitor brain activity in an effort to spot irregularities that could point to insider threats or criminal inte Neurotechnology may be able to identify stress or malevolent intent in workers before more conventional markers show up signs of malbehaviour. Insider threats are a serious danger to an organization's cybersecurity, but they may be lessened with early identification.
Technologies for cognitive improvement, including brain stimulation or nootropics, are being investigated to improve cybersecurity experts' cognitive capacities. Enhancing concentration, decision-making, and problem-solving abilities is the goal in a field where prompt and precise replies are critical performing better in more efficient threat identification and response with enhanced cognitive resilience [9-10].

1. NEUROSCIENTIFIC TECHNIQUES IN CYBER SECURITY:

2.1 Brain-Computer Interfaces (BCIs): Bridging the mind and machine

Brain-computer interfaces (BCIs) [11] are a rapidly evolving technology that can alter dramatically human interaction with computers to measure brain activity and translate it into commands for a computer or other device, allowing users to control machines and devices using only their thoughts divided into unidirectional and bidirectional categories based on action direction. This intersection of neurobiology and computing has the capability to alter dramatically various aspects of human life, from healthcare and rehabilitation to communication and entertainment, operating through various modalities which includes electroencephalography (EEG), functional magnetic resonance imaging (fMRI), electrocorticography (ECoG), and invasive neural implants that metamorphose external commands into electrical signals transmitted through the nervous system. In functional near-infrared spectroscopy (fNIRS), magnetoencephalography, and electrocorticography, the electroencephalogram (EEG), giving a visual image of the brain activity and track sleeping patterns, diagnose and treat neurological conditions, and investigate cognitive functions offering excellent levels of precision is a commonly used instrument for tracking electrical activity in the brain which quantify various neuronal subtypes in the human brain. Depending on the neural signals recording, it can be bifurcated into invasive and non-invasive BCI [12].
Invasive BCI offers three prime advantages [13]: (1) it can take down activities from every single neuron or modulate the activities of a small population of neurons with much greater spatial and temporal resolution [14]; (2) it has a higher signal-to-noise ratio (SNR) and more resilient to electrical noise interferences or movement artefacts; and (3) its electrodes can be placed in close proximity to or directly in the target cortical areas or subcortical structures. Along with the advantages, it also offers numerous disadvantages [13]. Firstly, the direct insertion of electrodes into brain tissues necessitates an intrusive surgical procedure that raises the possibility of problems. Second, the system requires considerably greater dependability and reduces some degree of flexibility because it is impossible to replace any component or correct hardware issues after it is implanted. Finally, the cost of invasive BCI has to be addressed in order to make it more accessible because of the intricacy of the surgical technique and the post-operation care required.
Non-invasive Brain–Computer Interfaces (BCIs) [13] use techniques including (MEG), (EEG), (fMRI), and (fNIRS) to gather data on brain activity without the need for brain surgery. It takes into consideration the activities through surgically inserted electrodes in close proximity to the targeted neurons in the cortex or deep brain structures. There are benefits such as safety, accessibility, and less invasiveness. On the other hand, its temporal and geographical resolution as well as signal quality could be limited. Noise, artefacts in movement, and the incapacity to distinguish between various parts of the brain can all affect data from non-invasive brain imaging (BCI) as they rely so heavily on measurements from the scalp surface, making it difficult to reliably record deep brain activity. Because everyone's

scalp and skull are different, BCI's utility and reliability might vary as well. Furthermore, significant preprocessing and signal analysis—which can be laborious and computationally demanding—are needed to extract useful information from BCI data.
Brain-computer interfaces (BCIs) rely on electroencephalograms (EEGs) [15] to obtain brain wave data and facilitate brain-to-external device connection, used for a variety of purposes, such as motor imagery (MI), in which people visualise carrying out a certain movement. The ability to comprehend imagined movements and operate external devices has showed promise for EEG-based MI-based BCIs. Wearable EEG devices have further broadened BCI applications, offering more easy and accessible ways to track brain activity.

2.2 Neuroimaging techniques:

The non-invasive surveillance of the structure and activity of the brain is made possible by neuroimaging, an essential technique that clarifies the capabilities that various brain areas play in behavioural and cognitive tasks including language, choice-making, emotion control, insight, attention, and memory [16,17]. When examining brain function, particularly in severe mental diseases like bipolar disorder, neuroimaging is very significant as it evaluates therapy outcomes. Through neuroimaging, scientists may map neural networks, see how the brain functions, and investigate the processes underlying a range of neurological conditions [18]. On deeper understanding the anatomy and function of the brain, it has become much more accurate and detailed with the recent developments in neuroimaging methods helping researchers get an exact picture of the brain's structure, including the sub-millimeter structures of the cortex using high-resolution structural magnetic resonance imaging, facilitating the mapping and identification of unidentified brain areas [19,20].
With an emphasis on human thought, emotion, and behaviour, cognitive biometrics is a novel approach to biometric technology that combines physiological and behavioural traits wherein biosignals pertaining to cognitive and emotional processing are the foundation of it originating from the brain, heart, and autonomic nerve systems [21]. Users may be protected, privacy compliance is ensured, and there is resilience against manipulation using cognitive biometrics [22]. Their non-volitional nature and internal nature shield them from public scrutiny, which reduces their susceptibility to spoofing assaults. Unless the user actively engages in the process, it is unlikely that these biosignals will be detected remotely or in secret using the sensor technologies available today [22, 23].
Users are shielded from presentation assaults by cognitive biometrics, which also provide liveness detection and continuous apps. Because they are not static, biosignals may also be cancelable. Brain biometrics [24] based on event-related potentials enable for the substitution of compromised biometric identifiers with new ones, a capability not accessible in standard biometric modalities like tracks, palmprints, and iris. The benefits of cognitive biometrics have prompted several papers on the subject, highlighting the need for more study and guidance in this area.

3. NEURO-ETHICAL CONSIDERATIONS IN CYBERSPACE:

Neuro-ethics in cybersecurity has emerged as a result of the deep ethical problems raised by the junction of neuroscience and cybersecurity with technologies penetrating the workings of the human mind giving rise to the ethical considerations for use of neuro data. It has emerged as a response to the believe that the frontiers of the skull mark the boundary between the observable and unobservable dimensions of a living person. However, recent advances in neuroscience and neurotechnology has made it possible to unlock the potentials of human brain and throw light on how various brain functions relate to observed behaviour and mental states [25]. Privacy concerns are significant in neurosecurity or cybersecurity, as neurodata captures intimate details of an individual's thoughts and mental states necessitating the defining of boundaries for curation, storage and utilisation of neural data [25, 26]. Standards and regulatory frameworks for neurosecurity or integration of neuroscience in cyber security are crucial,

and neuroethics plays a role in developing the rules guiding the moral use of brain-computer interfaces (BCIs), neural tracking, and cognitive security techniques [27].

The inner workings of human psychology could be altered by neurotechnology, opening the door for external impact on basic human values like agency, mental privacy, and biographical identity. It is crucial to understand that these dangers are neither special nor unique, though, since a large body of research highlighting this fragility makes use of commonplace social manipulation techniques like verbal communication [28]. Modifying the brain and, thus, human agency, identity, and privacy with accuracy and efficacy is what neurotechnology offers. Still, given how difficult it is to control discussions that might purposefully or unintentionally change someone's memory compared to consciously changing memories using BCI, neurotechnologies might be more open to public scrutiny than social manipulation [29, 30]. The slightest alteration in the neural information of brain data can pose significant risks of increased mal-intentions of cyber criminals leading to sophisticated attacks like phishing, vishing, identity theft, ransomware, brainjacking [32] and much more.

Cognitive liberty [34], a concept rooted in autonomy and freedom of thought, is increasingly in talks with relation to emerging technologies that interact with the human mind encompassing the right to autonomy and control over one's cognitive processes, as well as the ethical challenges posed by manipulation and coercion. Autonomy and control pose as the fundamental aspects, emphasizing the right to govern mental processes, thoughts, and decisions without external interference while ethical considerations include informed consent, privacy-preserving technologies, and user-centric design [33]. Manipulation and coercion [34] pose significant ethical challenges about the unintended consequences of influencing or coercing cognitive processes, challenging the essence of individual freedom resulting in the reveal of personal identity as well as information like banking details with ease in the hands of cyber criminals delineating the areas of infringement of individual's rights in autonomous decision making.

While there might be major scientific and therapeutic benefits, the capacity to record and modify brain activity via implantable and non-implantable neural devices also presents difficult ethical questions endangering individual neuro-privacy deciphering unfettered and trading neuro data [31]. Developing legal safeguards specifically addressing the ethical use of neuro-technologies can provide additional protection against manipulation and coercion. Examples include cognitive enhancements in employment, where employees may feel compelled to enhance their cognitive abilities to meet job expectations, and neurotechnological marketing influence, where advertisers may manipulate consumer preferences or decision-making processes [25,33,35]. The development of neuro data guidelines [26] is the primary concern to safeguard individuals from the clutches of cybercriminals who are prone to trick individuals into revealing confidential data and misusing it with more vigor and ease and performing activities like brain hacking. The above mentioned ethical issues pose a considerable need for the development of framework with experts in the field of neuroscience, ethics, neurotechnology and cybersecurity.

4. CONCLUSION

Neurotechnology applications are growing rapidly both on the inside as well as on the outside of the clinical and research setting in terms of volume and variety making the availability of more affordable, scalable, and user-friendly neuro applications. In terms of clinical benefit, prevention, self-quantification, bias reduction, personalized technology use, marketing analysis, military dominance, national security, and even judicial accuracy, this technological trend may be extremely advantageous for society as a whole. However, its implications for ethics and the law are yet to be taken care of. A proposal that the normative landscape needs to be established swiftly to prevent misuse or unanticipated negative repercussions, given the disruptive revolution that neurotechnology is bringing about in the digital environment. The emergence of neuroscience in the domain of cybersecurity poses the question of ethical considerations of the use of neuro data which has been highlighted in this paper. A need for

proper guidelines and framework at global scale to prevent misuse of data and impart proper ethical standards is the need of the hour safeguarding individual's right to privacy.

REFERENCES

[1] J. Das et al., "Neuroscience is ready for neuroethics engagement," Front. Commun., vol. 7, p. 909964, 2022.

[2] M. Ienca et al., "Towards a governance framework for brain data," Neuroethics, vol. 15, no. 2, p. 20, 2022.

[3] Kritika, "Cyber Security and its cognitive ramifications on e-governance," IJIRMF, vol. 9, no. 5, 2023.

[4] Kritika, "Demystifying Cyber Crimes," in Perspectives on Ethical Hacking and Penetration Testing, K. Kaushik and A. Bhardwaj, Eds. IGI Global, 2023, pp. 63–94. [Online]. Available: https://doi.org/10.4018/978-1-6684-8218-6.ch003

[5] J. Jain and P. R. Pal, "A recent study over cyber security and its elements," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 3, pp. 791–793, 2017.

[6] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal Approach for Enhancing Biometric Authentication," J. Imaging, vol. 9, no. 9, p. 168, 2023.

[7] F. Babiloni and P. Cherubino, "Consumer Neuroscience: A Neural Engineering Approach," in Handbook of Neuroengineering, Singapore: Springer Nature Singapore, 2023, pp. 2861–2889.

[8] J. A. Olson et al., "Emulating future neurotechnology using magic," Conscious. Cogn., vol. 107, p. 103450, 2023.

[9] Y. Eski, A Criminology of the Human Species: Setting an Unsettling Tone. Springer Nature, 2023.

[10] N. Liv and D. Greenbaum, "Cyberneurosecurity," in Policy, Identity, and Neurotechnology: The Neuroethics of Brain-Computer Interfaces, Cham: Springer International Publishing, 2023, pp. 233–251.

[11] J. Peksa and D. Mamchur, "State-of-the-Art on Brain-Computer Interface Technology," Sensors, vol. 23, no. 13, p. 6001, 2023.

[12] M. A. Lebedev and M. A. Nicolelis, "Brain-Machine Interfaces: From Basic Science to Neuroprostheses and Neurorehabilitation," Physiol. Rev., vol. 97, pp. 767–837, 2017.

[13] Z. Zhao et al., "Modulating Brain Activity with Invasive Brain–Computer Interface: A Narrative Review," Brain Sci., vol. 13, no. 1, p. 134, 2023, doi: 10.3390/brainsci13010134.

[14] S. Saha et al., "Progress in Brain Computer Interface: Challenges and Opportunities," Front. Syst. Neurosci., vol. 15, p. 578875, 2021.

[15] A. Saibene et al., "EEG-Based BCIs on Motor Imagery Paradigm Using Wearable Technologies: A Systematic Review," Sensors, vol. 23, no. 5, p. 2798, 2023, doi: 10.3390/s23052798.

[16] M. C. Litwińczuk, N. Trujillo-Barreto, N. Muhlert, L. Cloutman, and A. Woollams, "Relating cognition to both brain structure and function: A systematic review of methods," Brain Connect., vol. 13, no. 3, pp. 120–132, 2023.

[17] T. Morita, M. Asada, and E. Naito, "Contribution of neuroimaging studies to understanding development of human cognitive brain functions," Front. Hum. Neurosci., vol. 10, p. 464, 2016.

[18] C. Yen, C. L. Lin, and M. C. Chiang, "Exploring the frontiers of neuroimaging: a review of recent advances in understanding brain functioning and disorders," Life, vol. 13, no. 7, p. 1472, 2023.

[19] C. Zeng et al., "Advanced high resolution three-dimensional imaging to visualize the cerebral neurovascular network in stroke," Int. J. Biol. Sci., vol. 18, no. 2, pp. 552–562, 2022.

[20] E. B. Vanstrum et al., "Development of an ultrafast brain MR neuronavigation protocol for ventricular shunt placement," J. Neurosurg., vol. 138, no. 2, pp. 367–373, 2022.

[21] M. Wang, X. Yin, Y. Zhu, and J. Hu, "Representation learning and pattern recognition in cognitive biometrics: a survey," Sensors, vol. 22, no. 14, p. 5111, 2022.

[22] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 7, pp. 1618–1629, 2016.

[23] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: an evaluation methodology and lessons learned," IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, 2015.

[24] Q. Gui, M. V. Ruiz-Blondet, S. Laszlo, and Z. Jin, "A survey on brain biometrics," ACM Comput. Surv., vol. 51, no. 6, pp. 1–38, 2019.

[25] M. Ienca and R. Andorno, "Towards new human rights in the age of neuroscience and neurotechnology," Life Sci. Soc. Policy, vol. 13, no. 1, p. 1, 2017.

[26] H. T. Greely et al., "Neuroethics guiding principles for the NIH BRAIN initiative," J. Neurosci., vol. 38, no. 50, p. 10586, 2018.

[27] S. Burwell, M. Sample, and E. Racine, "Ethical aspects of brain computer interfaces: a scoping review," BMC Med. Ethics, vol. 18, no. 1, pp. 1–11, 2017.

[28] S. Rainey et al., "Data and Consent Issues with Neural Recording Devices," in Clinical Neurotechnology meets Artificial Intelligence: Philosophical, Ethical, Legal and Social Implications, 2021, pp. 141–154.

[29] S. Goering et al., "Recommendations for responsible development and application of neurotechnologies," Neuroethics, vol. 14, no. 3, pp. 365–386, 2021.

[30] E. Hildt, "What will this do to me and my brain? Ethical issues in brain-to-brain interfacing," Front. Syst. Neurosci., vol. 9, p. 17, 2015.

[31] R. Yuste, "Advocating for neurodata privacy and neurotechnology regulation," Nat. Protoc., vol. 18, no. 10, pp. 2869–2875, 2023.

[32] L. Pycroft et al., "Brainjacking: implant security issues in invasive neuromodulation," World Neurosurg., vol. 92, pp. 454–462, 2016.

[33] P. Sommaggio and M. Mazzocca, "Cognitive Liberty and Human Rights," in Neuroscience and Law: Complicated Crossings and New Perspectives, 2020, pp. 95–111.

[34] B. C. M. M. is Mine, "Cognitive Liberty as a Legal Concept," in Cognitive Enhancement. An Interdisciplinary Perspective, E. Hildt and A. G. Franke, Eds. Dordrecht: Springer, 2013, pp. 233–264.

[35] T. Istace, "Neurorights: The Debate About New Legal Safeguards to Protect the Mind," Issues L. Med., vol. 37, p. 95, 2022.

[36] R. Rupp et al., "Brain–computer interfaces and assistive technology," in Brain-Computer-Interfaces in their ethical, social and cultural contexts, 2014, pp. 7–38.

[37] N. Rose, "The human brain project: social and ethical challenges," Neuron, vol. 82, no. 6, pp. 1212–1215, 2014.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 64 – 68 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

კიბერ ინციდენტების პროგნოზირება მანქანური სწავლების ალგორითმების გამოყენებით

PREDICTING CYBER INCIDENTS USING MACHINE LEARNING ALGORITHMS

Tinatin Mshvidobadze[1]
[1]Gori State University, Gori, Georgia

აბსტრაქტი. ნაშრომში წარმოდგენილია კიბერ ინციდენტებთან დაკავშირებული მეთოდები, სხვადასხვა მკვლევარების მიერ. მანქანური სწავლების ალგორითმები (DM-ML) მნიშვნელოვან როლს თამაშობს კიბერუსაფრთხოების[1] სფეროში კიბერ ინციდენტების (SCI) პროგნოზირებასა და გამოვლენაში. ნაშრომში მოცემულია კარგად ცნობილია ML კლასიფიკატორები, მონაცემთა კლასიფიკაციისათვის. მონაცემები აღებულია სტრატეგიული და საერთაშორისო კვლევების ცენტრის (CSIS) ანგარიშის მიხედვით. განხილულია ცენტრალიზებული კლასიფიკატორის მიდგომა მსოფლიოს ექვსი კონტინენტის მონაცემების მიხედვით. ნაშრომში კლასიფიკატორების შედარების საფუძველზე მაღალი სიზუსტით პროგნოზირებულია, თუ რომელი ტიპის კიბერ ინციდენტი შეიძლება მოხდეს და მსოფლიოს რომელ ნაწილში.

საკვანძო სიტყვები: კიბერ ინციდენტი, კიბერუსაფრთხოება, მონაცემთა მოპოვება, მანქანური სწავლება.

ABSTRACT. The paper presents methods related to cyber incidents by various researchers. Machine learning algorithms (DM-ML) play an important role in the prediction and detection of cyber incidents (SCI) in the field of cyber security. The paper presents well-known ML classifiers for data classification. The data set is taken from a report by the Center for Strategic and International Studies (CSIS). A centralized classifier approach based on data from six continents of the world is discussed. Based on the comparison of classifiers in the paper, it is predicted with high accuracy which type of SCI may occur and in which part of the world.

KEYWORDS: cyber incidents, cyber security, data mining, machine learning.

1.შესავალი

IoT და 5G ტექნოლოგიების სწრაფი ზრდა კიბერსივრცეს არაუსაფრთხოს ხდის, რაც საბოლოოდ იწვევს მნიშვნელოვანი კიბერ ინციდენტების განვითარებას [1]. მოსალოდნელია, რომ IoT მოწყობილობების რაოდენობა 2025 წლისთვის დაახლოებით 75 მილიარდს მიაღწევს

[1] კიბერუსაფრთხოება არის ტექნიკა, რომელიც იცავს სისტემას ინტერნეტში კიბერ ინციდენტებისაგან.

[2]. "კიბერუსაფრთხოების ალმანახის" მიხედვით, რომელიც გამოქვეყნდა "Cybersecurity Ventures"-ის მიერ, გლობალური კიბერდანაშაულის ღირებულება 2025 წელს 10,5 ტრილიონ აშშ დოლარს მიაღწევს.

კიბერ ინციდენტი ნიშნავს აქტივობას ან მოვლენას, რომელიც ხდება ინტერნეტის საშუალებით და საფრთხეს უქმნის საკომუნიკაციო სისტემის კონფიდენციალურობას, მთლიანობასა და ხელმისაწვდომობას ნებისმიერი საშუალებით. ტერმინი მნიშვნელოვანი კიბერ ინციდენტი (SCI) ნიშნავს ინციდენტს, რომელიც იწვევს ეროვნული უსაფრთხოებისა და ეკონომიკის აშკარა ზიანს [3].

SCI-ის ზრდასთან ერთად, კიბერუსაფრთხოების ზომები ასევე გაუმჯობესდა ამ ინციდენტების მოსაგვარებლად. მონაცემთა მოპოვება და მანქანური სწავლება (DM-ML) მნიშვნელოვან როლს თამაშობს კიბერ ინციდენტების პროგნოზირებაში, პრევენციასა და გამოვლენაში სხვადასხვა მიდგომების გამოყენებით [4].

ნაშრომში განვიხილავთ სხვადასხვა მკვლევარების მიერ მიღებულ ეფექტურ შედეგებს ამ ინციდენტების აღმოსაფხვრელად.

მოცემულია უსმან აშრაფის და სხვა მკვლევარების მიერ პროექტის ფარგლებში ჩატარებული კვლევის შედეგები [5]. ასევე ნაჩვენებია ცენტრალიზებული კლასიფიკატორის სარგებელი მომავალში *SCI* -ის აღმოსაფხვრელად [2].

ML ალგორითმები, როგორიცაა ნაივ ბაიესი (NB) [6], დამხმარე ვექტორული აპარატი (SVM) [7], ლოგისტიკური რეგრესია (LR)[8] და გადაწყვეტილებათა ტყე (RF)[9] გამოიყენება მონაცემთა კლასიფიკაციისათვის [10], კიბერ ინციდენტების პრევენციასა და პროგნოზირებისათვის.

2. ლიტერატურის მიმოხილვა

კიბერუსაფრთხოება არის განვითარებადი და უზარმაზარი გამოწვევა მსოფლიოში სხვადასხვა კიბერ ინციდენტებთან დაკავშირებით. მნიშვნელოვანი ნაწილია არსებული ინციდენტების იდენტიფიცირება სხვადასხვა DM-ML ალგორითმის გამოყენებით. DM-ML-ზე დაფუძნებული მიდგომები არის ძალიან ცნობილი ტექნიკა, რომლებიც გამოიყენება კიბერუსაფრთხოების დაუცველობის გამოსავლენად და სწორედ ამიტომ გამოიყენება BoW მოდელში, ხოლო კლასიფიკატორისათვის გამოიყენება NB, SVM, LR და RF ალგორითმები.

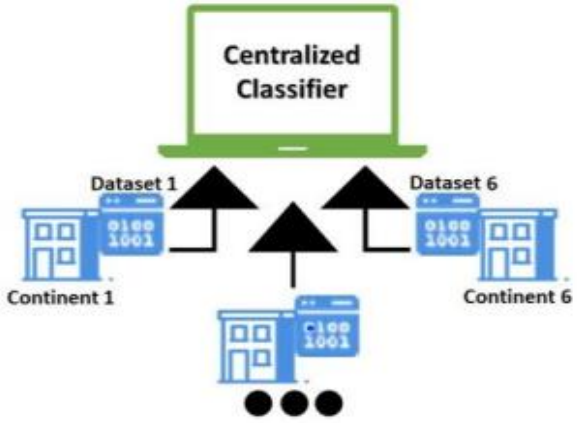
ბისვასმა და სხვა ავტორებმა [11] გამოიყენეს ტექსტის მოპოვების მიდგომა ციფრული ჯანდაცვის სფეროში კიბერ ინციდენტების გამოსავლენად. ავტორებმა გამოიყენეს ბუნებრივი ენის დამუშავება (NLP) ახალი ამბების მონაცემების მოსაპოვებლად და ინფორმაციის მისაღებად.

სურიმ და სხვა ავტორებმა [12] წარმოადგინეს ანომალიის დეტექტორი ავარიის შეტყობინების გამოყენებით. ისინი მუშაობდნენ ტექსტურ მონაცემებზე და გამოიყენეს *Local Outlier Factor* (LoF) ანომალიური მდგომარეობის გამოსავლენად. ავტორებმა გამოიკვლიეს სხვადასხვა DM-ML მიდგომები მავნე პროგრამების აღმოსაჩენად, ასევე ღრმა სწავლების მეთოდოლოგია, რომელიც გამოიყენება კიბერშეტევების პროგნოზირებისათვის, ქსელის ტრაფიკიდან მიღებული მონაცემების საფუძველზე.

[2] Research work through the project number: IFP22UQU4310108DSR188.

ფანგმა და სხვებმა [13], შეიმუშავეს კიბერშეტევის მეთოდები დამხმარე ვექტორის აპარატის (SVM) გამოყენებით, ML ალგორითმში. ავტორებმა დაასკვნეს სხვადასხვა DM-ML მიდგომები, როგორიცაა ბაიესის ქსელი, გადაწყვეტილების ხე, კლასტერირება და ხელოვნური ნეირონული ქსელები (ANN) კიბერუსაფრთხოებაში კიბერ ინციდენტების გამოსავლენად.

აშრაფმა და სხვა მკვლევარებმა აჩვენეს ცენტრალიზებული კლასიფიკატორის გამოყენების ეფექტურობა (ნახ.1). ნაჩვენებია, თუ რომელი ტიპის *SCI* მოხდა და მსოფლიოს რომელ კონტინენტზე, მონაცემთა ნაკრები გამოიყენეს ცენტრალიზებული კლასიფიკატორის მოსამზადებლად თითოეული კონტინენტისათვის.



სურათი 1. ცენტრალიზებული კლასიფიკატორის მონაცემთა ბაზა ექვსი კონტინენტის მიხედვით

მონაცემთა ნაკრები არის *SCI*-ის ტიპი, რომელიც მოხდა მსოფლიოს 6 კონტინენტზე (2003 წლის სექტემბრიდან 2023 წლის ოქტომბრამდე), სტრატეგიული და საერთაშორისო კვლევების ცენტრის (CSIS) ანგარიშის მიხედვით[14]. SCI რაოდენობა აზიისთვის უფრო მაღალია, რადგან ეს არის ყველაზე დიდი კონტინენტი მსოფლიოში.(ცხ.1.).

ცხრილი I
მონაცემების განაწილება

SCI ტიპი	აფრიკა	აზია	ევროპა	ჩრდილოეთ ამერიკა	ოკეანია	სამხრეთ ამერიკა	SCI რაოდენობა
APT	4	62	25	20	5	0	116
DDoS	0	15	13	6	3	0	37
DoS	0	1	0	0	0	0	1
Espionage	1	8	7	7	1	0	24
Malware	4	46	53	19	3	0	125
Man-in-Middle	1	1	1	1	1	0	5
Phishing	3	55	86	47	6	8	205
SQL Injection	2	3	6	2	0	0	13
Total	15	203	194	103	20	8	543

ამ კვლევამ გამოავლინა, გამოიკვლია და გადაჭრა, თუ როგორ უნდა გამოვთვალოთ კონტინენტის სახელი *SCI*-ის ტიპის მიხედვით.

კლასიფიკაციისათვის გამოიყენება მანქანური სწავლების ოთხი განსხვავებული კლასიფიკატორი [15]:

ნაივ ბაიესი (NB) - იგი ეფუძნება ბაიესის თეორემას, რომელიც გამომდინარეობს პირობითი ალბათობიდან. ის ჩვეულებრივ გამოიყენება ზედამხედველობით სწავლაში ტექსტის მონაცემთა კლასიფიკაციისთვის. *NB* ეფექტურია არაწრფივი ამოცანებისთვის.

დამხმარე ვექტორის აპარატი (SVM) - ეს არის ზედამხედველობითი სწავლebის კლასიფიკატორი. *SVM* არის ვექტორული მიდგომა და ძალიან ეფექტურია, თუ პრობლემა წრფივია და მონაცემთა ნაკრები შეზღუდულია.

ლოგისტიკური რეგრესია (LR) - პროგნოზირებს ორობით პრობლემას და მის შედეგებს ეფექტურად. ის გვაწვდის ინფორმაციას მახასიათებლების სტატისტიკური მნიშვნელობის შესახებ და იყენებს ალბათურ მიდგომას.

გადაწყვეტილებათა ტყე (RF) - *Random Forest* შედგება მრავალი გადაწყვეტილების ხისგან, მოდელის ეფექტურობის გაზრდით. ის ასევე მუშაობს არაწრფივ ამოცანებზე. ტექნიკური თვალსაზრისით, ეს არის მეთოდი გადაწყვეტილების ხეების გენერირებისათვის მონაცემთა ნაკრების ქვეჯგუფიდან.

პროექტის შესრულებისას გამოიყენეს უნიგრამის და ბიგრამის მოდელების კონცეფცია, მონაცემებიდან სიტყვების გასაფილტრად მინიმალური სიხშირით.

ექსპერიმენტული კვლევისას კლასიფიკატორების გამოყენების შედეგია კონტინენტის სახელის პროგნოზირება *SCI*-ის ტიპის მიხედვით. კლასიფიკატორების მუშაობის შესაფასებლად, გამოიყენება სიზუსტე და F1-ზომა, როგორც შესრულების ინდიკატორები. სიზუსტის ზომები NB, LR და RF არის (0.952396, 0.920829), (0.984139, 0.962375), (0.978099, 0.962375) შესაბამისად. SVM, NB, LR და RF კლასიფიკატორები შეფასდა სათითაოდ და დადგინდა რომ აზია, ყველაზე მეტად დაზარალებული რეგიონია *SCI* კუთხით.

3. დასკვნა

ეს ნაშრომი ფოკუსირებულია 2003 წლის სექტემბრიდან 2023 წლის ოქტომბრის ჩათვლით მნიშვნელოვან კიბერ ინციდენტებზე (SCI) დაფუძნებულ კვლევაზე, სტრატეგიული და საერთაშორისო კვლევების ცენტრის (CSIS) ანგარიშის მიხედვით. ოთხი განსხვავებული კლასიფიკატორით, ასევე პროგნოზირებულია რომელი კონტინენტი უფრო მეტად განიცდის *SCI*-ს ამ პერიოდის განმავლობაში.

მომავალში, *SCI*-სათვის სხვადასხვა მონაცემთა ნაკრები შეიძლება განიხილებოდეს და სხვადასხვა მანქანური სწავლების კლასიფიკატორების გამოყენებით, მათი ეფექტურობის შესამოწმებლად, როგორიცაა ფედერალური მანქანური სწავლება (FML). გარდა ამისა, აღნიშნულ მოდელში უსაფრთხოების გასაძლიერებლად ასევე შეიძლება Blockchain-ის განხორციელება.

გამოყენებული ლიტერატურა:

1. Li Y., and Liu Q., 2021, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186;
2. Hejase H., Kazan H., Hejase A, and Moukadem I, 2021, "Hejase et al. Cyber Security paper," Computer and Information Science, vol. Vol. 14, pp. 10–25, doi: 10.5539/cis. v14n2p10;
3. Hodgson Q,, Clark-Ginsberg A., Haldeman Z., Lauland, A and Mitch I.,2022, Managing Response to Significant Cyber Incidents: Comparing Event Life Cycles and Incident Response Across Cyber and Non Cyber Events. Santa Monica, CA: RAND Corporation, doi: 10.7249/RRA1265-4;
4. Handa A., Sharma A., and Shukla S., 2019, "Machine learning in cybersecurity: A review," WIREs Data Mining and Knowledge Discovery, vol. 9, no. 4, p. e1306, doi: 10.1002/widm.1306;
5. Mumtaz G., Akram S., Waseem M., Iqbal M., Ashraf U., Almarhabi K., Mohammed A., and Adel A., 2017, "Classification and Prediction of Significant Cyber Incidents (SCI) using Data Mining and Machine Learning (DM-ML)".
6. Alqahtani H,. Sarker I., Kalim, A., Minhaz Hossain M., Ikhlaq S., and Hossain 2020, "Cyber Intrusion Detection Using Machine Learning Classification Techniques," in Computing Science, Communication and Security, Singapore, pp. 121–131.;
7. Bhusal N., Gautam M., and Benidris M., 2021, "Detection of Cyber Attacks on Voltage Regulation in Distribution Systems Using Machine Learning," IEEE Access, vol. 9, pp. 40402–40416, doi: 10.1109/ACCESS.2021.3064689.
8. Bapat R., et al., 2018, "Identifying malicious botnet traffic using logistic regression," in Systems and Information Engineering Design Symposium (SIEDS), pp. 266–271. doi: 10.1109/SIEDS.2018.8374749;
9. Ustebay S., Turgut Z., and Aydin M., "Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier," in 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Dec. 2018, pp. 71–76. doi: 10.1109/IBIGDELFT.2018.8625318.;
10. Chayal N., and Patel N., 2021, "Review of Machine Learning and Data Mining Methods to Predict Different Cyberattacks," in Data Science and Intelligent Applications, Singapore, pp. 43–51;
11. Biswas B., Mukhopadhyay A., Bhattacharjee S., Kumar A., and Delen D., 2022, "A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums," Decision Support Systems, vol. 152, p. 113651, doi: 10.1016/j.dss.2021.113651;
12. Souri A., and Hosseini R., 2018, "A state-of-the-art survey of malware detection approaches using data mining techniques," Hu-man-centric Computing and Information Sciences, vol. 8, no. 1, p. 3, doi: 10.1186/s13673-018-0125-x;
13. Fang X., Xu M., and Zhao P., 2019, "A deep learning framework for predicting cyber-attacks rates," EURASIP Journal on Information Security, doi: 10.1186/s13635-019-0090-6;
14. "Significant Cyber Incidents (SCIs)." [Online]. Available: https://www.csis.org/programs/strategictechnologies-program/significant-cyber-incidents;
15. Xu S., 2018, "Bayesian Naïve Bayes classifiers to text classification," J. Inf. Sci., vol. 44, no. 1, pp. 48–59, doi: 10.1177/0165551516677946.

Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 69 – 75 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

A MULTI-PRONGED FRAMEWORK FOR A CYBER-SECURE NIGERIA

Ahmed Abubakar Aliyu[1,2]
[1] School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072
[2] Faculty of Computing, School of Science, Computing and Engineering, Kaduna State University, Kaduna 800283, Nigeria

ABSTRACT. The digital revolution has presented significant opportunities, but it has also introduced new threats, such as cybercrime. Nigeria is facing substantial cyber threats, which cost billions of Naira and impact individuals and businesses. The challenges include inadequate awareness, weak legal frameworks, limited digital literacy, and poor cyber hygiene. To enhance cybersecurity in Nigeria, a multi-pronged approach is necessary. This includes advanced cybersecurity tools, robust legal frameworks, education campaigns, capacity building, and public-private partnerships. Success stories from other countries, such as Singapore and Kenya, offer valuable lessons for Nigeria. Therefore, this paper proposes a multi-pronged framework to improve cybersecurity in Nigeria. By adopting these frameworks and best practices as well as working together, Nigeria can create a secure and prosperous digital future.

KEYWORDS: Cybersecurity, Digital literacy, National Security, Cyber Crime, Cyber hygiene

1. INTRODUCTION

The digital revolution has profoundly changed our lives, affecting the way we connect and do business, changing the way we live, the way we connect, and the way we do business as technology has become an integral part of our existence. In Nigeria, the digital sphere offers tremendous opportunities for economic growth, social development, and individual empowerment [1]. However, this connectivity also exposes us to new threats, such as the ever-evolving realm of cybercrime. As new technologies emerge, cybercriminals are constantly adapting and innovating, developing sophisticated methods to exploit vulnerabilities and cause devastating damage [2]. Cybercrime covers a wide range of activities, from online fraud and data breaches to malware attacks and cyber espionage, and its impact is far-reaching and diverse. Businesses suffer significant financial and reputational losses, individuals lose their hard-earned savings and sensitive information, and critical infrastructure is compromised, posing a threat to public safety and national security. In the face of escalating threats, a robust and proactive cybersecurity posture in Nigeria is more important than ever [3]. This is not only a technical challenge, but also a societal imperative. Achieving a cyber-secure Nigeria requires a holistic approach that goes beyond technological solutions. It requires collaboration, awareness, and a commitment to fostering a culture of cybersecurity at all levels of society.

The Cyber Security Experts Association of Nigeria (CSEAN) National Cyber Threat Forecast 2023 paints a concerning picture for Nigeria's cybersecurity landscape [4]. The report anticipates a rise in ransomware attacks targeting both public and private entities, alongside growing concerns about misinformation campaigns and attacks on vulnerable government assets. Furthermore, the potential

for insider threats, potentially involving malicious use of Artificial Intelligence, raises additional concerns. The report emphasizes the need for collaboration between individuals, organizations, and law enforcement to combat these evolving threats and build a safer digital environment. This necessitates proactive security measures and continuous vigilance from all stakeholders in Nigeria. Table 1 compares some top cybercrime around the world based on the MSSPAleart cybersecurity list and annual research.

Tab. 1. Comparative overview of some cybercrime concerns

Country	Ranking	Key Concerns	Notes
China	1	High number of cyberattacks, often targeting critical infrastructure	Data breaches, espionage, intellectual property theft
Brazil	5	High volume of cybercrime targeting the financial sector	Banking fraud, credit card scams, data breaches
United States	10	High volume of cybercrime incidents due to extensive digital infrastructure	Phishing attacks, malware infections, identity theft
Russia	N/A	High prevalence of cybercrime actors and activity	Ransomware attacks, disinformation campaigns, online fraud
Nigeria	16	High volume of cybercrime targeting individuals and businesses	Online scams (e.g., romance scams), phishing attacks, malware infections

This study examines the complex landscape of cybercrime in Nigeria. It analyses the evolving threats, assesses the current state of cybersecurity, and identifies the vulnerabilities that require immediate attention. It also explores potential solutions and strategies to build a cyber-secure nation and ensure a prosperous digital future for the next generation. The study aims to encourage stakeholders in government, the private sector, civil society, and academia to recognize the urgency of addressing cyber threats. It advocates a multi-pronged approach that includes proactive defense mechanisms, robust regulatory frameworks, comprehensive awareness campaigns, and investment in critical cybersecurity infrastructure.

2. PREVALENCE AND IMPACT OF CYBERCRIME IN NIGERIA

Cybercrime is a significant and growing threat in Nigeria, affecting individuals, businesses, and the nation as a whole [5]. Understanding its prevalence and impact is critical to developing effective strategies to combat this evolving threat. This paper provides a statistical snapshot: As cybercrime is estimated to cost the world about $7 billion, it costs Nigeria over $500 million annually, representing a significant drain on the country's economy[6]. In 2021 alone, Nigeria experiences 14.7 million cyber-attacks, the highest in Africa and the seventh highest in the world. Individuals aged 18-34 are particularly vulnerable, accounting for 60% of cybercrime victims. Online scams such as 'Yahoo Yahoo' scams, romance scams, and phishing attacks targeting bank accounts and sensitive information are widespread. Data breaches are also an issue. The National Identity Management Commission (NIMC) database breach in 2019 exposed the personal information of over 50 million Nigerians. Ransomware attacks, which target businesses and critical infrastructure, are increasingly common. Online platforms are often used for cyberbullying and harassment of individuals, especially women and children [7]. These are just a few examples of the diverse and pervasive nature of cybercrime in Nigeria. The CSEAN predicts that there will be an increase in insider threats in Nigeria in 2024 due to the malevolent use of artificial intelligence [8]. The consequences can be devastating, ranging from financial loss and identity theft to emotional distress

and reputational damage. Several factors contribute to the prevalence and impact of cybercrime in Nigeria, including a lack of cybersecurity awareness. Many Nigerians lack basic knowledge about cyber threats and how to protect themselves online.

Nigeria faces a significant challenge with inadequate cybersecurity awareness among its citizens, who often lack basic knowledge about cyber threats and how to protect themselves online. Furthermore, the country's cybercrime laws are still evolving, resulting in gaps and challenges in enforcement [9]. Limited access to technology and a lack of digital literacy skills can impede individuals' ability to protect themselves online. Poor cyber hygiene practices, such as weak passwords, insecure Wi-Fi networks, and the use of pirated software, can increase vulnerability to cyber-attacks. To address these vulnerabilities, a multi-pronged approach is necessary. This includes raising cybersecurity awareness through public education campaigns, community outreach programs, and school curricula. Equipping Nigerians with the knowledge and skills to stay safe online is crucial. Additionally, it is important to strengthen the legal framework by implementing robust cybercrime laws with clear definitions, effective enforcement mechanisms, and proportionate penalties to deter cybercriminals. Promoting digital inclusion is crucial. Nigerians can be empowered to participate in the digital world safely and securely through affordable internet access, technology training programs, and digital literacy initiatives. To reduce the risk of cyber-attacks, it is important to promote strong passwords, secure Wi-Fi networks, and responsible online behavior.

Moreover, a report by leading cybersecurity professionals has anticipates a significant rise in cyber threats throughout 2024. The report urges individuals, organizations, and governmental bodies to adopt a proactive and vigilant approach to safeguarding cyberspace. One of the most concerning trends highlighted in the report is the anticipated surge in ransomware attacks. Malicious software programs, designed to lock or encrypt critical data and demand ransom payments for its recovery, are expected to continue targeting both public and private entities across diverse sectors. This poses a significant threat to national security, economic stability, and individual privacy, as successful attacks can disrupt critical operations, lead to financial losses, and expose sensitive information. Moreover, the report highlights the increasing danger of misinformation and disinformation campaigns. Malicious actors are using digital platforms more and more to spread false or misleading information, with the aim of manipulating public opinion, causing division, and eroding trust in institutions. This can have serious consequences, hindering informed decision-making, exacerbating social divisions, and potentially threatening national security. There are concerns regarding the vulnerability of government online assets. As the public sector increasingly relies on digital infrastructure, government websites and databases become more attractive targets for cybercriminals. These attacks can aim to disrupt critical services, steal sensitive data, or manipulate information for malicious purposes. This underscores the need for strong cybersecurity measures in government agencies to safeguard the security and integrity of critical infrastructure. Furthermore, the growing concern of insider threats, particularly with the potential integration of Artificial Intelligence (AI) in cyberattacks, disgruntled employees or individuals with authorized access to sensitive information pose a significant risk as well as malicious actors may exploit insider access to orchestrate sophisticated attacks. Therefore, robust access control mechanisms, employee education, and continuous monitoring within organizations are necessary.

3. MULTI-PRONGED FRAMEWORK PROPOSAL

Cybersecurity has become a critical national imperative for Nigeria due to the country's increasing reliance on digital infrastructure. A multi-pronged framework approach is required to combat the evolving threat landscape, which requires a mix of technological advancements, robust regulatory

frameworks, proactive education, and collaborative efforts among various stakeholders. Investing in advanced cybersecurity tools and building a robust cybersecurity workforce is both fundamental to ensuring effective cybersecurity. Capacity building in this area is essential. This includes the deployment of intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) tools, and threat intelligence platforms [10]. It is also essential to strengthen critical infrastructure with secure hardware, software, and network architecture. Improve incident response capabilities, including rapid threat identification. Strong legal frameworks serve as a deterrent and ensure accountability. Nigeria should regularly review and update its cybercrime laws to keep pace with evolving threats and modus operandi. It is essential to have clear definitions of cybercrimes, proportionate penalties, and effective enforcement mechanisms. Working with international partners to develop harmonized cybercrime legislation will enhance global security and facilitate cross-border investigations.

Implementing national awareness campaigns through a variety of channels, from traditional media to targeted online platforms, is critical. These campaigns should educate individuals and businesses about common cyber threats, phishing tactics, password hygiene, and safe online practices. Integrating cybersecurity education into school curricula will equip future generations with the knowledge and skills necessary to navigate the digital world safely. Building a robust cybersecurity workforce which requires investment in training and development programs to create a skilled pool of cybersecurity professionals is essential. Specialized training in areas such as digital forensics, incident response, threat analysis, and vulnerability assessment is essential. Establishing centers of excellence for cybersecurity research and innovation can further propel Nigeria to become a regional leader in the field.

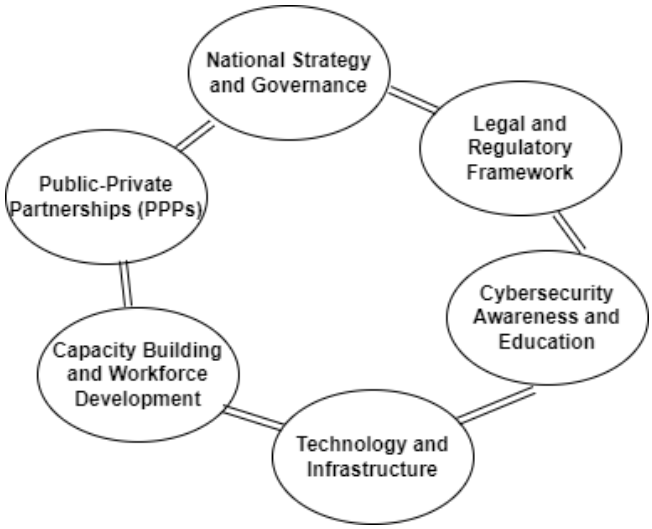


Fig. 1. Multi-Pronged Framework Proposal

As depicted in Figure 1, Public-private partnerships (PPPs) are powerful drivers of cyber resilience. Establishing formal platforms for collaboration between government agencies, private sector entities, and civil society organizations promotes knowledge sharing, resource pooling, and coordinated responses to cyber threats. Leveraging the expertise and resources of the private sector enhances technological capabilities and incident response agility. Civil society organizations play a critical role in raising awareness, advocating for stronger regulatory frameworks, and empowering vulnerable communities. Through this multi-pronged approach, Nigeria can chart a path to cyber resilience. Through technological fortification, robust legal frameworks, proactive education, capacity building, and collaborative synergies, the country can protect its digital assets,

foster trust in its digital economy, and empower its citizens to navigate the digital world with confidence. Table 2 explains the Multi-Pronged Framework proposal description.

Tab. 2. Multi-Pronged Framework description

Framework Component	Description	Example Initiatives
National Strategy and Governance	Develop a comprehensive national cybersecurity strategy with clear goals, priorities, and action plans. Establish a dedicated cybersecurity agency or department to oversee implementation.	Develop a national cybersecurity strategy in line with Singapore's model. - Establish a National Cybersecurity Center to coordinate efforts across government agencies.
Legal and Regulatory Framework	Enact robust cybercrime laws with clear definitions of offenses, proportionate penalties, and effective enforcement mechanisms. Strengthen data protection regulations and promote international cooperation on cybercrime.	Implement mandatory data breach notification laws similar to the EU's GDPR. - Collaborate with Interpol and ITU on cyber threat intelligence sharing and capacity building.
Cybersecurity Awareness and Education	Implement nationwide awareness campaigns to educate individuals and businesses about cyber threats, best practices, and personal responsibility. Integrate cybersecurity education into school curriculums.	Launch public awareness campaigns through diverse channels like TV, radio, and social media. - Develop age-appropriate cybersecurity curricula for schools.
Technology and Infrastructure	Invest in advanced cybersecurity tools and technologies, including intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) tools, and threat intelligence platforms. Secure critical infrastructure and government systems.	Modernize government IT infrastructure with secure hardware, software, and network architecture. - Establish a national cyber incident response center.
Capacity Building and Workforce Development	Train and develop a skilled workforce of cybersecurity professionals through specialized training programs in areas like digital forensics, incident response, threat analysis, and vulnerability assessment.	Establish centers of excellence for cybersecurity research and innovation. - Partner with universities and private sector companies to offer cybersecurity training programs.
Public-Private Partnerships (PPPs)	Foster collaboration between government agencies, private sector entities, and civil society organizations to share resources, expertise, and best practices. Encourage joint initiatives to address cyber threats and build cyber resilience.	Establish platforms for dialogue and information sharing between stakeholders. - Partner with private companies to develop and deploy innovative cybersecurity solutions.

4. ADAPTING BEST PRACTICES

Singapore's Cyber Security Agency (CSA) is a model of effective public-private partnership (PPP) in cyber security. The CSA actively works with private companies and civil society organizations on initiatives such as awareness campaigns, threat intelligence sharing, and talent development. This collaborative approach has significantly improved Singapore's cyber resilience. Estonia's X-Road data exchange platform is another secure data exchange platform that enables seamless and secure information sharing between government agencies, businesses, and citizens. Its

decentralized architecture and strong encryption protocols offer valuable lessons for Nigeria in building a secure government information infrastructure. In Africa, Kenya's Cybercrime Unit is a specialized unit within the Directorate of Criminal Investigations that focuses on investigating and prosecuting cybercrime [11]. Its success in securing convictions and raising awareness has deterred cybercriminals and fostered a culture of cybersecurity in Kenya.

Develop a national cybersecurity strategy: Inspired by Singapore's comprehensive national cybersecurity strategy, Nigeria can articulate a clear vision, strategic priorities, and concrete action plans for building cyber resilience.

Establish a cybercrime task force: Similar to Kenya's dedicated cybercrime unit, Nigeria can create a specialized task force with law enforcement, technical experts, and legal professionals to effectively investigate and prosecute cybercrimes in addition to The Nigerian Computer Emergency Response Team which was established in the Office of the National Security Adviser.

Implement mandatory data breach notification laws: Following the European Union's General Data Protection Regulation (GDPR), Nigeria can implement mandatory data breach notification laws to hold organizations accountable for protecting personal data and informing individuals of security breaches.

Promoting digital literacy through public-private partnerships: Collaborations between government agencies, NGOs, and telecommunications companies can implement targeted digital literacy initiatives through mobile phone subscriptions, community centers, and school curricula.

Facilitating regional and international collaboration: Engaging in knowledge sharing and joint initiatives with other African nations and international organizations such as Interpol and ITU can enhance cyber threat intelligence sharing, capacity building, and coordinated responses to cross-border cybercrime.

5. CONCLUSION

The specter of cyber threats casts a long shadow over our increasingly interconnected world, and Nigeria stands at a critical juncture. The nation faces a stark choice: succumb to the vulnerabilities of cyberspace or forge a path towards a secure and prosperous digital future which is a call to action that cannot be ignored. Cybercrime flourishes in the digital shadows, inflicting significant economic losses, jeopardizing national security, and eroding trust in the online ecosystem. Data breaches expose the sensitive information that forms the bedrock of our digital identities, while malware infections cripple essential infrastructure and disrupt vital services. These are not distant threats; they are the harsh realities confronting the global community, and Nigeria is not immune. Yet, amidst these challenges, a glimmer of hope remains. Nigeria boasts a vibrant and resilient population, a burgeoning technology sector brimming with innovation, and a growing understanding of the critical need for cybersecurity [12]. These factors provide the foundation upon which the nation can not only overcome cyber threats but thrive in the digital age. Imagine a Nigeria where businesses operate with unwavering confidence, secure in the knowledge that their data and transactions are protected. Imagine citizens navigating the digital realm with unbridled curiosity, empowered by knowledge and shielded by a robust legal framework. Imagine a future where young minds, unfettered by the fear of cyber-attack, harness the power of technology to solve the pressing societal challenges that confront the nation. This is the vision for Nigeria's digital future, a future that must be collectively built. But this vision cannot be realized through individual efforts alone. It necessitates a collective endeavor, a unified voice rising against the shadows of cyber threats. This necessitates unwavering commitment from governments to enact robust cybercrime

legislation, invest in vital infrastructure, and foster a culture of cyber awareness. It requires the ingenuity of the private sector to develop cutting-edge security solutions and foster a thriving cybersecurity ecosystem. It necessitates the dedication of educators to equip future generations with the skills and knowledge to navigate the digital landscape with confidence. Finally, and most importantly, it demands the active participation of every citizen, young and old, to adopt safe online practices and champion the cause of cyber resilience. This is not just a fight against a faceless enemy; it is a fight for the very foundation of Nigeria's digital future. To secure this future, the nation must move forward with unity and purpose, embracing the collective responsibility of building a cyber-secure Nigeria. Let the world witness not the echoes of vulnerability, but the resounding anthem of a nation that refuses to be defined by cyber threats, but rather empowered by the boundless possibilities of the digital age. Together, this vision of a safer, more secure, and prosperous Nigeria can be achieved, where technology becomes a force for good, not a weapon of darkness. Let this be the digital legacy of this generation, a testament to the enduring spirit of resilience that defines the nation.

REFERENCES:

[1] K. Njenga, *Information Systems Security in Small and Medium-Sized Enterprises: Emerging Cybersecurity Threats in Turbulent Times*. 2022. doi: 10.52305/KSVB7323.

[2] A. A. Aliyu, "Improving Cloud Data Security by hybridization of Zero-Knowledge Proof and Time-Based One-Time Password," *KASU J. Math. Sci. KJMS*, vol. 1, no. 2, pp. 116–126, Dec. 2020.

[3] T. Akinyetun, "Poverty, Cybercrime and National Security in Nigeria," *J. Contemp. Sociol. Issues*, vol. 1, pp. 1–23, Aug. 2021, doi: 10.19184/csi.v1i2.24188.

[4] C. Kanu *et al.*, "Frauds and forgeries in banking industry in Africa: a content analyses of Nigeria Deposit Insurance Corporation annual crime report," *Secur. J.*, vol. 36, no. 4, pp. 671–692, Dec. 2023, doi: 10.1057/s41284-022-00358-x.

[5] J. Garba, J. Kaur, and E. N. M. Ibrahim, "Awareness of cybercrime among online banking users in Nigeria," *Niger. J. Technol.*, vol. 42, no. 3, pp. 406–413, Nov. 2023, doi: 10.4314/njt.v42i3.14.

[6] S. Olomu, "Nigeria tightens laws to tackle yearly cyber-crime losses of $500m," ITWeb Africa. Accessed: Mar. 04, 2024. [Online]. Available: https://itweb.africa/content/mYZRXM9gxVNvOgA8

[7] B. Sule, M. Yahaya, U. Sambo, and B. Mat, "Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy," vol. 4, pp. 27–61, Oct. 2021.

[8] S. Odeniyi, "Nigeria to witness high cyber threats in 2024 – Report," Punch Newspapers. Accessed: Mar. 02, 2024. [Online]. Available: https://punchng.com/nigeria-to-witness-high-cyber-threats-in-2024-report/

[9] A. A. Abubakar and A. U. Shamsuddeen, "Information Security: An Effective Tool For Sustainable Nigerian National Security And Development," *Sci. Pract. Cyber Secur. J.*, 2023, Accessed: Apr. 18, 2023. [Online]. Available: https://journal.scsa.ge/papers/information-security-an-effective-tool-for-sustainable-nigerian-national-security-and-development/

[10] A. A. Abubakar, J. Liu, and E. Gilliard, "An efficient blockchain-based approach to improve the accuracy of intrusion detection systems," *Electron. Lett.*, vol. 59, no. 18, p. e12888, 2023, doi: 10.1049/ell2.12888.

[11] K. V. Chitechi, B. Kiprono, and F. Tireito, "Cyber- Security Vulnerability and Initiatives in Kenyan County Governments," *Afr. J. Comput. Inf. Syst. AJCIS*, vol. 7, no. X, Art. no. X, Oct. 2023, doi: 10.1234/ajcis.v7iX.38.

[12] S. K. Fakunmoju, O. Banmore, A. Gbadamosi, and O. I. Okunbanjo, "Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance," *Binus Bus. Rev.*, vol. 13, no. 1, Art. no. 1, Jan. 2022, doi: https://doi.org/10.21512/bbr.v13i1.7305.